Computer Networks 80 (2015) 1–26

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

A survey on the recent efforts of the Internet Standardization Body for securing inter-domain routing

M.S. Siddiqui [a,b,*], D. Montero [a], R. Serral-Gracià [a], X. Masip-Bruin [b], M. Yannuzzi [a]

[a] *Networking and Information Technology Lab (NetIT Lab), Technical University of Catalonia (UPC), Spain*
[b] *Advanced Network Architectures Lab (CRAAX), Technical University of Catalonia (UPC), Spain*

ARTICLE INFO

Article history:
Received 20 November 2013
Received in revised form 22 January 2015
Accepted 27 January 2015
Available online 3 February 2015

Keywords:
BGP
Security
BGPSEC
Routing
Internet
Inter-domain

ABSTRACT

The Border Gateway Protocol (BGP) is the de facto inter-domain routing protocol in the Internet, thus it plays a crucial role in current communications. Unfortunately, it was conceived without any internal security mechanism, and hence is prone to a number of vulnerabilities and attacks that can result in large scale outages in the Internet. In light of this, securing BGP has been an active research area since its adoption. Several security strategies, ranging from a complete replacement of the protocol up to the addition of new features in it were proposed, but only minor tweaks have found the pathway to be adopted. More recently, the IETF Secure Inter-Domain Routing (SIDR) Working Group (WG) has put forward several recommendations to secure BGP. In this paper, we survey the efforts of the SIDR WG including, the Resource Public Key Infrastructure (RPKI), Route Origin Authorizations (ROAs), and BGP Security (BGPSEC), for securing the BGP protocol. We also discuss the post SIDR inter-domain routing unresolved security challenges along with the deployment and adoption challenges of SIDR's proposals. Furthermore, we shed light on future research directions in managing the broader security issues in inter-domain routing. The paper is targeted to readers from the academic and industrial communities that are not only interested in an updated article accounting for the recent developments made by the Internet standardization body toward securing BGP (i.e., by the IETF), but also for an analytical discussion about their pros and cons, including promising research lines as well.

1. Introduction

The Border Gateway Protocol (BGP) is the protocol used for exchanging reachability information in the inter-domain arena of the Internet. Unfortunately, it is widely accepted that the current version of BGP (version 4, usually denoted as BGP-4), does not provide any performance or security guarantees [1]. The intrinsic assumption of trust on the information exchanged between Autonomous Systems (AS) through the BGP protocol does not stand realistic anymore, as a number of day-to-day social as well as business applications, such as telephony, online-banking, and stock trading, increasingly rely on the Internet. The heavy reliance on such mission critical applications has played a vital role in motivating the increased interest in improving the security of the Internet. BGP has always been an interesting topic for the research community mainly due to several concerns related to its convergence [2–10], its churn [11–13], its limitations in terms of traffic engineering [14–17], policies [18–25], documented anomalies

* Corresponding author at: Networking and Information Technology Lab (NetIT Lab), Technical University of Catalonia (UPC), Spain. Tel.: +34 938967294.

E-mail addresses: siddiqui@ac.upc.edu (M.S. Siddiqui), dmontero@ac.upc.edu (D. Montero), rserral@ac.upc.edu (R. Serral-Gracià), xmasip@ac.upc.edu (X. Masip-Bruin), yannuzzi@ac.upc.edu (M. Yannuzzi).

http://dx.doi.org/10.1016/j.comnet.2015.01.017
1389-1286/© 2015 Elsevier B.V. All rights reserved.

[26–31], and other issues [32–40], but the recent large scale outages in the Internet acted as a catalyst for reviving the research focus toward its security [41–53].

The security issues in BGP arise from the implicit trust among BGP speakers, paving the way for a number of vulnerabilities and attacks. Furthermore, due to the complex way that BGP operates, it is hard to distinguish between a malicious attack and the unfortunate result of a misconfiguration. The misconfiguration in BGP is a regular occurrence, some of which have caused internationally noticeable Internet service disruptions in the past [54], as well as recently [55,56]. In fact, BGP is not a very complicated protocol, but the way it is operated in practice, that is, allowing flexible policies while maintaining global scalability, makes it intricate [57].

One of the main security problems of BGP is traffic hijacking, which occurs due to false IP prefix origination or false route propagation. The false IP prefix origination refers to the scenario when an AS advertises an IP prefix as its owner where in fact it is not. In 2008, the diversion of Youtube traffic toward an ISP in Pakistan caused unavailability of Youtube for several hours for almost the entire Internet, and this is just one of the several incidents occurring every year [56]. The false route propagation refers to the scenario where an AS manipulates the AS-path information, not related to itself, to influence the decision process of route selection on other ASes. In April 2010, one of the telecommunications companies in China allegedly hijacked 15% of the entire Internet traffic for about 15 min, by announcing routes belonging to other ISPs [58].

Another apparently simple but complex security problem regarding BGP that has caused large scale disruption in Internet service is referred to as a “route leak”. A route leak is a policy related anomaly that occurs when a route is not advertised according to the business relationship or the link classification—we will exemplify and delve into this issue along the paper (cf. Section 2.4). For instance, in February 2012, a misconfiguration at a multi-homed ISP leaked all its internal routes to one of its providers, including the routes from other providers, causing a national level disruption in Internet service in Australia [55].

In light of this, the improvement of BGP security has been an active research area since its adoption. There are detailed best practices and recommendations [59], which can be used as a first line of defense in mitigating the BGP anomalies, but even after such countermeasures, BGP remains vulnerable to some major attacks related to the authenticity and integrity of the exchanged information, stemming from the implicit trust model and the lack of intrinsic security mechanisms in BGP. As a result, several security mechanisms and protocols have been proposed during the past decade or so [60–81], suggesting from small changes up to the complete replacement of the BGP protocol. Despite these efforts, only minor tweaks have finally reached an operational status in practice. In this context, the Secure Inter-Domain Routing (SIDR) [82], an IETF [84] Working Group (WG), has put forward several recommendations which have gained interest from industry as well as from the research community. Indeed, a couple of the recommendations have already been adopted by regional Internet registries [85,86] and several providers.

In this paper, we particularly examine the SIDR’s contributions for securing BGP, including the Resource Public Key Infrastructure (RPKI) [87], Route Origin Authorizations (ROAs) [88] and BGPSEC [89], in light of the well-known set of BGP attacks. We also discuss the unresolved security vulnerabilities and considerations for BGP in the presence of SIDR’s solutions. SIDR’s recommended solutions do not attempt to address an important set of security anomalies, specifically, the policy related attacks [83]. Most of the existing proposals—including SIDR’s—approach BGP security from an operational perspective, and do not take into consideration the business policies among the ASes for securing BGP. This is mainly because the ASes keep the information regarding their relationships and routing policies with other ASes confidential, which makes the mitigation of policy related attacks, such as route leaks, a challenging problem. Then, we discuss the excess baggage of SIDR’s solution in terms of software, hardware and changes required to the current version of the BGP protocol. We also look at the deployment and adoption challenges of the SIDR’s solution. Although some of SIDR’s security recommendations are already in testing phase, the BGPSEC protocol is facing resistance because apart from requiring hardware upgrades on the routers it requires syntactical and operational changes in the BGP protocol as well. In this regard, it is crucial to explore different ways by which a proposed security mechanism could be integrated while avoiding collateral burden and fatal entropy to the existing inter-domain routing system. In this paper, we also discuss the proposition of decoupling or outsourcing the security requirements away from the protocol itself.

The rest of the paper is organized as follows. In Section 2, we present a brief overview about the AS polices in inter-domain routing and illustrate some of the main security vulnerabilities of the BGP-4 protocol. Section 3 compares the design principles of SIDR WG recommendations with earlier proposed solutions. We survey the contributions made by SIDR in Section 4. In Section 5, we examine SIDR’s contributions with respect to the BGP vulnerabilities described earlier, and discuss about their pros and cons. Section 6 discusses the potential of outsourcing inter-domain routing security chores; and finally, Section 7 concludes the paper.

2. Major vulnerabilities of BGP

The blind trust with which two neighboring BGP speakers accept the exchanged information gives rise to vulnerabilities that can be exploited in different ways. Besides, given the complex operation of BGP, a number of BGP anomalies can even occur due to misconfigurations rather than to malicious intent. In a nutshell, the attacks in BGP can be broadly classified into three categories, namely, false information exchange attacks (e.g., false IP prefix origination and false BGP update), BGP protocol manipulation attacks (e.g., Route Flap Damping and Minimum Route Advertisement Interval attacks [43,90]), and AS policy violations attacks (e.g., route leaks). It is important highlighting that the focus of this paper is not on the BGP attacks and anomalies themselves, but rather on providing a survey on the security proposals made by the SIDR WG, covering also crucial aspects such as their pros and cons as well as the main vulnerabilities and threats that will remain unsolved. The interested readers can refer to [91,92] and the references therein for detailed surveys on the security issues of BGP. In order to provide a self-contained survey, in this section we will briefly describe the security issues that were analyzed by the SIDR WG, and provide references to the literature for a profound analysis on the different security issues.

Before discussing the BGP anomalies, we will briefly review the business relations and policies among ASes, along with the BGP protocol, so as to facilitate the understanding of the BGP security issues and the limitations of SIDR's solutions.

2.1. Common business relations and policies among autonomous systems

The business relation between any two ASes dictates the kind of policies that would be implemented on that particular link. These business relationships can be typically classified into either provider–customer or peer-peer relation [93]. In the former case, the provider AS provides transit toward Internet for customer's traffic, and in the latter case, the two ASes provide transit for their respective customer traffic toward each other. From the business revenue perspective, a provider AS charges its customer AS for forwarding traffic to and from it, whereas a peer-peer relation may not involve financial settlement up to a certain agreed traffic ratio. Hence, in line with profit maximization objectives, for any received route, a customer route has preference over a peer or a provider route, and a peer route has preference over a provider route.

In a nutshell, the following model, known as valley-free rules [6], is usually adopted by an AS for further advertisement of received routes:

- Routes learned from customers are further advertised to other customers, peers and providers (Fig. 1(a)).
- Routes learned from peers are further advertised to customers only (Fig. 1(b)).
- Routes learned from providers are further advertised to customer's only (Fig. 1(c)).

However, there are exceptions to valley-free constraints [24,94] as they are not upheld sometimes to accommodate customized economic models due to a complex AS relationship between the ASes. For example, for contingency connectivity, ASes usually have one or more backup links with other ASes. These backup links deliberately do not follow valley-free rules to rectify the impact of primary link failures or network congestion [95]. We contend that understanding of AS relationship and AS policies is essential to better comprehend the attacks described next. For a detailed literature on AS relationship and AS policies, the reader can refer to [93].

As mentioned earlier, the protocol used for exchanging routing information between ASes is the BGP protocol. BGP enabled routers, called BGP speakers, exchange routing information with their direct neighbors through BGP updates. The BGP updates may consists of a list of withdrawn routes and a list of advertised routes along with their attributes. A BGP route has multiple attributes associated to it, which assist the receiving BGP speaker in selecting the best route following the BGP decision process (Section 9 in [1]). The first attribute used in the BGP decision process for selecting the best route for a destination is the *local pref*. It is usually used to enforce the preference of customer routes over peer and provider routes or preference of peer routes over provider ones. The route attributes allow ASes to implement their business policies by tuning their values for a route before considering it for route selection or advertising it further. For in-depth details of the BGP protocol itself, the reader can refer to [1,96,97].

2.2. Advertisement of false AS-Paths

The BGP speakers exchange BGP updates for sharing the reachability information among each other. One of the most important attributes of an advertised route is its

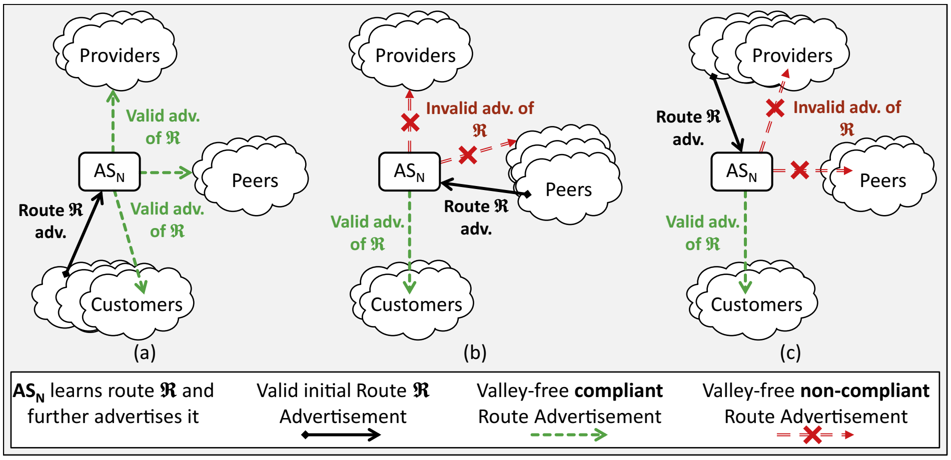


Fig. 1. Route re-advertisements according to the valley-free rules: (a) routes learnt from customers; (b) routes learnt from peers; and (c) routes learnt from providers.

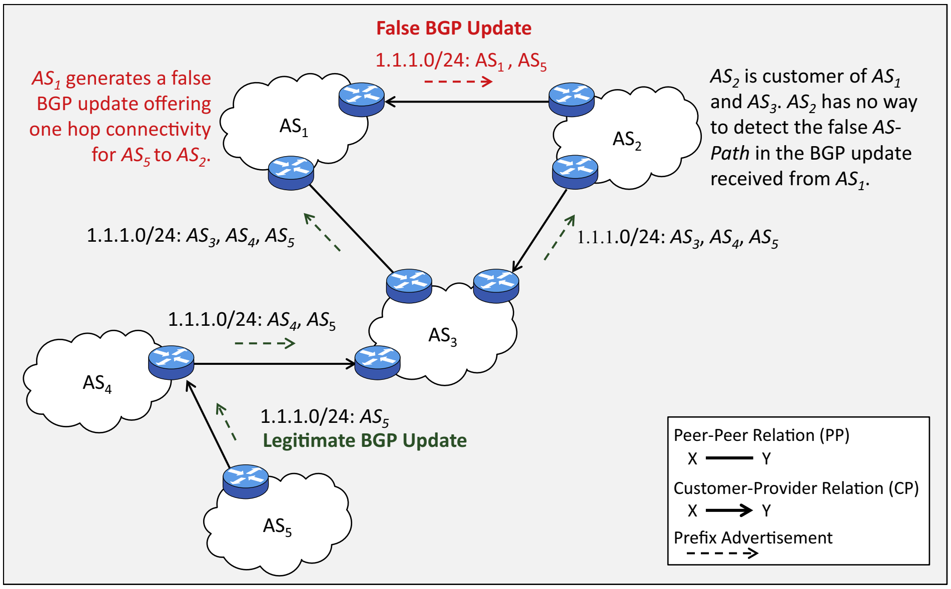

False BGP Update
1.1.1.0/24: AS1 , AS5
AS1 generates a false BGP update offering one hop connectivity for AS5 to AS2.
AS2 is customer of AS1 and AS3. AS2 has no way to detect the false AS-Path in the BGP update received from AS1.
AS1
AS2
1.1.1.0/24: AS3, AS4, AS5
1.1.1.0/24: AS3, AS4, AS5
AS3
1.1.1.0/24: AS4, AS5
AS4
1.1.1.0/24: AS5
Legitimate BGP Update
AS5
Peer-Peer Relation (PP)
X Y
Customer-Provider Relation (CP)
X Y
Prefix Advertisement

Fig. 2. False AS-Path attack.

AS_Path attribute. It lists all the ASes, starting from the origin AS to the AS which sent the update. However, a receiving BGP speaker has no means to verify the authenticity of the AS-Path information attached to a route in the update. Manipulating the *AS_Path* attribute can affect the BGP route decision process and thus lead to hijacking or black-holing of the traffic. For example, in Fig. 2 AS_1 generates a false BGP update offering one hop connectivity for IP prefix 1.1.1.0/24 owned by AS_5 to AS_2. AS_2 also receives the valid BGP update advertising IP prefix 1.1.1.0/24, but it will prefer the shortest path according to the BGP decision process (Section 9 in [1]). Without external means, AS_2 has no mechanisms to counter check the AS-Path information in the BGP update received from AS_1. This could result in either traffic black-holing, which is detectable as the traffic does not reach its destination, or in the worse case, traffic sniffing which is undetectable as the traffic is forwarded to the destination through a sub-optimal path, i.e., if AS_1 forwards the traffic to AS_5 via AS_3.

AS-Path Shortening: It is a particular case of false AS-Path attack. In this case, an AS deliberately manipulates the AS-Path information by reducing the AS-Path length so that it becomes more favorable during the route selection process at the next hop (Section 9 in [1]). It is worth mentioning that BGP legitimately allows BGP speakers to elongate an AS-Path for a route, by only prepending their own autonomous system number (ASN) in the *AS_Path* attribute for more than one time, calling it AS-Path prepending. The AS-Path prepending allows an AS to tune its policy on a link to some extent, but manipulating information other than its own in the AS-Path, or more precisely, removing another AS from the AS-Path refers to AS-Path shortening attack.

2.3. False route origination

Every AS advertises the IP prefixes it owns to its neighbor ASes through BGP peering, according to its internal policies and the business relationship that it has with each neighbor. The BGP protocol does not define any mechanism to verify that the AS originating the IP prefix advertisement is in fact the actual owner of this prefix, hence leaving room for exploitation due to unintentional or deliberate misconfigurations. As shown in Fig. 3, the IP prefix 1.1.1.0/24 is owned by AS_4, but AS_1 falsely originates the IP prefix 1.1.1.0/24 as its own to AS_2. AS_2 receives advertisements for the same IP prefix from AS_1 and AS_4 and without any out-of-band precautionary measures, AS_2 falls prey to the false advertisement. Following the BGP decision process [1], AS_2 will prefer the route from AS_1, since it offers the shortest AS-Path toward the destination IP prefix. This way, AS_1 successfully hijacks AS_2's traffic for AS_4.

The lack of in-built mechanisms in BGP to verify the AS origin of an IP prefix leads to the false route origination attack, resulting in either undetectable hijacking or detectable black-holing of the traffic. The false route origination attack differs from the false AS-Path attack in the sense that the latter does not lie about the origin of the prefix, but tries to inject a non-existent path in the network.

2.4. Route leaks

A route leak occurs when a route gets advertised over a link by an AS, which does not coincide with the link classification [98]. A more precise definition of a route leak is given as the receipt of a non-customer route advertisement over a peer or a customer link [99]. For example, in Fig. 4(a), AS_1 and AS_2 have a peer-peer relation. AS_3 is customer of both, AS_1 and AS_2, i.e., it is multi-homed. AS_2 has another customer, AS_4, which owns the IP prefix 1.1.1.0/24. AS_4 advertises the prefix 1.1.1.0/24 to its provider AS_2 (Step (i)). AS_2 being a provider of AS_3 and a peer of AS_1, advertises it to both of them (Steps (ii.a) and (ii.b)).

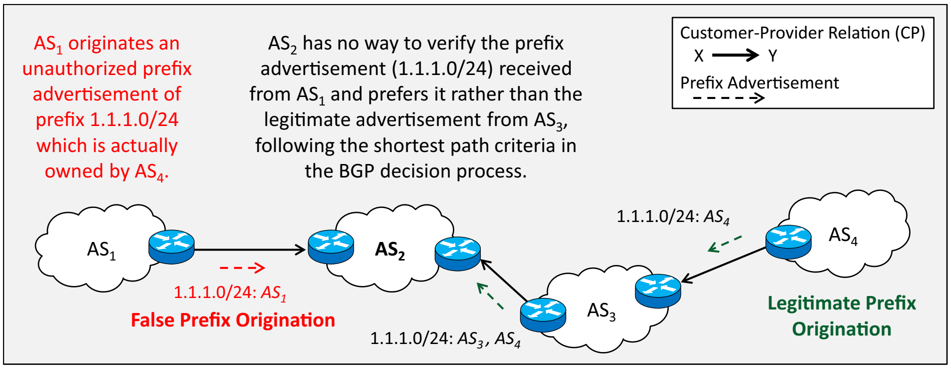
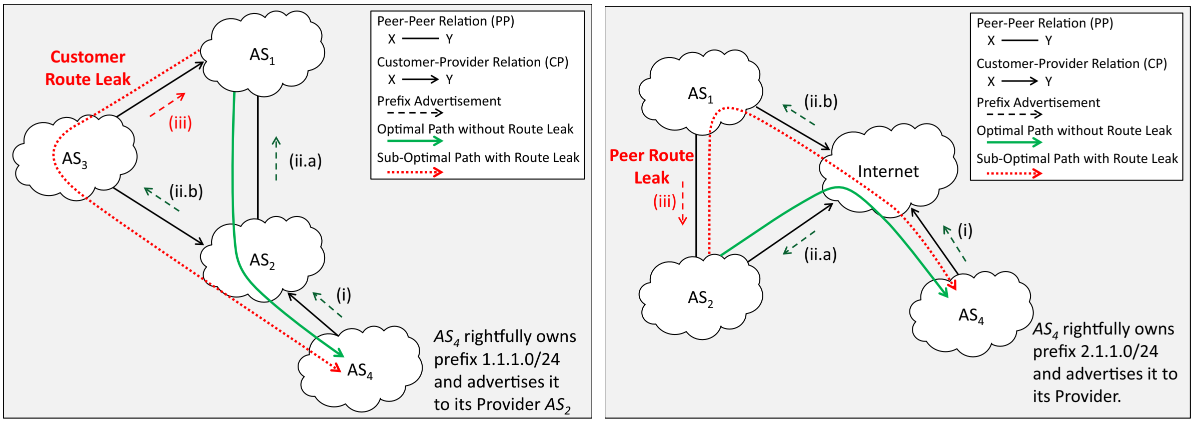

AS_1 originates an unauthorized prefix advertisement of prefix 1.1.1.0/24 which is actually owned by AS_4.
AS_2 has no way to verify the prefix advertisement (1.1.1.0/24) received from AS_1 and prefers it rather than the legitimate advertisement from AS_3, following the shortest path criteria in the BGP decision process.
Customer-Provider Relation (CP)
X → Y
Prefix Advertisement
AS_1
AS_2
AS_3
AS_4
1.1.1.0/24: AS_1
False Prefix Origination
1.1.1.0/24: AS_4
1.1.1.0/24: AS_3, AS_4
Legitimate Prefix Origination

Fig. 3. False IP prefix origin attack.


Customer Route Leak
AS_1
AS_2
AS_3
AS_4
(iii)
(ii.a)
(ii.b)
(i)
Peer-Peer Relation (PP)
X — Y
Customer-Provider Relation (CP)
X → Y
Prefix Advertisement
Optimal Path without Route Leak
Sub-Optimal Path with Route Leak
AS_4 rightfully owns prefix 1.1.1.0/24 and advertises it to its Provider AS_2
Peer Route Leak
(iii)
(ii.b)
(ii.a)
(i)
Internet
AS_4 rightfully owns prefix 2.1.1.0/24 and advertises it to its Provider.

(a) Route leak on a customer link.

(b) Route leak on a peer link.

Fig. 4. Route leak scenarios.

Now if AS_3 advertises 1.1.1.0/24 to AS_1 (Step (iii)), this falls in the category of a route leak. In this case, AS_1 gets advertisements for the same prefix from AS_3 and AS_2. As mentioned in Section 2.1, customers' routes are typically preferred over peer routes, hence AS_1 selects AS_3 as its next hop for the IP prefix 1.1.1.0/24, which apart from being sub-optimal, also allows AS_3 to sniff all the traffic from AS_1 to AS_4. This may also result in congestion at AS_3 causing traffic black-holing. The increase in the AS-Path length of the route advertised by AS_3 does not help in detecting this problem because customer routes are preferred by setting a higher *local-pref* attribute, which is evaluated before the *AS_Path* attribute [1]. In other words, the route is decided before comparing the AS-Path lengths. The route leak occurring on a customer–provider link is termed as a customer route leak. However, route leaks are also possible on a peer-peer link. In Fig. 4(b), the steps (i), (ii.a), (ii.b) and (iii) illustrate how route leaks can occur on a Peer-Peer link. AS_4 advertises its IP prefix 2.1.1.0/24 to its provider. AS_1 and AS_2 learn about this prefix from their respective providers. Now, if AS_1 advertises 2.1.1.0/24 to AS_2, then AS_2 would prefer the peer route over the route learnt from provider resulting in a route leak, causing the traffic between AS_2 and AS_4 to go through AS_1, making it vulnerable to sniffing.

3. Comparison of basic design principles of past inter-domain routing security proposals and SIDR's WG

During the past years, several proposals emerged to counter the security vulnerabilities of the inter-domain routing system. A detailed technical discussion on these proposals is certainly out of the scope of this paper, but interested readers can refer to [91,92,100] for detailed surveys on previous efforts addressing BGP security. The proposals that have received the majority of the attention—especially from the industrial sector—as they provide extensive BGP security solutions contemplating a wide set of BGP anomalies include s-BGP [60], so-BGP [61], ps-BGP [62] and IRV [63]. The recent security proposals from the SIDR WG describe a complete security framework for semantically securing BGP. Before we survey the SIDR proposals', namely, RPKI [87], ROAs [88] and BGPSEC [89], we will proceed to overview the main design principles on which the past solutions were based on, and compare them with the ones adopted in SIDR's proposals.

The SIDR WG approaches inter-domain routing security from the point of view of reducing the vulnerabilities in the system and precisely states the vulnerabilities it plans to address. The two main target goals dictating the design principles of SIDR's security proposals include prefix origin authorization and AS-Path validation. The prefix origin authorization refers to ensuring if an AS is authorized to originate an IP prefix. The AS-Path validation signifies ensuring that the AS-Path indicated in the BGP update is the path traveled by the BGP update. The SIDR security proposals explicitly narrow down their focus on the prefix origin authorization and AS-Path validation as design principles because in absence of such mechanisms several attacks with potential to cause large-scale damage can be launched against BGP, as described in the previous section. In a nutshell, the SIDR's proposals accomplish the two design principles with the help of a globally distributed security infrastructure, called Resource Public Key Infrastructure (RPKI) [87] (cf. Section 4.1), security objects called Route Origin Authorizations (ROA) [88] (cf. Section 4.2), and the BGPSEC protocol [89] (cf. Section 4.3). The ROA targets prefix origin authorization and the BGPSEC protocol addresses AS-Path validation, whereas the RPKI facilitates ROA and BGPSEC in achieving their goals. Next, we briefly review the design principles of past security proposals and compare them with the SIDR ones. Table 1 summarizes the comparison of design principles considered by different BGP security proposals.

3.1. s-BGP design principles

In terms of design principles, s-BGP [60] defines security of BGP as *the correct operation of BGP speakers*. That is, any action that causes an incorrect BGP operation is termed as an attack and should be countered as part of securing BGP. According to the s-BGP, the correct operation of a BGP speaker essentially implies three main constraints, (i) authenticity and integrity of a received BGP update; (ii) valid route advertisement authorized by the legitimate prefix owner; and (iii) correct application of BGP rules and AS policies while exporting, importing, and selecting the routes. The first constraint requires ensuring that the BGP update is sent by the BGP peer as indicated, received by the intended recipient and the content of the BGP update was not altered in transit. That is, s-BGP deems it fundamental to secure the sender and receiver identity along with the contents of a BGP update to avoid false BGP update attacks (cf. Section 2.2). The second constraint signifies ensuring that the BGP peer advertising an IP prefix is authorized to do so on behalf of the AS it belongs to and the legitimate owner of the IP prefix has authorized the AS to originate and advertise the prefix. That is, s-BGP considers route advertisement authorization essential along with prefix ownership authorization to counter false prefix originations and illegitimate route advertisements (cf. Section 2.3). The third constraint obligates ensuring that the BGP peer sending and the one receiving the BGP update have correctly followed the BGP rules and respective AS policies while processing it for route selection and further advertisement. In other words, s-BGP considered it a fundamental design principle for securing BGP to secure the way BGP rules and AS polices are applied to mitigate policy related attacks (cf. Section 2.4).

In comparison, the design principles of s-BGP are a super set of design principles of SIDR security proposals. The two target goals set by SIDR are almost the same as the first two constraints set by s-BGP, however the latter also includes the authentication of BGP peers apart from securing the contents of the BGP update. The SIDR security proposals do not address the authentication of BGP peers per se but assume the presence of transport security mechanisms, such as TCP MD5 authentication [101], for that purpose. Both security proposals consider it fundamental to ensure prefix origin authorization and AS-Path validation for securing the inter-domain routing. One apparent difference between the above mentioned security proposals is that the s-BGP considers correct application of BGP rules and AS policies as part of their security design principle, whereas the SIDR proposals do not. Although s-BGP includes policy related security in its design principles, it concedes that it remains unattended in its security proposal. As mentioned earlier, this is mainly because the local AS policies are kept confidential which makes it hard for an AS to ensure if they were not violated by another AS.

In terms of implementation, s-BGP's [60] Public Key Infrastructure (PKI) for establishing and maintaining verifiable security credentials, out-of-band address attestations for prefix origin authorizations, and an in-band and new optional transitive BGP attribute to support route validation, appears to be the inspiration behind SIDR's RPKI, ROA and BGPSEC, respectively. In fact, the SIDR's proposals can be seen as a refined version of s-BGP, and this represents the core of what is being standardized by the IETF [102]. However, SIDR's proposals describe mechanisms in far more detail and also give explicit considerations to pragmatic aspects of BGP, such as AS-Path prepending and Internet Exchange Point (IXP) transparency, as well as to partial and flexible deployments as compared to s-BGP, explained in detail in Section 4.

3.2. so-BGP design principles

The design principles adopted by so-BGP [61] for securing BGP include (i) prefix origin authorization; (ii) ensuring path availability from the advertising AS to the advertised

Table 1
Comparison of BGP security design principles of SIDR proposals with past BGP security proposals.

BGP security design principles	BGP security proposals				
	SIDR	s-BGP	so-BGP	ps-BGP	IRV
BGP peer authentication		√			
BGP update message integrity		√		√	√
IP prefix origin authentication	√	√	√	√	√
Route advertisement authorization	√	√	√		√
AS-Path Validation	√	√	√	√	√
AS-Policy compliance check		√	√		√

destination; (iii) route advertisement authorization and (iv) AS policy compliance for route advertisements. The first goal is the same as in s-BGP that to ensure if an AS is authorized to originate a particular IP prefix. The second goal is to make sure that there exist a path from the advertising AS to the destination it is advertising to counter BGP updates containing false AS-Path information. This design principle is a softer constraint on BGP security as compared to the burdensome AS-Path validation constraint in s-BGP. The intention for authorization and AS policy compliance of route advertisements are similar to second and third BGP security constraints of s-BGP mentioned above, however so-BGP security framework does not fulfill these two goals. The so-BGP is perceived to be an improvement over s-BGP as it relaxes the strict AS-Path validation requirement by path availability check to establish integrity of the AS-Path [91]. In comparison, both so-BGP and SIDR security proposals, consider IP prefix origin authorization and AS-Path verification, however, so-BGP also states route advertisement's AS policy compliance check as a goal but fails to accomplish it.

With respect to implementation, the so-BGP proposal recommends extensive use of different types of certificates, namely, *EntityCert*, *AuthCert*, and *ASPolicyCert*. The *EntityCert* and *AuthCert* are used to establish trust among entities and resources and for prefix origin authorizations, respectively. The *ASPolicyCert* contains the list of direct neighbor ASes which enables each AS to build their internetwork graph. This internetwork graph is used to verify the existence of advertised AS-Paths. One fundamental design differences between so-BGP and SIDR proposals is the use of web of trust instead of a PKI for validating signed objects. In this way, so-BGP avoided the burden of a PKI, but was required to establish trust anchors to support its validation framework in the absence of a PKI. The ambiguous validation framework of so-BGP casted doubts on the establishment of sufficient trust required for attestations and their validations. In this regard, SIDR proposals employ a hierarchical PKI for trust establishment. Another major design difference was the weak requirement of checking if the AS advertising a certain destination has a feasible route to it (with the use of ASPolicyCert) as compared to the strict AS-Path cryptographic verification employed by SIDR proposals. The design trade-offs including PKI avoidance and weak AS-Path validation was to make it less demanding in terms of processing and memory, but at the cost of weaker security. The SIDR proposals face a set of new challenges due to the hierarchical PKI and strict cryptographic AS-Path validation (cf. Sections 5.2 and 5.3), but it clearly does not compromise on the level of security.

3.3. ps-BGP design principles

The design goals of ps-BGP [62] are almost aligned with the SIDR design principles for securing BGP. They include AS number authentication, BGP speaker authentication, data integrity of BGP update, prefix origination verification and AS-Path verification. Like SIDR, the ps-BGP also does not consider assurance of correct application of AS policies as one of its design principles. With respect to s-BGP which has almost the same security goals, ps-BGP is also seen as an enhancement to it, however ps-BGP puts forward a different BGP security framework to achieve those goals.

From implementation perspective, the ps-BGP proposal realizes *Prefix Assertion Lists (PAL)* for accomplishing prefix origin authorization and digital signatures, similar to s-BGP, for securing the AS-Path. A *Prefix Assertion Lists (PAL)* is regularly generated by each AS containing the ASN to IP prefix bindings for the IP prefixes owned by the AS as well as for the known IP prefixes owned by its direct neighbor AS. Based on these *PALs*, each AS computes a *AS Prefix Graph* individually, which can be used to establish prefix origin authorization up to a certain level according to the internal policies of the AS. ps-BGP employs strict cryptographic validation of AS-Paths by using digital signatures, which is also the case in SIDR's proposals, however, ps-BGP allows partial AS-Path validations as compared to SIDR proposal's advocation of either plain AS-Path or complete cryptographically verifiable AS-Paths. The former establishes the validity of the AS-Path by using a rating mechanism depending on the ASes which include their signatures in the AS-Path. The allowance of partial AS-Path validations through the utilization of confidence levels makes ps-BGP "partial deployment friendly", however, SIDR proposals argue that using incomplete AS-Path validations is as good as no AS-Path validation at all, since unverifiable portions of an AS-Path undermine the security feature itself (cf. Section 4.3).

Another worth mentioning point is that, for establishing trust for resource authorization, psBGP utilizes a hierarchical PKI for AS numbers, but it suggests to use Internet Route Registries (IRRs) for authenticating the utilization of IP addresses. In this regard, ps-BGP inherits the shortcomings of IRRs including doubts on the authenticity and integrity of information. As mentioned earlier, SIDR proposals utilize a hierarchical PKI for both, AS numbers as well as for IP address resources, and trust is established using cryptographically verifiable certificates. Given the drawbacks of IRRs, it is obvious why SIDR did not choose an IRR-like framework for the dissemination of security credentials. Instead, the SIDR proposals accomplish the distribution of security credentials by means of a hierarchical infrastructure of repositories and local-caches (cf. Section 4.1).

3.4. IRV design principles

The design principles of Inter-domain Routing Validation (IRV) [63] are similar to the ones of s-BGP that is verification of information in the BGP updates including policy compliance check, prefix origin authorization, route advertisement authorization and AS-Path validation. However, IRV also considers design goals for achieving those verifications from an implementation point of view. These are based on the reasons for which past inter-domain security proposals fail to accomplish their targets. These design goals include incremental deployment, flexible routing information processing, and decoupling of the security solution from the BGP protocol. The incremental deployment implies that the solution offers considerable benefits even in the case of partial deployment of the solution. The flexibility in acquiring and validating routing information is important to avoid overwhelming the existing computational resources in the routers at run-time. The solution must run independent of the BGP protocol so as to offer minimum entropy to the installed base of BGP protocol. Thus, IRV is based on a query response framework that is completely separated from the BGP protocol. According to the proposal, on reception of a BGP update, the corresponding IRV service can query the respective IRV servers in other ASes to verify the required information for prefix origin authorization and AS-Path validation. However, the IRV proposal is silent on the details of how these authorizations and validations would be realized. Moreover, for AS-Path verification, it advocates for the validation of the queries and responses for all the ASes in the AS-Path. The main drawback of this approach is that it requires an underlying functioning network that greatly reduces the protocol scalability in an Internet wide topology. In comparison to SIDR security proposals, although the design principles of securing the BGP are same, a complete out-of-band on-demand security infrastructure was not an option for SIDR proposals, as they put huge emphasis on the practicality of their solution. However, the SIDR WG have taken a hybrid approach in the realization of their BGP security design principles in the sense that the RPKI and ROA are based on an out-of-band security framework whereas, the BGPSEC protocol is tightly coupled with the BGP protocol, as described next in Section 4.

4. IETF's secure inter-domain routing working group contributions

In spite of the efforts made by the research community for almost a decade and a half, the security of the BGP protocol remains as precarious as ever. The obvious conclusion that can be drawn is that, none of the main proposals made thus far has been sufficiently pragmatic to be adopted. While some of them required the addition or replacement of hardware elements, others needed the replacement of key software components, or they simply lacked details about their deployment and entire functioning, hence they did not convince the industrial players that needed to support an initiative of such magnitude. In this adverse scenario, the IETF's Secure Inter-Domain Routing (SIDR) working group (WG) [82] has put up serious effort, and is developing recommendations for securing BGP with strong focus on practical aspects, such as partial deployments. A list of published RFCs and drafts by the SIDR WG can be found in [82]. In the rest of this section, we survey SIDR's security proposals while focusing on RPKI, ROA and BGPSEC, and describe their roles in securing BGP, while illustrating their mechanisms and functioning in achieving their respective goals.

4.1. Resource Public Key Infrastructure (RPKI)

RPKI is a vital part of SIDR proposals since it defines and provides the basic security skeleton. RPKI consists of three main parts: (1) a resource allocation hierarchy; (2) a set of cryptographically protected objects; and (3) a distributed repository framework to hold these objects. Overall, RPKI mirrors the currently practiced administrative allocation hierarchy of Internet Number Resources (INRs) (e.g., IP addresses and AS numbers), where resources are distributed from the Internet Assigned Numbers Authority (IANA) [103], as root, to regional Internet registries (RIRs), and all the way down to Internet Service Providers (ISPs). However, in the case of RPKI, the resources are accompanied by X.509 certificates to form a chain of trust from top to bottom as illustrated in Fig. 5.

In the presence of X.509 certificates, each resource allocation action becomes cryptographically verifiable, as the certificate attests to the allocation of a particular resource, i.e., IP address or AS number. A Certification Authority (CA) corresponds to an entity that can further sub-allocate resources and delegate authorities using resource certificates. A CA uses a resource certificate called, "Certification Authority Certificate" (or CA certificate) to sub-allocate resources. Fig. 5 gives an overview of the CA certificate hierarchy. These CA certificates enable to form a chain of cryptographically verifiable trust from the root CA to a particular AS or ISP. End Entity (EE) certificates are another type of resource certificates which are used for delegating authorities, e.g., every ROA includes an EE certificate which enables its cryptographic verification, as shown in Fig. 5. These certificates and authorities are published in the respective RPKI repository publication point of each CA. Every CA in the RPKI regularly issues Certificate Revocation Lists (CRLs) to revoke invalid certificates. The collection of all such distributed repositories from all the CAs constitute the global RPKI, which is available to Relying Parties (RP) that would want to validate an attestation or authority.

Given such security skeleton, ASes can obtain certificates for the resources they own from the concerned resource allocation authorities. The ROA and the BGPSEC utilize these certificates to offer security to the exchanged information, such that the receiving party could verify the presented credentials with the help of the RPKI. Therefore, both ROA and the BGPSEC extensively rely on RPKI to achieve their goals, that is, verifying route origin advertisements, and securing route propagation updates, respectively. Each AS can have its own RPKI cache, which should be synchronized and updated regularly with the global RPKI. In fact, the global RPKI does not refer to one huge mother repository, but rather to a collection of distributed repositories which form the RPKI.

Observe that the RPKI is a new addition in the inter-domain routing infrastructure, and therefore, it requires extra investment for new hardware and software components. The SIDR WG has published a number of proposed standards as well as best practices RFCs related to RPKI. The RFC 6480 [87] provides detailed description of an infrastructure to support secure Internet routing.

4.2. Route Origin Authorization (ROA)

The Route Origin Authorization (ROA) is a signed authority contained in the RPKI which targets the traffic hijacking problem due to false route origination. The ROA makes use of RPKI to assure integrity in the route origin announcements. The RPKI enables the legitimate owner

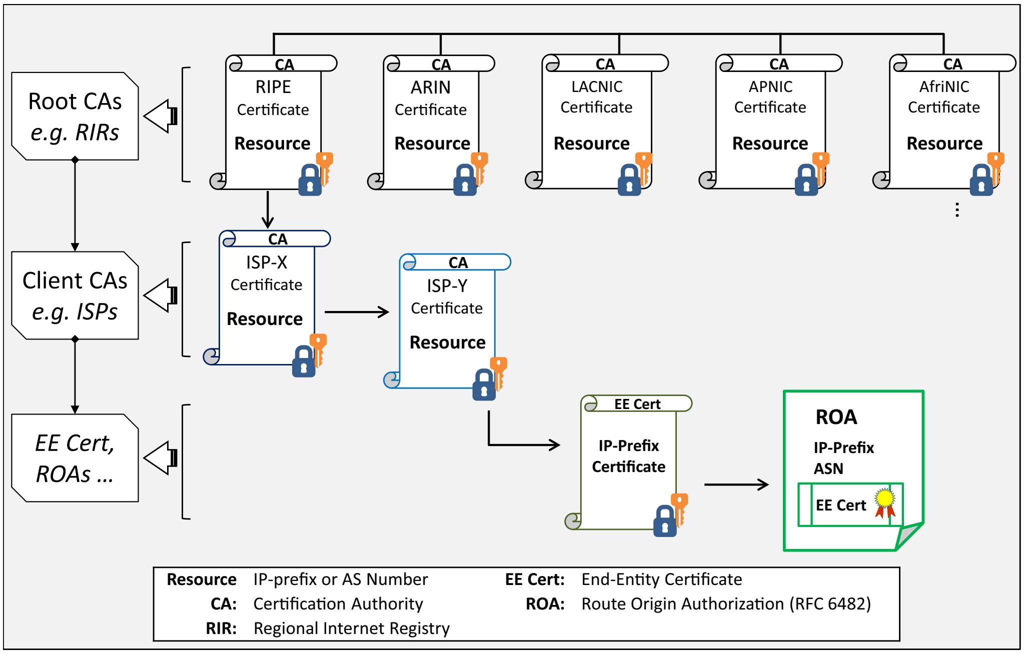


Fig. 5. Administrative resource allocation hierarchy.

of an IP prefix to produce an ROA and publish it in the RPKI repository. This signed authority binds the IP prefix resource with its owner's ASN by including the corresponding EE certificate inside it (see the bottom right of Fig. 5). Now, when an AS announces a particular IP prefix as its owner, the Relying Party (RP) can verify if this route origination announcement is legitimate or not with the help of RPKI. The RP queries the RPKI to confirm whether or not there exists an ROA for the announced IP resource with the advertising AS as its legitimate owner. The response of the query from the RPKI can be used to influence the BGP decision process according to the internal policy of the AS. In practice, instead of querying the global RPKI repository for every route origin announcement, RPs create validation filters using locally cached collection of valid ROAs.

For example, in Fig. 6, AS_2 has RPKI presence and BGP peering sessions with AS_1 and AS_3. Let us assume that AS_1 owns IP prefix 1.1.1.0/24, so it creates an ROA using the respective RPKI EE certificate and publishes it in the global RPKI repository. Then, AS_1 advertises the prefix to AS_2. On the other hand, AS_3 tries to advertise the same IP prefix to AS_2 as its originating AS, but it cannot produce a valid ROA from any administrative resource allocation authority as it is not the rightful owner of the prefix 1.1.1.0/24. When AS_2 receives the IP prefix announcement from AS_1, it verifies against the ROA validation filters extracted from RPKI for origin validation. The existence of a valid ROA for the respective prefix from AS_1 in the RPKI not only assures AS_2 the integrity of AS_1's announcement but also assures AS_2 that AS_3's prefix announcement is false.

As shown in Fig. 6, a new protocol called Router-RPKI (Rtr-RPKI), allows routers to reliably interact with RPKI to retrieve IP prefix origin data from a trusted RPKI cache [104]. Clearly, the RPKI caches need to be synchronized with the global RPKI repository, and for the moment, this is done through rsync (see Fig. 6). Finally, it is important to mention that without additional means, ROA requires minor changes to the BGP protocol itself for performing IP prefix origin validation. More specifically, as we shall discuss later in Section 6, the advent of Software Defined Networking (SDN) [105] could avoid the introduction of such changes in BGP, since the origin validation can be outsourced and run as a separate process not embedded in BGP. For further details on the procedure for validating an ROA using RPKI, the reader is referred to RFC 6483 [106].

4.3. Securing Route Propagation (BGPSEC)

The BGP updates exchanged among BGP peers for propagating reachability information, contain advertised and withdrawn routes along with their attributes as mentioned in Section 2.1. The false AS-Path vulnerability stems from the lack of verification of the authenticity of the *AS_Path* attribute of the advertised route. The *AS_Path* attribute of a route contains the path information, in effect, a sequential list of all the ASes that a specific route passed through. Essentially, securing route propagation refers to securing the *AS_Path* attribute of a particular route. The BGPSEC protocol [89] provides such mechanism, based on public key cryptography to secure the AS-Path information of an advertised route. Even though the BGPSEC protocol requires changes in the way BGP operates along with the requirement of a new BGP attribute, called *BGPSEC_Path*, it is backward compatible with the legacy BGP-4 protocol. Furthermore, the BGPSEC protocol is only recommended for securing inter-domain routing and not intra-domain

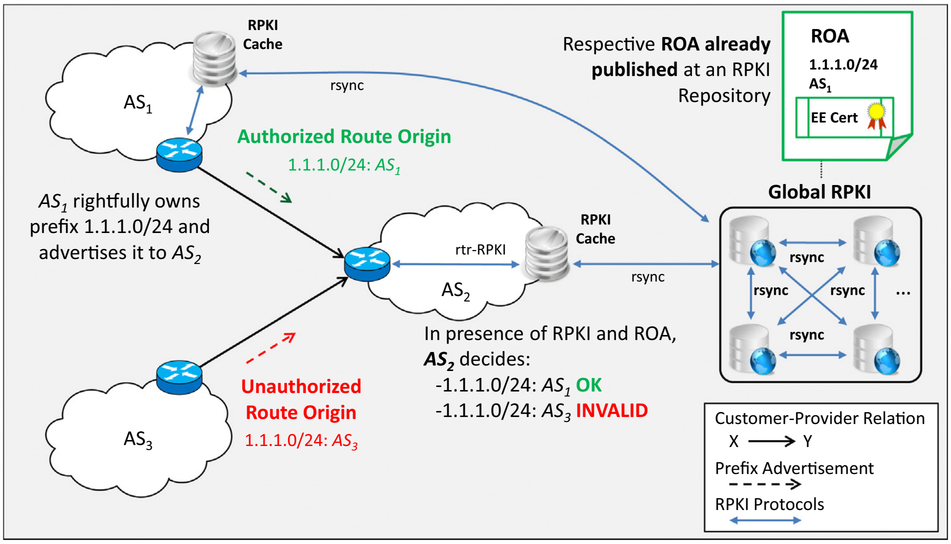


Fig. 6. Mitigating false IP-prefix origin advertisement using ROA.

routing (i.e., routing within the AS), implying that the BGPSEC protocol is to be practiced only on the edge routers—the eBGP routers—between different ASes. Fig. 7 illustrates the origination and propagation of a secure BGP update from AS_N to AS_{N+1} according to the BGPSEC protocol. In a nutshell, AS_N uses digital signatures to sign particular information (discussed later in the section) to secure the AS-Path information. The inclusion of the next-hop AS number in the signature (AS_{N+1} in this case), not only enables backward traceability all the way to the origin of the route, but also secures the forward direction of the update, hence the process shown in Fig. 7 is known as "Forward Signing".

After negotiating the BGPSEC capability and related security credentials with a BGP peer, a BGP speaker can originate a secure IP-prefix advertisement, i.e., a BGPSEC update, toward it. The BGPSEC router certificates along with a pair of cryptographic keys allow a BGP speaker, now called a BGPSEC speaker, to sign BGP updates on behalf of its AS. It is worth mentioning that the corresponding ROA of the IP prefix to be advertised must have already been published in the RPKI, as it is necessary for successful validation of a BGPSEC update. The BGPSEC speaker originating the update constructs the Signature-Segment by signing over a Secure_Path segment, the target ASN and the NLRI. The Secure_Path segment contains own ASN, a pCount field and Flags. The pCount field is the prepend count referring to the number of repetitions of the associated ASN that the signature covers. Note that the pCount field enables a secure and optimized way of performing AS-Path prepending. A BGPSEC update message does not contain an *AS_Path* attribute—but instead it has an *BGPSEC_Path* attribute consisting of a *Secure_Path*, which encloses one Secure_Path segment from each AS in the path. The *Secure_Path* enables backward compatibility with BGP-4, and assists in converting the *BGPSEC_Path* attribute into a BGP-4 *AS_Path* attribute whenever necessary.

When a BGPSEC speaker receives a BGPSEC update, it verifies the update using a validation procedure [89]. For validation of a received BGPSEC update, a BGPSEC speaker relies on the ROA and the RPKI. The SIDR's recommendations leave it to the discretion of ASes for interpreting the outcome of the BGPSEC update validation process according to their internal policies. This implies that ASes have the freedom to prioritize a BGP-4 update over a valid BGPSEC update for a particular IP prefix, or vice versa to satisfy their internal policies. Moreover, a BGPSEC speaker can further propagate a received BGPSEC update either as a BGPSEC update or a BGP-4 update. These flexibilities facilitate partial deployment scenarios. Now, to propagate as a BGPSEC update, the intermediate BGPSEC speaker creates a new BGPSEC update for the same IP prefix. The *BGPSEC_Path* attribute of the new update includes the received Signature-Segments along with the new Signature-Segment of the BGPSEC-speaker creating the update, prepended in front. The signature field of the new Signature-Segment consists of the Target AS Number, the Secure_Path segment, the Flags and the received signature fields. Fig. 7 details the propagation of a BGPSEC update for an intermediate BGPSEC speaker AS_{N+1} toward AS_{N+2}. Hence, signing of certain portion of the BGP update enables the receiving party to verify the claimed information with the help of the ROA and RPKI.

4.3.1. *Practical considerations of BGPSEC*

The introduction of changes in the structural and operational aspects of BGP make the BGPSEC proposal prone to rejection. The structural changes are due to the need of new optional attributes, while the operational ones take into consideration ROA validations and the signature verifications. However, SIDR's contributions have given explicit considerations to practical aspects of BGPSEC, such as making it backward compatible with the BGP-4 protocol. In this paper, we only highlight a couple of practical

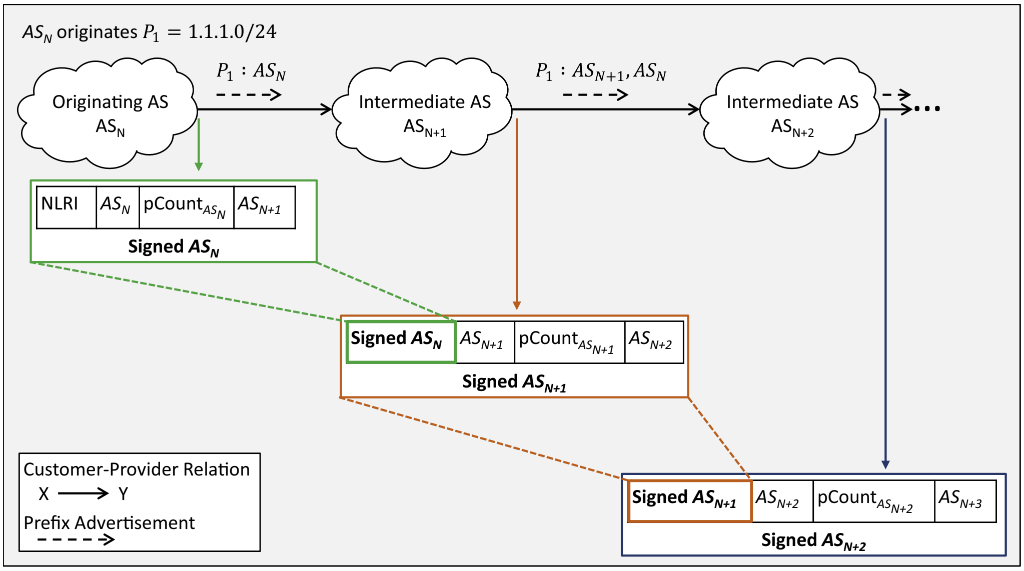

AS_N originates $P_1 = 1.1.1.0/24$
$P_1 : AS_N$
$P_1 : AS_{N+1}, AS_N$
Originating AS AS_N
Intermediate AS AS_{N+1}
Intermediate AS AS_{N+2}
NLRI | AS_N | $pCount_{AS_N}$ | AS_{N+1}
Signed AS_N
Signed AS_N | AS_{N+1} | $pCount_{AS_{N+1}}$ | AS_{N+2}
Signed AS_{N+1}
Signed AS_{N+1} | AS_{N+2} | $pCount_{AS_{N+2}}$ | AS_{N+3}
Signed AS_{N+2}
Customer-Provider Relation
X → Y
Prefix Advertisement

Fig. 7. BGPSEC origination and propagation with "Forward Signing".

considerations made by SIDR's contributions, so interested readers are referred to [107,108] for further information.

IXP Route Server Transparency: An Internet Exchange Point (IXP) is the place where different ISPs interconnect with each other. The Route Servers (RS) at the IXP provide an easy and efficient way of peering with multiple ASes. Usually, there are two ways an IXP can propagate routes:

- Direct Bilateral (DB) peering through the IXP.
- Multi-Lateral (ML) peering between clients via a route server at the IXP.

On one hand, the DB peering enables more control over the selection of specific networks to peer with, by allowing to directly establish BGP sessions with the other network at the IXP, but it requires more effort and configuration to peer with all the IXP members separately. On the other hand, the ML peering eases the configuration by just establishing a single BGP session with a route server at the IXP, which is connected to all the other networks, but at the cost of limited control over selection of networks to peer with.

The IXP-RS are said to be "transparent" if they do not include their own ASN in the *AS_PATH* attribute while peering between the clients. The DB peering works unaffectedly with BGPSEC, but ML peering cannot remain completely transparent, as the sender requires the destination ASN in order to forward sign the update. This either requires the client to know in advance the ASN of all the other clients to whom it wants to peer with, or forward sign it toward the IXP-RS ASN and then the IXP-RS forward signs it further to other clients. In the latter case, an IXP-RS can partially remain transparent by putting a '0' in the pCount field when it signs. This way, IXP route servers will show up in the AS-Path but will not contribute to increasing the AS-Path length, as it is computed by summing up the pCounts in BGPSEC. In a way, BGPSEC makes the IXP route servers semi-transparent.

Partial Deployment Scenarios: The BGPSEC protocol explicitly tackles partial deployment scenarios and this may be one of the main reasons why the SIDR's proposals have a chance of adoption into the real world. Partial deployment refers to the scenario where the Internet consists of interconnected islands of BGPSEC and BGP-4 ASes. The BGPSEC protocol does not allow partial AS-Path information protection, therefore BGPSEC cannot be tunneled through non-BGPSEC (BGP-4) ASes. Thus, when an update goes from a BGPSEC enabled AS to a non-BGPSEC AS, the signatures of the BGPSEC update have to be stripped off, and the BGP-4 *AS_Path* attribute has to be constructed using the Secure_Path information available in the *BGPSEC_Path attribute*, since the BGPSEC protocol is backward compatible with the BGP-4 protocol. Once a BGPSEC update gets converted into a BGP-4 update, it cannot be reversed back into a BGPSEC update, even if it enters again a BGPSEC enabled AS. This is an important compromise which makes the BGPSEC protocol impotent in the presence of BGP-4 islands, though it is crucial to accommodate partial deployments.

On the boundary of a BGPSEC island, the *Secure_Path* is converted into a BGP-4 *AS_Path* attribute. Any prepended ASN, that was collapsed in BGPSEC, will be repeated pCount number of times and any transparent route server, with pCount equal to zero, will be removed from the BGP-4 *AS_Path* attribute. Fig. 8 illustrates different scenarios that may occur in the life of a BGPSEC update and BGP-4 update in case of partial deployment of the BGPSEC protocol.

In addition, SIDR's recommendations also allow two BGPSEC enabled ASes to negotiate an asymmetric BGPSEC communication, called simplex BGPSEC. In simplex BGPSEC, a stub AS sends BGPSEC updates and receives BGP-4 updates from its provider through a mutual trust agreement. This lifts up the burden of BGPSEC update validation

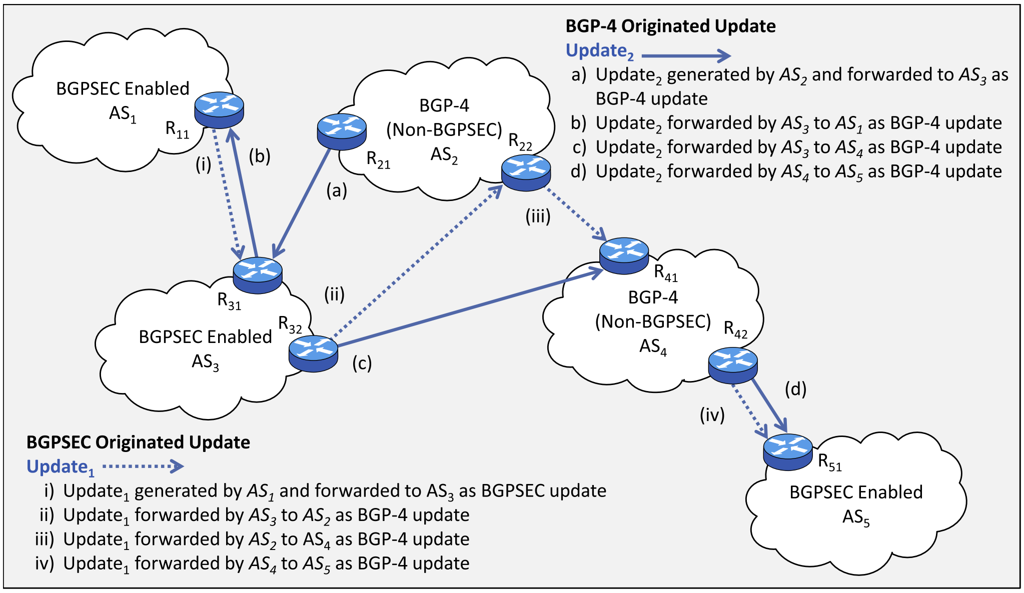

BGP-4 Originated Update
Update$_2$
a) Update$_2$ generated by AS_2 and forwarded to AS_3 as BGP-4 update
b) Update$_2$ forwarded by AS_3 to AS_1 as BGP-4 update
c) Update$_2$ forwarded by AS_3 to AS_4 as BGP-4 update
d) Update$_2$ forwarded by AS_4 to AS_5 as BGP-4 update
BGPSEC Enabled AS$_1$
R$_{11}$
(i)
(b)
BGP-4 (Non-BGPSEC) AS$_2$
R$_{21}$
R$_{22}$
(a)
(iii)
R$_{31}$
BGPSEC Enabled AS$_3$
R$_{32}$
(ii)
(c)
R$_{41}$
BGP-4 (Non-BGPSEC) AS$_4$
R$_{42}$
(d)
(iv)
R$_{51}$
BGPSEC Enabled AS$_5$
BGPSEC Originated Update
Update$_1$
i) Update$_1$ generated by AS_1 and forwarded to AS$_3$ as BGPSEC update
ii) Update$_1$ forwarded by AS_3 to AS_2 as BGP-4 update
iii) Update$_1$ forwarded by AS_2 to AS$_4$ as BGP-4 update
iv) Update$_1$ forwarded by AS_4 to AS_5 as BGP-4 update

Fig. 8. BGPSEC updates in partial deployment scenarios.

from stub ASes, which constitute around 80% of the ASes in the Internet [109], encouraging early adoption for resource constrained stub ASes, as they would experience less pressure to upgrade hardware equipment.

5. SIDR proposals' impact on inter-domain routing

The SIDR proposals address both of their design goals with RPKI facilitating ROA and BGPSEC to provide a wider security blanket for inter-domain routing. However, RPKI, ROA and BGPSEC introduce extra burdens that must be taken into serious consideration. Indeed, SIDR's proposals require to fulfill certain characteristics to assure effective security, which are not only challenging but also represent huge barriers for wider acceptance. As a result, there is skepticism about SIDR's solutions and a considerable reluctance among the key actors that need to lead and push for a wide scale deployment.

In this section, we study the SIDR's proposals from three different perspectives, including, residual security issues, deployment obstacles, and adoption challenges. In the residual security issues, we examine the well-known BGP attacks in presence of SIDR's solutions and illustrate the ones that still persist. With respect to deployment obstacles, we investigate the impediments faced by the SIDR solutions in terms of practical real world implementation, i.e., we examine the estimated size and synchronization requirements of the global RPKI repository, as well as the adjunct issues of maintaining it scalable in a distributed manner. We also study the extra burdens that BGPSEC adds to the whole security solution as well as its impact on the router resources. Finally, we provide insight into different challenges and strategies currently being discussed to foster early adoption and gradual deployment, which aim at accelerating the acceptance of SIDR's solutions by the Internet community.

5.1. Post SIDR residual security issues

The security criteria for inter-domain routing considered by the SIDR WG included empowerment of ASes to mitigate false prefix origination and false AS-Path advertisement attacks. From this perspective, SIDR's solutions technically guarantee to achieve their target with the help of the proposed security infrastructure consisting of RPKI, ROA and BGPSEC. As described in Section 4.2, the availability of RPKI and valid ROAs assures mitigation of false route origination attacks completely. The false AS-Path advertisement attack is not feasible anymore with the use of BGPSEC updates due to the chained signatures and verifications, as explained in Section 4.3. The AS-Path shortening also fails in face of BGPSEC, as the pCount field is part of the signature, and altering the signature will result in the update being dropped during the validation process. Furthermore, the SIDR's solutions also fulfill the requirement of no policy disclosure and AS-Path integrity traceable back to the origin of the announcement. However, out of the three major problems described in Section 2, namely false AS-Path advertisement, false route origination and route leaks, the latter is not addressed by SIDR's solutions. Even though with an extensive security infrastructure, there are other BGP vulnerabilities, such as replay and coordinated attacks, that also remain unattended by the SIDR's proposals. Next, we describe the known residual attacks that remain unsolved by the SIDR's solutions, and provide related work of solutions that have been proposed to counter them.

Route Leaks:

As described in Section 2.4, route leaks are a routing security problem that occur when business policies are violated. Route leaks can occur even in the presence of RPKI, ROA and BGPSEC, because they secure the operations of BGP and not the business policies among the ASes,

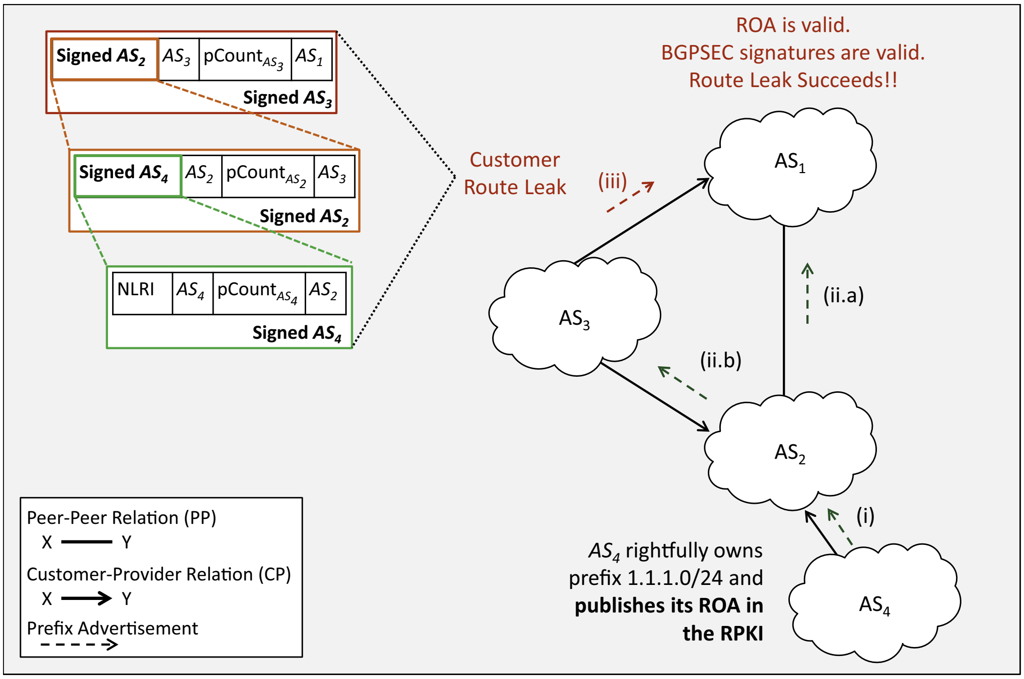

Signed AS2 | AS3 | pCountAS3 | AS1
Signed AS3
Signed AS4 | AS2 | pCountAS2 | AS3
Signed AS2
NLRI | AS4 | pCountAS4 | AS2
Signed AS4
ROA is valid.
BGPSEC signatures are valid.
Route Leak Succeeds!!
Customer Route Leak
(iii)
AS1
AS3
(ii.a)
(ii.b)
AS2
(i)
AS4
AS4 rightfully owns prefix 1.1.1.0/24 and publishes its ROA in the RPKI
Peer-Peer Relation (PP)
X Y
Customer-Provider Relation (CP)
X Y
Prefix Advertisement

Fig. 9. Route leak on a customer link in presence of RPKI, ROA and BGPSEC.

whereas route leak exploits the fact that customer routes are preferred over peer or provider routes, and peer routes are preferred over provider routes. Fig. 9 illustrates the customer route leak scenario described in Section 2.4 in the presence of the SIDR's solutions. It can be observed in the figure that even if AS_4 had published an ROA for the IP prefix 1.1.1.0/24 in the RPKI, and all the ASes in the scenario propagated BGPSEC updates, the route leak still succeeds if AS_3 advertises IP prefix 1.1.1.0/24 to AS_1. The ROA and BGPSEC update validation processes will output valid as they are legitimate (see Fig. 9). A route leak over a peer link will also succeed in a similar manner.

In [110], Goldberg et al. analyze how effective secure BGP solutions, including ROA and BGPSEC, are against a set of attack strategies—route leaks is one of the attack strategies studied. The study contends that the route leak problem is as damaging, in terms of attracting traffic, as the false AS-Path advertisement attacks. Furthermore, they conclude that the route leak problem remains unattended by the secure BGP solutions. Goldberg et al. suggest to use Prefix Filtering for countering route leaks. They show that the route leak attacks can be completely prevented with the use of appropriate prefix filtering techniques in stub ASes. However, it falls short in the case the attacker is not a Stub AS. Apart from this, other main problems with filters in large domains are the administrative overhead and the cost of maintaining them updated. The timely and accurate maintenance of route filters becomes challenging as the number of allowed prefixes increase up to thousands, due to the administrative burden. As a result, the ASes prefer to rely on trust and do not maintain up-to-date prefix filters—hence saving their high maintenance cost. The YouTube incident in 2008 [56], and the Google incident in 2012 [111], could have been avoided if the route filters at the providers were effective. Thus, we consider that prefix filters are a stopgap solution applicable in specific contexts for securing the inter domain system against route leaks.

As described in Section 3, securing AS policies is not among the design principles under consideration by SIDR WG for securing the inter-domain routing. For this reason, the SIDR WG did not attempt to address the route leak problem as it was considered out of their charter's scope. However, SIDR WG acknowledges route leak as a persisting routing security vulnerability [112]. SIDR WG has delegated the effort to address this vulnerability to the Global Routing Operations WG [113], and currently it is been studied [114].

Recently an idea of using Route Leak Protection (RLP) field inside the BGPSEC signatures to counter route leak problem is under discussion in the GROW WG [115]. The RLP field consists of two bits whose value is set by the AS sending the BGPSEC update to indicate the receiving AS if it is allowed to advertise the routes included in the update to its providers or peers. If the RLP field is set to 00 then the receiving AS can forward the update to its providers or peers and if it is set to 01 then the receiving AS is not allowed to forward the update to its providers or peers. Now, if an AS receives a update from its customer AS such that it observes 01 in the RLP field while unwinding and verifying the signature segments of all the ASes in the AS-Path, then it can consider this update as a route leak. Let us explain the RLP working using the topology in Fig. 9. According to solution, AS_4 will put 00 while advertising its IP prefix 1.1.1.0/24 toward its provider AS_2, i.e., it allows AS_2 to further advertise the IP prefix. Now, in step (ii.b), AS_2 puts 01 while advertising the IP prefix to AS_3, i.e., disallowing AS_3 to advertise the update to its providers and peers. Now, if AS_3 leaks the route to AS_1, then AS_1 can establish it as a route leak as it will observe a 01 in the signature segment added by AS_2. The RLP solution works well for mitigating route leaks, however it suffers from two main adjunct problems. Firstly, the RLP solution will only be effective if everyone is playing BGPSEC. During the partial deployment tenure, the RLP solution can be deceived legitimately as BGPSEC allows BGPSEC functionality downgrade (more on this later in the section). Secondly and most importantly, the RLP solution reveals AS policies more than what BGP already does. This is because in the RLP solution, an AS has to explicitly indicate and sign if the next hop is allowed or not allowed to further advertise a particular route. The former problem puts a question mark on the robustness of the RLP solution for mitigating route leaks, however it will be more difficult to convince the industrial players for the latter one, that is to earn relaxation on the confidentiality of the AS policies.

Sundaresan et al. [116] proposed a similar strategy for countering route leaks by setting a one bit flag in the BGP advertisement when it is sent to a peer AS or a customer AS. In essence, to detect export policy violations they exploit the valley-free path feature that a particular BGP update once traversed through a provider–customer link or a peer-peer link should not go over a customer–provider link or another peer-peer link, respectively. The shortcomings of this scheme are similar to the ones of the RLP technique mentioned above, including disclosure of more AS policies and relationships information as compared to the BGP. The RLP scheme [115] has an edge over Sundaresan et al. [116] in the sense that it utilize two bits. The unused bit codes, 10 and 11, can be consumed to accommodate complex AS relationship scenarios as well for detecting route leaks.

In [98], the author attempts to provide a detection scheme for route leaks using colors along the AS-Path. The scheme suggests to color each AS-hop in the AS-Path according to the corresponding link type, i.e., an AS-hop has color "Green" if toward a provider and has color "Yellow" if toward a peer or customer. In other words, a route received from a customer must have all AS-hops marked "Green" or otherwise it is a route leak. Likewise, a route received from a peer must have all AS-hops marked "Green" except the last AS-hop marked "Yellow" or else its a route leak. In [117], the author contends that such a coloring scheme can be employed in conjunction with BGPSEC by having a signature block similar to the AS-Path signature block. This mode of implementation adds extra burden of signing and verifying the color signature block on the already resource demanding BGPSEC implementation.

Replay Attacks:

Replay attacks refer to malicious re-advertisement of withdrawn routes through BGPSEC updates. That is, a withdrawn route is replayed exploiting the fact that the associated certificates are still valid. In the worst case, the replay attack remains feasible until the expiry time associated with the EE certificate of the router that originated the route advertisement in the first place. The replay attack window, i.e., the time interval during which a withdrawn route can be re-advertised, can possibly be on the order of several days depending on the validity of EE certificate of the originating AS router. According to the BGPSEC protocol, the withdrawals are not signed, as it assumes transport security between any two neighboring BGPSEC routers, which will mitigate injection of false withdrawals or replaying of stale withdrawals by an alien entity. However, this assumption fails to stop the re-advertisement of withdrawn routes by neighbor ASes within the expiration time window of the EE certificates.

One proposed way to mitigate replay attacks is by explicitly limiting the life of a route advertisement with an expiry time field inside a BGPSEC update [118]. The route originating AS includes the expire time field in its signature, whereas the ASes along the AS-Path need not to include expire time fields in their respective signatures. This solution requires a regular beaconing mechanism for refreshing the routes, i.e., the originating AS re-originates the route with new expire time to extend the life of the route propagated earlier. The duration of the time interval for the re-origination of a route is an important parameter, since large time intervals will cause less BGPSEC churn, but will lead to large replay attack windows; whereas short time intervals will minimize the replay attack windows, but at the cost of more BGPSEC chattiness. Another proposed mechanism that can be used to counter replay attacks is the BGPSEC router key rollover [119]. It describes the process of replacing a router's key pairs along with a new EE certificate, hence renewing the life span of a route advertised through a BGPSEC update. It does not suffer from beaconing burden; however, it adds administrative burden of frequent rollovers in order to have a reduced replay attack window. As BGPSEC is an ongoing effort, there is no concrete indication at the moment about which mechanism will be used to provide protection against replay attacks.

Route Withdrawal Starvation:

Route withdrawal starvation refers to the scenario when an AS suppresses a withdrawal update, i.e., it does not forward the withdrawal update to other ASes, to whom it had advertised this route or set of routes earlier. If the malicious AS keeps forwarding the traffic on the old route, then the traffic could be dropped further up the path and hence detected by ASes which were deprived of the withdrawal information. On the other hand, if the malicious AS forwards the traffic toward the destination through some other path, then this may not only result in suboptimal routing but traffic hijacking as well. In the latter case, the malicious AS would be able to sniff all the traffic undetected. The SIDR WG recognizes the route withdrawal starvation attack in its threat model [112] and consider it a residual vulnerability as it remains feasible in the presence of BGPSEC and ROA. According to the BGPSEC protocol, the withdrawals are not signed but for the sake of argument even if the withdrawals were signed, route withdrawal starvation is still feasible as it occurs due to the withholding of withdrawal information rather than exploiting the semantics or operations of BGP.

Moreover, the transport security assumption between two neighboring BGPSEC routers works fine for shielding

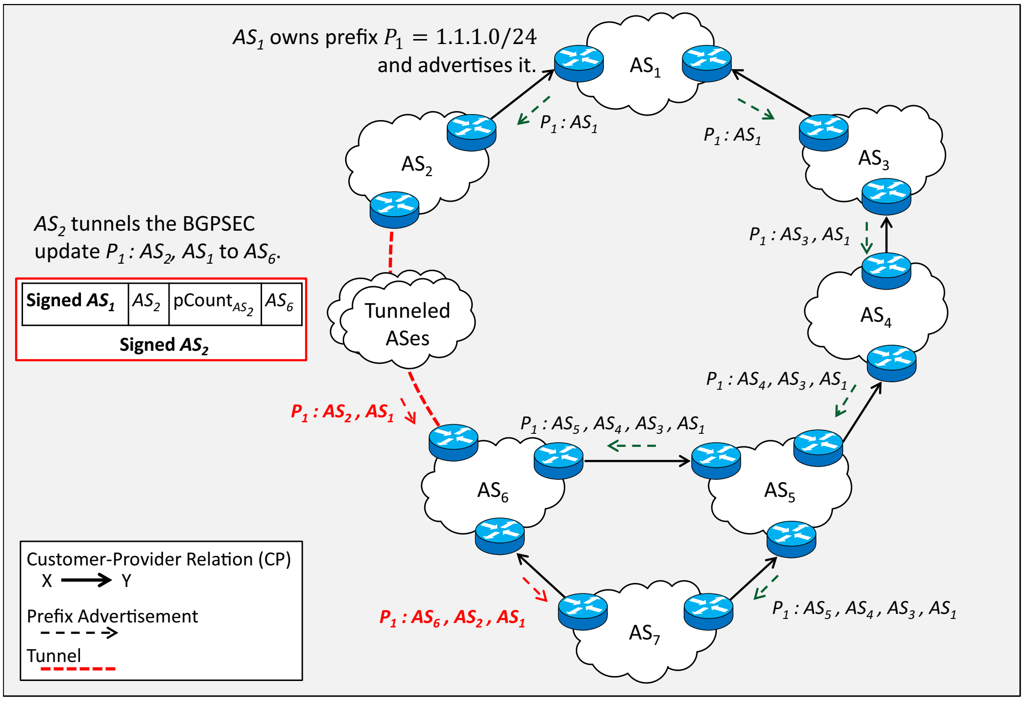

AS_1 owns prefix P_1 = 1.1.1.0/24 and advertises it.
AS_1
$P_1 : AS_1$
$P_1 : AS_1$
AS_2
AS_3
AS_2 tunnels the BGPSEC update $P_1 : AS_2, AS_1$ to AS_6.
$P_1 : AS_3 , AS_1$
Signed AS_1
AS_2
pCount$_{AS_2}$
AS_6
Signed AS_2
Tunneled ASes
AS_4
$P_1 : AS_4, AS_3 , AS_1$
$P_1 : AS_2 , AS_1$
$P_1 : AS_5 , AS_4 , AS_3 , AS_1$
AS_6
AS_5
Customer-Provider Relation (CP)
X → Y
Prefix Advertisement
Tunnel
$P_1 : AS_6 , AS_2 , AS_1$
AS_7
$P_1 : AS_5 , AS_4 , AS_3 , AS_1$

Fig. 10. Co-ordinated false AS-Path attack on BGPSEC.

off external false withdrawal injections, but does not counter the potential suppression of withdrawal updates by a neighbor AS. The main difference between route withdrawal starvation and replay attacks is that in the latter case an AS re-advertises routes that it withdrew earlier—hence exploiting the fact that the certificate associated with a route is still valid—whereas in the former case, an AS suppresses the propagation of withdrawal information. The mitigation of route withdrawal starvation is similar to replay attacks, i.e., either limiting the life time of an advertisement or router key rollover mechanisms can be used to counter it.

Co-ordinated False AS-Path Attack:

The BGPSEC protocol secures AS-Path information in BGP updates with the use of chained signatures and verifications, but it still falls short of countering coordinated attacks on the AS-Path information. Fig. 10 illustrates a naive example where two ASes, AS_2 and AS_6, collude to propagate false AS-Path, even when BGPSEC is deployed, which can result in traffic hijacking. In this example, we assume that all the ASes employ BGPSEC, as described in Section 4.3. As shown in Fig. 10, AS_1 advertises its IP prefix P_1 to its customers, AS_2 and AS_3. According to BGPSEC, AS_1 inserts AS_2 in the target ASN field for the BGPSEC update toward AS_2, and places AS_3 in the target ASN field for the BGPSEC update toward AS_3. AS_3 does the same for AS_4 and so forth, such that the IP prefix advertisement of P_1 received by AS_7 from AS_5 contains the AS-Path AS_5–AS_4–AS_3–AS_1. If AS_2 creates a BGPSEC update for IP prefix P_1 by inserting AS_6 in the target ASN field, and then tunnels this update directly to AS_6, then it technically enables AS_6 to advertise P_1 toward AS_7 through AS_2. The BGPSEC update from AS_6 to AS_7 containing the forged AS-Path AS_6–AS_2–AS_1 will pass all the validation checks proposed by SIDR, including ROA validation and the verification of BGPSEC signatures along the AS-Path. Now, AS_7 has two routes for P_1, and by virtue of the shortest AS-Path preference, it will opt for the route through AS_6. AS_6 can either black-hole the traffic or undetectably sniff the traffic while sub-optimally routing it toward AS_1 through AS_5.

Li et al. [120] throughly analyze a more rigid coordinated false AS-Path attack where even the data-plane traffic is tunneled between the colluding ASes before reaching its destination. The study also presents a solution to counter this attack by building collaborations with potential intermediate tunneled ASes and victims. Therein, this attack is referred as "TIGER", and the anti-TIGER solution to counter it is based on the observation that the attack leverages a tunnel to generate fake links, hence, there must exist at least one node in between the fake link that can facilitate in detecting the attack on the observance of suspicious tunneled traffic. To achieve this, the solution requires (i) building a neighbor AS graph (x-NAG) for each AS by assembling routing updates received from its peers (x is the diameter of the NAG) and (ii) a three-way detection protocol consisting of covert challenge and response exchanges between the intermediate and the victim ASes. In summary, an orchestrated collaborative effort between victim and intermediate ASes is required to mitigate the coordinated false AS-Path attack. This example clearly highlights the existence of security holes that can be exploited even after the deployment and adoption of RPKI, ROA and BGPSEC.

RFD and MRAI Attacks:

Song et al. [90] highlight two BGP protocol manipulation attacks that remain feasible in the presence of SIDR solutions. The Route Flap Damping (RFD) and Minimum Route Advertisement Interval (MRAI) attacks misuse the mechanisms that BGP employs to maintain route stability and to assure convergence, respectively. The RFD mechanism measures instabilities of routes, based on how frequently they are advertised and withdrawn, and blocks a route when it is unstable beyond a certain cut-off threshold. Hence, an on-the-path malicious AS can cause a victim AS to block a certain route to a destination by frequently advertising and withdrawing it. The MRAI timer puts a limit on how frequent route advertisements and withdrawals can be send to a neighbor AS. By exploiting the application of MRAI on the withdrawal sent to a neighbor, an on-the-path malicious AS can intelligently sequence advertisements and withdrawals of a route toward a victim AS such that the destination remains unreachable for the victim AS [90]. The SIDR proposals do not mitigate RFD and MRAI attacks as they are intrinsic to BGP stability and convergence mechanism but question the motives of such attacks, as the malicious AS will cause loss of revenue for itself and unreachability to a certain destination for the victim AS. In order to avoid RFD attacks, Song et al. propose to adopt RFD penalty in the presence of a special cryptographically verifiable message inside the update which indicates that it is in fact a result of a genuine link failure. Furthermore, the study recommends to confine the use of MRAI timers only for route advertisements to prevent MRAI attacks.

BGPSEC Functionality Downgrade:

The BGPSEC functionality downgrade attack refers to the scenario where a BGPSEC-enabled AS deliberately downgrades itself to BGP-4 to avoid signatures and verifications, in order to launch an attack. The SIDR threat model [112] considers BGPSEC functionality downgrade as a possible attack. This attack succeeds by exploiting the very flexibility in SIDR's recommendations that allows a BGPSEC speaker to peer with a BGP-4 speaker for tackling partial deployment scenarios [121] (see Section 4.3.1). Lychev et al. [122] detail the feasibility of this attack in presence of secure BGP solutions. The downgrade to BGP-4 is a possibility due to the requirement of partial deployment scenarios, and learning from the experience of IPv6 deployments and its adoption, the partial deployment scenarios for BGPSEC will be a reality for a long period of time.

For example, let us consider the false AS-Path attack described in Section 2.2 in the context of a BGPSEC downgrade scenario (see Fig. 2). If we assume that the ASes along the legitimate BGP update path AS_3–AS_4–AS_5 use the BGPSEC protocol and AS_1 deliberately downgrades itself to BGP-4, then AS_2 receives both a valid BGPSEC update and a BGP-4 update (the latter with a false AS-Path). In this scenario, the fate of the attack launched by AS_1 will depend on the internal policy of AS_2, i.e, whether valid BGPSEC updates are preferred over unverifiable BGP-4 updates. However, the attack will succeed either AS_2 treats them equally, or a shortest path over a valid BGPSEC update is preferred. The assumption of a BGPSEC speaker preferring a shortest path coming from an unverifiable BGP-4 update over a valid BGPSEC update is indeed rational, since a recent survey [95] among large ISPs shows that 40% of the respondents indicated that they will place the BGPSEC update information below the shortest path tie breaker in the BGP route selection algorithm (Section 9 in [1]). The results presented in this survey clearly put a question mark on the effectiveness of BGPSEC even if it is adopted (cf. Section 5.3).

Deviant RPKI Authorities Attack:

The deviant RPKI authorities attack arises when the trust among the RPKI authorities is violated. The abnormal behavior of RPKI authorities can be due to misconfiguration, malfunctioning of equipment or on the request of official authorities. A deviant RPKI authority can revoke a set of resource certificates under its administration causing several legitimate ROAs and AS-Paths to become invalid. Cooper et al. [123] argue that RPKI authorities enjoy unchecked power to revoke or overwrite resource certificates and ROAs, hence making it difficult to distinguish between abusive and normal revocations. They also highlight that in case of cross-country certifications, a deviant RPKI authority can avoid any legal repercussions if it targets resource certificates and ROAs outside its legal jurisdiction. Heilman et al. [124] also provide a threat model for misbehaving RPKI authorities and suggests mechanisms to enhance the transparency of the RPKI for countering the possible attacks. They recommend to modify the current RPKI in order to include consent, using signed objects, from all affected parties to counter illegitimate revocations of certificates or ROAs. The study also proposes a detection strategy for consent-less revocations but does not provide any concrete post-alarm mechanisms to resolve the resulting dispute. Such grave drawbacks and their respective consequences due to compromised RPKI authority are few of the many open issues faced by SIDR's solutions in the practical world.

5.2. Deployment obstacles faced by SIDR's proposals

In this section, we examine the viability of SIDR's solutions by looking into how the academic and industrial communities have perceived them. In particular, we survey the practical and theoretical studies related to the workability of RPKI/ROA and BGPSEC, and highlight the disagreements and challenges for their realization in the real world. Particularly, for each solution we focus in researching different key features that may produce acceptance or resistance. First, we dive into the distributed repository infrastructure RPKI, alongside with ROA, by researching different estimations regarding the total size of the global repository and the synchronization delays among the distributed RPKI repositories as key gauging metrics for its successful deployment. Next, we investigate the overhead incurred by BGPSEC in terms of processing and memory requirements along with the changes required in the BGP protocol.

5.2.1. Deployment challenges of the RPKI security infrastructure

As explained in Sections 4.1 and 4.2, the RPKI framework provides a cryptographic hierarchy of authorities that allocate and sub-allocate Internet Number Resources (e.g., AS numbers or IP prefixes) as well as stores digitally signed authorization objects, i.e., ROAs. A distributed set of repositories are part of a global RPKI repository, thus, in our discussion we address the following two important interconnected concerns:

- Estimation of the total number of security objects, such as certificates and ROAs, that are going to be published and stored in the distributed repositories.
- Estimation of the synchronization delays of security objects in terms of the global RPKI repository.

Estimation of the Global RPKI Size:

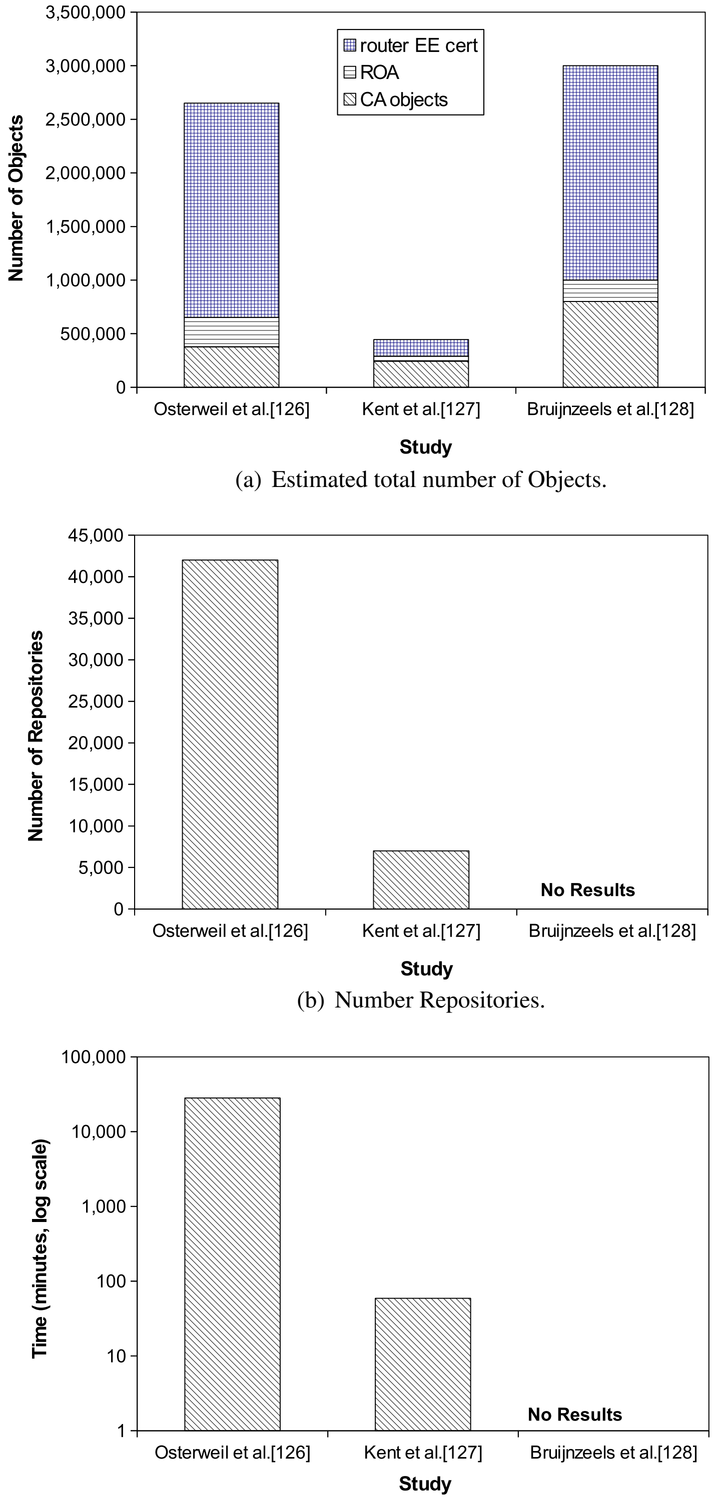
The estimation of the global RPKI size is a relevant exercise as it impacts the time required for synchronizing the distributed RPKI repositories. Osterweil et al. [125], Kent et al. [126], and Bruijnzeels et al. [127] evaluate the RPKI's scalability by estimating the global RPKI size, and the synchronization delays associated with the distributed repository system. Whilst these studies consider a global deployment of RPKI, ROA and BGPSEC for their estimations, it is important to remark that the different metrics required for the evaluations, such as the total number of RPKI repositories, router EE certificates and ROAs vary largely among them. There is no general consensus or similar approximations about the total expected size and complexity of the global RPKI, which leads to drastically diverse analyses regarding the scalability and functional requirements of RPKI.

According to Osterweil et al. [125], the estimated number of objects in the global RPKI is 650,796 excluding the BGPSEC EE router certificates, i.e., considering only RPKI and ROA deployments. The estimation increases up to 2,650,836 in the case of complete BGPSEC deployment. These results are based on the assumptions presented in Table 2. There are three important remarks about this study: (i) The number of repositories in the ideal case would be equal to the number of CA, however it is not clear whether each CA will administrate its own repository, or for example in the case of Stub-ASes it can be outsourced; (ii) The estimated number of ROAs considers more than one prefix per object and excludes the multi-homing scenarios; and (iii) the total number of BGPSEC router certificates are estimated to be 2,000,000 based on the rough estimation that there are around 1 million eBGP routers in the Internet [128], and a pair of BGPSEC router certificates per eBGP router is considered. The reason behind two BGPSEC router certificates, either per eBGP router or per AS, is to provide the next BGPSEC router certificate along with the current one, in case it gets revoked, expired or compromised, to save up on the BGPSEC router certificate replacement delays. In contrast, Kent et al. [126] estimates the total number of objects in the global RPKI to be 444,645 including the BGPSEC router EE certificates, and 289,501 excluding them. Their estimations (see Table 2) make two crucial assumptions in their analysis; first, that the stub ASes—which constitute 80% of the Internet—outsource their RPKI repository chores; and second, that all the edge routers (i.e., eBGP routers) of an AS will use only one pair of BGPSEC router certificates per AS for signing. These assumptions drastically reduce the total number of objects in the global RPKI as compared to the estimations provided by Osterweil et al. [125]. The third study, Bruijnzeels et al. [127] estimates the total size of a global RPKI, with ROA and BGPSEC deployed, to be around 3 million (see Table 2). Apart from considering a CA per AS, this study includes separate CAs and related security objects for Provider Independent resources as well. Furthermore, they assume the total number of ROA objects are dependent on the number of routes in the BGP FIBs in the Default-Free Zone, and with an aggregation factor of 3, i.e., 3 prefixes per ROA. This study estimates the total number of required BGPSEC router certificates to be around 2 million with the same line of reasoning as Osterweil et al. [125]. We can observe that Bruijnzeels et al. [127] and Osterweil et al. [125] provide relatively similar estimations regarding the total number of objects in the global RPKI, but there is a considerable difference with the estimations of Kent et al. [126] (see Fig. 11(a) and (b)), given that they are based on different hypotheses.

Table 2
Assumptions of the different studies for estimating total number of objects in the RPKI.

	Osterweil et al. [125]	Kent et al. [126]	Bruijnzeels et al. [127]
Number of RIRs	5	5	–
Number of ASes	42,000	43,000	40,000
Number of ROAs	273,592	47,305	200,000
Number of router EE certificates	2,000,000	155,144	2,000,000
Number of repositories	42,000	7000	–

Discussion: The discrepancies in identifying the total size of the global RPKI found in these studies reflect that the different actors working on the solutions have different opinions and expectancies about a global deployment of the RPKI. The first discrepancy we observe is in the assumption of total number of repositories (See Table 2). Kent et al. [126] are pragmatic in assuming that the stub ASes will outsource their publication points, however the adverse impact of deviant RPKI authorities, as described in [123,124], may encourage ASes to do otherwise. Besides, we also observe a conundrum about the total number of BGPSEC router certificates required in a complete BGPSEC deployment. Osterweil et al. [125] and Bruijnzeels et al. [127] prefer to assume that each BGPSEC router will at least have two BGPSEC router certificates, whereas Kent et al. [126] considers only two BGPSEC router certificates per AS, i.e., these two BGPSEC router certificates will be shared among all the AS's eBGP routers. However, sharing a pair of certificates among several routers of an AS adds extra burden of secure distribution of these certificates among those routers. Furthermore, if a shared BGPSEC router certificate gets compromised, then all the AS's routers sharing this certificate become vulnerable to attacks, and the BGPSEC router certificate of each of these routers needs to be replaced. On the other hand, in the case of a pair of BGPSEC router certificates per eBGP router, a compromised BGPSEC router certificate will affect one particular router only. In our opinion, considering only a pair of BGPSEC router certificates for all the routers of an AS is an over simplification on part of Kent et al. [126]. On the other hand, considering a pair of BGPSEC router certificates per router



(a) Estimated total number of Objects.

(b) Number Repositories.

(c) Total Sync Time for a global RPKI.

Fig. 11. Estimated RPKI overhead per study.

acutely increases the total number of security objects in the global RPKI. Approximately 3 million objects in the worst case might be considered to be a large lower-bound estimation. However, it will surely grow whenever any keys are rolled over and changed. Besides, the daily churn, i.e., the amount of new objects that are expected to be created within a period of time, like every day, is another factor to consider.

Estimation of Synchronization Time among RPKI Repositories:

Another important metric that has raised concerns is the synchronization time required to sync a new local cache with every Relying Party (RP) cache in the global RPKI repository. The studies Osterweil et al. [125] and Kent et al. [126] contemplate and evaluate the time required for a local cache to actually gather all the objects from a fully deployed global RPKI. The logic behind their calculations is first to compute an average time to gather an object from the repositories, then multiply it by the total number of objects. On the contrary, the Bruijnzeels et al. [127] study does not evaluate the synchronization time. Table 3 summarizes the assumptions made by the studies for estimating total synchronization time for a global RPKI.

The average time to gather an object considered by Osterweil et al. [125] is 628 ms/object. It was derived from 10 different RPKI repositories performance graphs. Therefore, the estimated time to gather all objects locally, considering 42,000 repositories, is 5.04 days excluding BGPSEC router certificates, and 19.57 days including them. They conclude that this total synchronization time provides a lower bound on the estimation of the total time required to populate and synchronize a global RPKI, as the number of security objects will increase whenever certificates are revoked, or the amount of objects will double during cryptographic algorithm rollovers. Moreover, this lower bound does not take into consideration the network-latency factor.

On the other hand, Kent et al. [126] estimate the total time to synchronize to be around 60 min, considering 7,000 repositories with an average time to gather a single object of 20 ms (see Fig. 11(c)). The average time per object is taken from private measurements data based on the traces of a RIPE repository. The total synchronization time for a global RPKI is an important factor that directly affects the scalability of a fully deployed RPKI. We observe another discrepancy between the two studies about the estimated time required for synchronization. The measurement of Kent et al. [126] is many fold lower than the one estimated in Osterweil et al. [125].

Discussion: The average synchronization time obtained in these studies presents a considerable variation ranging from tens of minutes to days. This discrepancy shows again that their assumptions and estimations of the total size, and the total synchronization time for a global RPKI are far apart, envisioning two extreme possible outcomes if a fully RPKI deployment is achieved. Besides, in the worst case scenario, we foresee a serious security threat not only due to large time-windows for replay attacks but also due to the wrong validations that would occur because of stale security data. The latter stems from the total time (in order of days) to synchronize the global RPKI, which jeopardizes the security and consistency of the whole system. Furthermore, we have to keep in mind that the publication and propagation time of an object in the global repository system is an important aspect that will affect the feasibility of the solution. For example, fast global visibility of a published ROA object would be required by all the RPs in order to be able to validate a BGPSEC route. Osterweil et al. [125] recommends that if a deadline for global synchronization is considered, the object synchronization rates must become faster as the repositories grow. However, Kent et al. [126] project global synchronization time to be in the range of tens of minutes only.

The estimations, evaluations and assumptions presented in Osterweil et al. [125], Kent et al. [126] and Bruijnzeels et al. [127], regarding the security and scalability of the global RPKI provide significant insight about the divergence of views. They question the feasibility and the potential deployment of a global security infrastructure. Observe that, even though in our discussion we only covered the estimation of a few important parameters of the global RPKI, mainly total size and synchronization time, the discrepancies highlighted above represent a large difference of opinion among some of the major players in this arena. We believe that further in-depth evaluations and measurements of the proposed RPKI are crucial to remove the mentioned discordances, in order to pave the way for its deployment.

Table 3
Assumptions of the different studies for estimating total synchronization time for a global RPKI repository. *Note:* Bruijnzeels et al. [127] do not provide an estimate in this regard.

	Osterweil et al. [125]	Kent et al. [126]
Avg second/object	0.628	0.2
Number of objects	2,650,836	445,000
Number of repositories	42,000	7000
Time to gather (s)	1,691,101	3600
Time to gather (days)	19.57293	1/24

5.2.2. Deployment challenges of BGPSEC

As described in Section 4.3, the solution proposed for securing route propagation in inter-domain routing, BGPSEC, is based on a forward signing mechanism. This solution fulfills the minimum security requirements for securing BGP announcements, however it introduces extra burdens which can be broadly classified as hardware and software challenges. The former affects directly the network hardware (e.g., the routers), and includes (1): the processing load due to the generation of signatures and their verifications; and (2) the increment on router's RIB memory in order to accommodate the BGPSEC advertisements. It is important to remark that the BGPSEC route updates are per-prefix, which amplifies these burdens. On the other hand, in terms of the software burden, BGPSEC requires changes on the current BGP protocol, which can be considered as a huge barrier in light of global acceptance. Hereafter, we present an extended discussion on the analysis of these burdens and their possible consequences over the solution's feasibility.

Estimation of Processor Load (hardware requirement):

An initial estimation of the impact of BGPSEC over the processing resources in a router is presented by Sriram et al. [109]. The study employs an 64bit ×86 Sandy Bridge Intel i7 3400 MHz processor, which requires 2530 ops/s for signing and 2215 ops/s for verifying for an ECDSA-P256 signature algorithm—a benchmark of the ECDSA-P256 algorithm over the machine was used to obtain these values. The CPU cost estimation model assumes a peer session reset for a large ISP BGPSEC router with a neighbor BGPSEC router—having a customer cone of around 32,000 routes spread over AS-Path lengths between 1 and 8—to estimate the CPU cost for re-validating all the 32,000 routes with varying AS-Path lengths. It is important to note that the validation process of BGPSEC is related to the length of the AS-path, as it defines the number of signature verifications that have to be performed for a particular route update. Sriram et al. [109] estimates 34.59 s as the time required to re-validate all the peer routes for this particular case. This result gives insight into how much time a very large ISP router will spend in validating all the routes from a peer if the session is reset. The result of the extra burden due to signature validation is considerable because 34.59 s are required for one peer session reset only at a large ISP. Furthermore, this value does not include the time required for fetching and validating certificates. An option is that the certificate fetching and verification can be done off-line and prior to the validations, hence speeding up the validation process.

Moreover, according to Sriram et al. [109], if this BGPSEC router peers with 3 other BGPSEC routers, to whom it has to sign and forward these 32,000 routes after the re-validation phase, then the total estimated time including re-validation and signing will be around 73 s. It is acceptable to consider a degree of 3 for a large ISP router for early deployment phase of BGPSEC. However, in a full BGPSEC deployment scenario, a router has to re-validate and sign thousands of routes for each of its peers. Then the total time to process, considering the amount of prefixes advertised, will grow acutely—this issue is amplified if multiple sessions are reseted. The results presented by Sriram et al. [109] can be improved by using cryptographic hardware accelerators for the required cryptographic chores, however this would require installation of new hardware modules on the existing routers. In both cases, a handsome increase in processing power on the routers (at least the ones at large ISPs) is required to cope with the extra processing burden in full BGPSEC deployment scenario.

Estimation of Required Memory (hardware requirement):

As explained in Section 4.3, apart from the extra processing that BGPSEC requires, the memory capacity of the routers has to be revised as well. The extra information e.g., the signatures, that a BGPSEC update contains compared with a legacy BGP update will impact the routers' memory resources. In fact, the size of a BGPSEC update increases along with the number of ASes in the AS-path, as each AS must include its signed information. As a result, a BGPSEC update contains all the information required to verify and validate the AS-Path integrity, while all the required information for the validation must be handled in the routers' memory.

Sriram et al. [129] present an initial estimation of the required RIB memory size for a Tier-1's Route Reflector (RR) to accommodate the BGPSEC updates. The study projects the adoption of BGPSEC based on a truncated Normal distribution model. Moreover, the estimation model considers both internal (IGP) and external prefixes (EGP) with an annual prefix growth rate of 15% for external prefixes and 5% for internal prefixes. According to their estimations, with an RSA-2048 signature algorithm, the required RIB size would be 0.51 GB for the year 2016 (anticipating the start of BGPSEC adoption), 8.30 GB in 2020 (anticipating 50% BGPSEC adoption) and 32.11 GB in 2025 (anticipating 100% BGPSEC adoption). In contrast, for the ECDSA-256 signature algorithm, the required RIB memory size is estimated to be 0.42 GB for the year 2016, 3.19 GB for the year 2020 and 11.57 GB for the year 2025. These estimations also imply RIB memory upgrades to accommodate BGPSEC operations. Table 4 provides an overview regarding the RIB memory requirements as of today for BGP-4, and the projected RIB memory requirements of BGPSEC for a large ISP RR. The requirement of upgrading hardware in terms of CPU and memory to cope with the proposed solution clearly implies an increase in CAPEX, which seems difficult to face since the Return Of Investment (ROI) model as well as the incentives for early adoption are yet in early stages of research.

Accommodation of a New BGP Attribute (software requirement):

In addition to the new software components required to implement the protocol to communicate with the RPKI local caches, BGPSEC requires changes in the BGP protocol itself. The most prominent change is the replacement of the *AS_Path* attribute with the *BGPSEC_Path* to facilitate the signature requirements (see Section 4.3). Another noticeable requirement is that every BGPSEC speaker must support BGP extended messages, since the size of a BGPSEC update can be large due to the accumulation of the signatures along the AS-Path. Furthermore, in order to consider the result of the BGPSEC update validation process, changes are required in the BGP best route selection algorithm. Even though, the BGPSEC protocol leaves it open for the ASes to accomplish it according to their local policies, the issue of introducing changes to the current BGP protocol could be considered a major barrier for global acceptance.

Discussion: The main deployment challenges faced by the BGPSEC solution include requirements such as router upgrades—both in terms of processing power and memory size—as well as changes to the BGP protocol for accommodating a new BGP attribute. Furthermore, in order to improve on the time required to re-validate and sign BGPSEC updates, a cryptographic hardware accelerator can be

Table 4
Comparison of RIB size requirements between BGP-4 and BGPSEC (Note: This table is an excerpt from a table presented in [129]).

Year	Total RIB size (GB)		
	BGP-4 (RR)	BGPSEC (RR, RSA-2048)	BGPSEC (RR, ECDSA-256)
2013	0.29	0.30	0.30
2015	0.34	0.35	0.35
2016	0.37	0.51	0.42
2018	0.44	2.23	1.05
2020	0.53	8.30	3.19
2022	0.65	18.06	6.61
2025	0.88	32.11	11.57

considered for the routers. These hardware upgrades requirements of BGPSEC can be downplayed in presence of strong Return Of Investment (ROI) plans along with financial incentives for early adopters (cf. Section 5.3), however, we believe that the most difficult challenge for BGPSEC deployment is not the hardware-related part, but rather the software changes required to the ever resistant BGP protocol.

5.3. Global acceptance and adoption: challenges and strategies

Besides the obvious scalability aspects, the two essential prerequisites for adoption of a security proposal in the inter-domain routing system are protocol backward compatibility and flexible accommodation of partial deployments. As detailed in Section 4, the SIDR's proposals fulfill these two conditions, but still this seems to be insufficient. This is because the advantages and trade-offs of BGPSEC as well as of ROA and RPKI, can be rapidly diminished due to the high burden and complexity that they incur in terms of extensive software and hardware upgrades. Although these solutions can be considered technically feasible, their deployment or adoption is dependent on the revenue based incentives they might offer to attract early adopters, as the inter-domain business model is revenue-oriented. Apart from provably increased security offered by RPKI, ROA and BGPSEC, economic benefits are crucial for their success in the practical world. Therefore, it is important to look at possible strategies to boost the acceptance and deployment of SIDR's proposals.

Unfortunately, merely securing the inter-domain routing system seems unlikely to provide sufficient incentives for global acceptance. Gill et al. [130] raise the question that the benefits provided by BGPSEC protocol do not become real until a large number of ASes have deployed it. Thus, it proposes a strategy that governments and industry groups can harness ISP's local business objectives and drive a global deployment. Their analysis is focused on three main perspectives which aim to impact the global deployment of the solution. First, on simplex BGPSEC to secure stub ASes. Second, they claim that convincing a small but influential set of ASes to be early adopters of the solutions would boost a faster deployment. And third, ensuring that BGPSEC influences traffic by requiring ASes to break ties between equally-good paths based on security. Similarly, Lychev et al. [122] recommend focusing on the deployment of simplex BGPSEC at stub ASes, incorporation of secure paths in AS policies, and the deployment of BGPSEC at Tier-2 ISPs for the partial deployment period, to pave the way for wide-scale adoption in the future.

We can also extract some pragmatic lessons from the success story of RPKI adoption in Ecuador [131]. The Ecuador Internet Exchange (NAP.EC) holds a unique and critical position in the Ecuadorian nation-wide network, as almost 97% of all Internet users in Ecuador are directly connected to it. Thus, the adoption of RPKI by NAP.EC will cause—or at least it will speed-up—the RPKI adoption by all the other ISPs in the country. This is basically the same strategy recommended by Gill et al. [130], in the sense that RPKI adoption by influential ASes will facilitate faster RPKI technology dissemination. However, rather than forcing the adoption on the smaller players, a consensus was built among all the ISPs, through a series of technical training and information sessions provided by LACNIC and industrial stakeholders, with the aim of securing the routing problems in the country. As a result of these efforts, almost 100% of all the IPv4 addresses allocated in Ecuador have there corresponding ROAs [131]. The main hurdle for the adoption of RPKI faced in Ecuador was the fear of the new technology, as most of the operators had little or no knowledge or experience of RPKI and ROA. This fear was overcome by raising awareness through technical information and training sessions with the help of the local RIR and a network hardware vendor. Despite this, it is not clear that the adoption strategy used in Ecuador for deploying RPKI will yield similar results in other regions, especially, with multiple stakeholders (e.g., multiple IXPs and large ISPs) and thousand fold more Internet users.

Another very important aspect is that, to effectively limit the attacks using BGPSEC, the path validity information should necessarily influence the decision process of selecting a route—the BGPSEC validation output should be considered in the BGP decision process at an appropriate priority. In this regard, the BGPSEC protocol provides flexibility to ASes to prioritize security information according to local policies. Gill et al. [95] provide a survey result with an interesting insight into how ISPs perceive secure AS-Paths over insecure ones. The survey inquired different small to large ISPs to define at what stage of the BGP decision process would they place secure AS-Paths as compared to other metrics. Surprisingly, only 9% of the respondents would prioritize security first, and 21% indicated that they would place secure AS-Paths between the *localpref* and the *shortest AS-Path* metric (recall that the *localpref* is used to prioritize routes based on local criteria). And more importantly, 40% of the respondents would place security considerations at a lower step, i.e., even below the AS-Path length. Mindful of the fact that the respondents included only a fraction of the total ISPs, the results still provide substantial insight in how BGPSEC would be treated even if it is deployed despite all the shortcomings highlighted above. Most of the major known attacks on BGP succeed with the manipulation and exploitation of the *localpref* and the *shortest AS-Path* metrics in the BGP decision process, and if 40% of ISPs are not going to consider BGPSEC validation information then the future for BGPSEC protocol does not seem very promising given the current trends in the Internet community. In this regard, Lychev et al. [122] suggest to deploy islands of secure ASes where secure AS-Paths can be prioritized within the island to improve the effectiveness of BGPSEC. However, the study questions the benefits of secure AS-Paths (BGPSEC) given their collateral burden and advocates to explore security solutions including origin authentication (ROA) and prefix filtering to achieve reasonable level of security without disrupting the existing system.

6. Future way forward and open issues

The security of inter-domain routing poses multiple challenges, and any proposed security mechanism needs to be thoroughly and exhaustively analyzed and evaluated—keeping in mind all the different theoretical, operational and practical aspects of the problem. The SIDR proposals have faced acceptance as well as resistance within the research and industrial communities. As mentioned earlier, RPKI and ROA are already standardized, implemented and are in an early phase of deployment. However, BGPSEC is still being discussed and is facing resistance, especially, from industry. The main reason behind the strong opposition against BGPSEC is due to the requirement of syntactical and operational disruptive changes in the BGP protocol. Thus, we foresee two possible directions, either everyone agrees to the disruptive changes in BGP to resolve the security issues or explore different ways by which a proposed security mechanism could be integrated into the existing inter-domain routing system, while avoiding collateral burden and causing minimum entropy. We consider the latter direction as a promising path to follow as any BGP security solution requiring disruptive changes to the BGP protocol will face fateful resistance for its adoption in the real world. In the rest of this section, we discuss different proposals and concepts that advocate outsourcing of BGP security.

The outsourcing of BGP security targets to decouple security from the BGP protocol with the aim of minimizing the impact on the routers' installed base. In light of this, some of the authors of this article developed in collaboration with Cisco Systems the Path-State Protocol (PSP) [132]. This protocol provides a distributed overlay for transparently securing the BGP protocol. By "transparently" we mean that BGP is not even aware that is being secured. The idea behind the solution is to intercept the BGP packets at the routers, and divert the BGP announcements toward an overlay, which is in charge of the required cryptographic verifications, such as resource certificate and ROA validation. Thus, the security chores are outsourced from BGP to the overlay. As a result, the overlay can inspect the updates, and forward them back to the router for normal processing in case valid, or discard them otherwise—clearly, without altering the standard operation of BGP-4. Observe that the advantage is that BGP remains unaware that the updates are being inspected and validated, so its operations remain as if there were no security at all. This idea was demonstrated in a scaled trial that was exhibited at LACNOG 2012 [133]. For the demonstrations [134], we used a geographically distributed network topology between Europe and Latin America, where PSP controllers were used for controlling ten open source routers (Quagga routers), representing the ten ASes in the network topology. The goal of the demo was to show the potential of outsourced BGP security using overlays for mitigating traffic hijacking attempts through false BGP advertisements.

A similar approach is adopted by Borchert et. al. [135] for prototyping SIDR's solutions based on Quagga routers for the research community. Even though these approaches require a few modifications on the BGP protocol, we contend that these modifications are minor. For instance, only 88 lines of the BGP-4 code were modified in our prototype, so as to support the interception and re-injection of BGP messages, and thereby enable the outsourcing of security. Another promising approach for outsourcing security is through Software Defined Networks (SDN). SDN enables to outsource control functions of an SDN-enabled network element to external applications, by either exposing the available capabilities through proprietary APIs. The BGP/LS and PCEP project under the umbrella of OpenDaylight[1] [136] is putting in efforts to cater the deficiency of native support for BGP in the OpenDaylight SDN controller. The SDN approach offers an attractive alternative for developing outsourced security mechanisms, which could be materialized by means of an overlay network of distributed SDN controllers. Indeed, these type of solutions could combine proprietary Northbound APIs for the communication between a controller and BGP-4 (see, e.g., [137,138]), with future standard protocols supporting the horizontal communications among SDN controllers residing in different ASes. However, further efforts are required to formalize a blueprint of a distributed infrastructure involving SDN controllers (per AS domain) and to identify and provide necessary north-bound and south-bound APIs to pave the way for the deployment of security applications on top of the BGP protocol.

It is worth mentioning that the outsourcing of security away from the BGP protocol implies a vital design requirement on the BGP security solutions, that is, the security solution is able to achieve its security goals as an external function, i.e., decoupled from the BGP protocol. For example, the use of ROA to mitigate the false prefix origination attack can be outsourced away from the BGP. This is because the essential change that the ROA solution requires in the BGP protocol is only the consideration of the outcome of the ROA validation procedure in BGP route decision process. On the other hand, the BGPSEC solution is tightly coupled with the BGP protocol and hence cannot be implemented as an external security function. This highlights the need to develop security solutions that are not tightly coupled with the BGP protocol but at the same time enable run-time mitigation of security attacks. Furthermore, it needs to be investigated that how the minor changes required by the external security applications impact the run-time functionality of the BGP protocol.

Finally, we would like to highlight an untapped opportunity of possible collaboration between two IETF working groups which are targeting routing aspects on the Internet from different angles. The efforts for developing security mechanisms by the SIDR WG for the BGP protocol and by the LISP WG [139] for the Locator/ID Separation Protocol (LISP) protocol [140], are now totally disjoint. LISP is an initiative promoted as an open standard, aimed to be a scalable next-generation routing and addressing architecture. We believe that both working groups can benefit from the mechanisms developed by each other. For instance, the LISP protocol can benefit from the security infrastructure developed by SIDR, including RPKI and ROA, so as to improve its control-plane security. The RPKI and ROA can provide authorization and prevent Man-in-the-Middle and over-claiming attacks on the LISP mapping system. For example, Montero et al. [141], proposed an end-to-

[1] The OpenDaylight project is a collaborative open source initiative, supported by the industry, to expedite the adoption of software defined networking. For more details, please refer to [136].

end security mechanism for map registrations in LISP leveraged on the design and infrastructure of ROA and RPKI. Similarly, SIDR can take inspiration from the way LISP outsources the mapping information to an overlay mapping system [142], for outsourcing the security mechanisms to an overlay network. In summary, the collaboration of these two working groups could not only avoid the development of solutions that might be at odds with the other, but could also help improving the overall Internet routing security.

7. Conclusion

In this paper, we surveyed the efforts that are being developed and standardized by the IETF SIDR WG for securing the inter-domain routing system. The SIDR proposals counter some of the existing vulnerabilities of BGP, but with the collateral burden of needing considerable software and hardware upgrades in the inter-domain routing system. More specifically, the BGPSEC protocol requires syntactical and operational changes to the BGP protocol, causing enough entropy to invite resistance from the industry. Furthermore, we discussed the BGP risks that remain unresolved even after fully adopting the SIDR's proposals along with the attacks that are possible by exploiting the operational shortcomings of SIDR proposals. We also discussed the deployment and adoption challenges faced by the SIDR solution. It is worth mentioning that the security solutions of the SIDR WG still represent work in progress, since the RPKI and ROA are currently in trial deployment phase, while the BGPSEC protocol is still under discussion.

From this perspective, we highlighted possible directions for future research in securing inter-domain routing. Firstly, to explore different ways for integrating the proposed security mechanisms into the inter-domain routing system with minimum entropy, such as through SDNs and Overlay solutions. Then, we pointed out a possible collaboration opportunity between the SIDR WG and LISP WG for developing security mechanisms coordinately, as they are addressing security aspects from different angles, even though they both involve the global routing system. We consider that the discussion presented in this paper will help researchers in the area, especially, in the necessity of looking for security alternatives that "almost" do not touch BGP, which, from a research point of view, is quite challenging.

Acknowledgements

The authors would like to acknowledge the support received from the Spanish Ministry of Science and Innovation under contract TEC2012-34682, project partially funded by FEDER, the Catalan Government under contract 2009 SGR1508, the IST Open-LAB Project under contract FP7-287581, and Cisco Systems through a Cisco RFP grant. In particular, the authors are grateful for the valuable discussions they had with Roque Gagliano, Keyur Patel, Fabio Maino, Rodolfo Milito, and Vina Ergaman from Cisco Systems.

References

[1] Y. Rekhter, T. Li, S. Hares, A Border Gateway Protocol 4 (BGP-4), RFC 4271, IETF, 2006.

[2] D. Pei, M. Azuma, D. Massey, L. Zhang, BGP-RCN: improving bgp convergence through root cause notification, Comput. Netw. 48 (2005) 175–194.

[3] D. Pei, X. Zhao, L. Wang, D. Massey, A. Mankin, S.F. Wu, L. Zhang, Improving BGP convergence through consistency assertions, in: Proceedings of the Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2002, vol. 2, IEEE, pp. 902–911.

[4] C. Labovitz, A. Ahuja, A. Bose, F. Jahanian, Delayed Internet routing convergence, in: Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, SIGCOMM '00, ACM, New York, USA, 2000, pp. 175–187.

[5] C. Labovitz, G.R. Malan, F. Jahanian, Internet routing instability, IEEE/ACM Trans. Network. 6 (1998) 515–528.

[6] L. Gao, J. Rexford, Stable internet routing without global coordination, SIGMETRICS Perform. Eval. Rev. 28 (2000) 307–317.

[7] A. Basu, C.-H.L. Ong, A. Rasala, F.B. Shepherd, G. Wilfong, Route oscillations in I-BGP with route reflection, in: Proceedings of the 2002 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, SIGCOMM '02, ACM, New York, USA, 2002, pp. 235–247.

[8] K. Varadhan, R. Govindan, D. Estrin, Persistent route oscillations in inter-domain routing, Comput. Netw. 32 (2000) 1–16.

[9] A. Feldmann, O. Maennel, Z.M. Mao, A.W. Berger, B.M. Maggs, Locating internet routing instabilities, SIGCOMM, ACM, 2004, pp. 205–218.

[10] T.G. Griffin, B.J. Premore, An experimental analysis of BGP convergence time, Ninth International Conference on Network Protocols, 2001, IEEE Computer Society, 2001, pp. 53–61.

[11] G. Huston, M. Rossi, G. Armitage, A technique for reducing BGP update announcements through path exploration damping, IEEE J. Sel. A. Commun. 28 (2010) 1271–1286.

[12] N. Valler, M. Butkiewicz, B. Prakash, M. Faloutsos, C. Faloutsos, Non-binary information propagation: Modeling BGP routing churn, in: IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2011, pp. 900–905.

[13] A. Elmokashfi, A. Kvalbein, T. Cicic, On Update Rate-Limiting in BGP, in: IEEE International Conference on Communication (ICC), 2011, pp. 1–6.

[14] B. Quoitin, C. Pelsser, L. Swinnen, O. Bonaventure, S. Uhlig, Interdomain traffic engineering with BGP, IEEE Comm. Mag. 41 (2003).

[15] N. Feamster, J. Winick, J. Rexford, A model of BGP routing for network engineering, SIGMETRICS Perform. Eval. Rev. 32 (2004) 331–342.

[16] W. Xu, J. Rexford, MIRO: multi-path interdomain routing, SIGCOMM Comput. Commun. Rev. 36 (2006) 171–182.

[17] S. Goldberg, S. Halevi, A.D. Jaggard, V. Ramachandran, R.N. Wright, Rationality and traffic attraction: incentives for honest path announcements in BGP, SIGCOMM Comput. Commun. Rev. 38 (2008) 267–278.

[18] L. Subramanian, S. Agarwal, J. Rexford, R. Katz, Characterizing the internet hierarchy from multiple vantage points, in: Proceedings of the Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2002, vol. 2, IEEE, pp. 618–627.

[19] T. Griffin, F.B. Shepherd, G.T. Wilfong, Policy disputes in path-vector protocols, in: Proceedings of the Seventh Annual International Conference on Network Protocols, ICNP '99, IEEE Computer Society, Washington, DC, USA, 1999, p. 21.

[20] L. Gao, On inferring autonomous system relationships in the internet, IEEE/ACM Trans. Netw. 9 (2001) 733–745.

[21] F. Wang, L. Gao, On inferring and characterizing internet routing policies, in: Proceedings of the 3rd ACM SIGCOMM Conference on Internet Measurement, IMC '03, ACM, New York, USA, 2003, pp. 15–26.

[22] H. Tangmunarunkit, R. Govindan, S. Shenker, D. Estrin, The impact of routing policy on internet paths, in: INFOCOM 2001. Proceedings of the Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 2, IEEE, pp. 736–742.

[23] J. Xia, L. Gao, On the evaluation of AS relationship inferences [Internet Reachability/Traffic Flow Applications], in: Global Telecommunications Conference, 2004, GLOBECOM '04, vol. 3, IEEE, pp. 1373–1377.

[24] S. Qiu, P. McDaniel, F. Monrose, Toward valley-free inter-domain routing, in: IEEE International Conference on Communications, 2007, ICC '07, pp. 2009–2016.

[25] G. Di Battista, T. Erlebach, A. Hall, M. Patrignani, M. Pizzonia, T. Schank, Computing the types of the relationships between autonomous systems, IEEE/ACM Trans. Netw. 15 (2007) 267–280.

[26] N. Feamster, H. Balakrishnan, J. Rexford, Some foundational problems in Interdomain routing, in: 3rd ACM SIGCOMM Workshop on Hot Topics in Networks (HotNets), pp. 41–46.

[27] M. Yannuzzi, X. Masip-Bruin, O. Bonaventure, Open issues in interdomain routing: a survey, Netwrk. Mag. Global Internetwkg. 19 (2005) 49–56.

[28] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S.F. Wu, L. Zhang, An analysis of BGP multiple origin AS (MOAS) conflicts, in: Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement, IMW '01, ACM, New York, USA, 2001, pp. 31–35.

[29] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S.F. Wu, L. Zhang, Detection of invalid routing announcement in the internet, in: Proceedings of the 2002 International Conference on Dependable Systems and Networks, DSN '02, IEEE Computer Society, Washington, DC, USA, 2002, pp. 59–68.

[30] T. Griffin, G. Huston, BGP Wedgies, RFC 4264, IETF, 2005.

[31] R. Mahajan, D. Wetherall, T. Anderson, Understanding BGP misconfiguration, in: Proceedings of the 2002 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, SIGCOMM '02, ACM, New York, USA, 2002, pp. 3–16.

[32] R. Perlman, Network Layer Protocols with Byzantine Robustness, Ph.D. thesis, Massachusetts Institute of Technology, MIT-LCS-TR-429, 1988.

[33] Z.M. Mao, J. Rexford, J. Wang, R.H. Katz, Towards an accurate AS-level traceroute tool, in: Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, SIGCOMM '03, ACM, New York, USA, 2003, pp. 365–378.

[34] R. Dube, A comparison of scaling techniques for BGP, SIGCOMM Comput. Commun. Rev. 29 (1999) 44–46.

[35] R. Teixeira, J. Rexford, A measurement framework for pin-pointing routing changes, in: Proceedings of the ACM SIGCOMM Workshop on Network Troubleshooting: Research, Theory and Operations Practice Meet Malfunctioning Reality, NetT '04, ACM, New York, USA, 2004, pp. 313–318.

[36] N. Feamster, H. Balakrishnan, J. Rexford, A. Shaikh, J. van der Merwe, The case for separating routing from routers, in: Proceedings of the ACM SIGCOMM Workshop on Future Directions in Network Architecture, FDNA '04, ACM, New York, USA, 2004, pp. 5–12.

[37] N. Feamster, J. Rexford, Network-wide prediction of BGP routes, IEEE/ACM Trans. Netw. 15 (2007) 253–266.

[38] R. Oliveira, B. Zhang, D. Pei, R. Izhak-Ratzin, L. Zhang, Quantifying path exploration in the internet, in: Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement, IMC '06, ACM, New York, USA, 2006, pp. 269–282.

[39] N. Feamster, H. Balakrishnan, Towards a logic for wide-area internet routing, SIGCOMM Comput. Commun. Rev. 33 (2003) 289–300.

[40] T. Bates, R. Chandra, D. Katz, Y. Rekhter, Multiprotocol extensions for BGP-4, RFC 4760, IETF, 2007.

[41] L. Gao, T. Griffin, J. Rexford, Inherently safe backup routing with BGP, in: Proceedings of tjhe Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2001, vol. 1, IEEE, pp. 547–556.

[42] M. Lad, R. Oliveira, B. Zhang, L. Zhang, Understanding resiliency of internet topology against prefix hijack attacks, in: Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN '07, IEEE Computer Society, Washington, DC, USA, 2007, pp. 368–377.

[43] K. Sriram, D. Montgomery, O. Borchert, O. Kim, D.R. Kuhn, Study of BGP peering session attacks and their impacts on routing performance, IEEE J. Sel. A. Commun. 24 (2006) 1901–1915.

[44] K. Sriram, O. Borchert, O. Kim, P. Gleichmann, D. Montgomery, A comparative analysis of BGP anomaly detection and robustness algorithms, in: Proceedings of the 2009 Cybersecurity Applications & Technology Conference for Homeland Security, CATCH '09, IEEE Computer Society, Washington, DC, USA, 2009, pp. 25–38.

[45] D. Wendlandt, I. Avramopoulos, Don't secure routing protocols, secure data delivery, in: Proceedings of the 5th ACM Workshop on Hot Topics in Networks (Hotnets-V).

[46] A.T. Mizrak, Y. Cheng, K. Marzullo, S. Savage, Fatih: detecting and isolating malicious routers, in: Proceedings of the International Conference on Dependable Systems and Networks, DSN 2005, 2005, pp. 538–547.

[47] Fang Fang, A.B. Whinston, M. Parameswaran, X. Zhao, Reengineering the internet for better security, Computer 40 (2007) 40–44.

[48] O. Nordström, C. Dovrolis, Beware of BGP attacks, SIGCOMM Comput. Commun. Rev. 34 (2004) 1–8.

[49] B. Kumar, J. Crowcroft, Integrating security in inter-domain routing protocols, SIGCOMM Comput. Commun. Rev. 23 (1993) 36–51.

[50] J. Karlin, S. Forrest, J. Rexford, Pretty good BGP: improving BGP by cautiously adopting routes, in: Proceedings of the 2006 IEEE International Conference on Network Protocols, ICNP '06, IEEE Computer Society, Washington, DC, USA, 2006, pp. 290–299.

[51] H. Chan, D. Dash, A. Perrig, H. Zhang, Modeling adoptability of secure BGP protocol, SIGCOMM Comput. Commun. Rev. 36 (2006) 279–290.

[52] K. Butler, P. McDaniel, W. Aiello, Optimizing BGP security by exploiting path stability, in: Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS '06, ACM, New York, USA, 2006, pp. 298–310.

[53] M. Zhao, S.W. Smith, D.M. Nicol, The performance impact of BGP security, IEEE Network 19 (2005) 42–48.

[54] V.J. Bono, 7007 Explanation and Apology, 1997 <http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html>.

[55] G. Huston, Leaking Routes, 2012 <http://www.potaroo.net/ispcol/2012-03/leaks.html>.

[56] RIPE NCC, Youtube Hijacking: A Ripe NCC RIS Case Study, 2010 <http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>.

[57] H. Balakrishnan, N. Feamster, Interdomain Internet Routing, Lecture Notes, 2009.

[58] C. Labovitz, China Hijacks 15% of Internet Traffic, 2010 <http://www.arbornetworks.com/asert/2010/11/china-hijacks-15-of-internet-traffic/>.

[59] R. Kuhn, K. Sriram, D. Montgomery, Border Gateway Protocol Security: Recommendations of the National Institute of Standards and Technology, Special Publication, 2007, pp. 800–854.

[60] S. Kent, C. Lynn, J. Mikkelson, K. Seo, Secure border gateway protocol (s-BGP), IEEE J. Sel. Areas Commun. 18 (2000) 103–116.

[61] R. White, Securing BGP through secure origin BGP (soBGP), Internet Protocol J. 6 (2003).

[62] P.v. Oorschot, T. Wan, E. Kranakis, On interdomain routing security and pretty secure BGP (psBGP), ACM Trans. Inf. Syst. Secur. 10 (2007).

[63] G. Goodell, W. Aiello, T. Griffin, J. Ioannidis, P. McDanial, A. Rubin, Working around BGP: an incremental approach to improving security and accuracy of interdomain routing, in: Proceedings of the Internet Society Symposium on Network Distributed Systems Security (NDSS), 2003.

[64] Y.-C. Hu, A. Perrig, M. Sirbu, SPV: secure path vector routing for securing BGP, SIGCOMM Comput. Commun. Rev. 34 (2004) 179–192.

[65] Q. Li, M. Xu, J. Wu, X. Zhang, P.P.C. Lee, K. Xu, Enhancing the trust of Internet Routing with Lightweight Route Attestation, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS '11, ACM, 2011, pp. 92–101.

[66] M. Suchara, I. Avramopoulos, J. Rexford, Securing BGP incrementally, in: Proceedings of the 2007 ACM CoNEXT Conference, CoNEXT '07, ACM, New York, USA, 2007, pp. 52:1–52:2.

[67] H. Yin, B. Sheng, H. Wang, J. Pan, Keychain-based signatures for securing BGP, IEEE J. Sel. A. Commun. 28 (2010) 1308–1318.

[68] M. Roughan, W. Willinger, O. Maennel, D. Perouli, R. Bush, 10 Lessons from 10 years of measuring and modeling the internet's autonomous systems, IEEE J. Sel. Areas Commun. 29 (2011) 1810–1821.

[69] B. Bruhadeshwar, S.S. Kulkarni, A.X. Liu, Symmetric key approaches to securing BGP-a little bit trust is enough, IEEE Trans. Parallel Distrib. Syst. 22 (2011) 1536–1549.

[70] W. Aiello, J. Ioannidis, P. McDaniel, Origin authentication in interdomain routing, in: Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS '03, ACM, New York, USA, 2003, pp. 165–178.

[71] H. Ballani, P. Francis, X. Zhang, A study of prefix hijacking and interception in the internet, in: Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, SIGCOMM '07, ACM, New York, USA, 2007, pp. 265–276.

[72] J. Israr, M. Guennoun, H.T. Mouftah, Credible BGP – extensions to BGP for secure networking, in: Proceedings of the 2009 Fourth International Conference on Systems and Networks Communications, ICSNC '09, IEEE Computer Society, Washington, DC, USA, 2009, pp. 212–216.

[73] M. Zhao, S.W. Smith, D.M. Nicol, Aggregated path authentication for efficient BGP security, in: Proceedings of the 12th ACM Conference on Computer and Communications Security, CCS '05, ACM, New York, USA, 2005, pp. 128–138.

[74] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, IETF, 1998.

[75] B. Smith, J. Garcia-Luna-Aceves, Securing the Border Gateway Routing Protocol, in: Global Telecommunications Conference, GLOBECOM '96, Communications: The Key to Global Prosperity, 1996, pp. 81–85.

[76] Z. Zhang, Y. Zhang, Y.C. Hu, Z.M. Mao, Practical defenses against BGP prefix hijacking, in: Proceedings of the 2007 ACM CoNEXT Conference, CoNEXT '07, ACM, New York, USA, 2007, pp. 3:1–3:12.

[77] E.L. Wong, P. Balasubramanian, L. Alvisi, M.G. Gouda, V. Shmatikov, Truth in advertising: lightweight verification of route integrity, in: PODC, ACM, 2007, pp. 147–156.

[78] Y.-C. Hu, Efficient security mechanisms for routing protocols, in: In Proc. NDSS03, pp. 57–73.

[79] T. Bates, R. Bush, T. Li, Y. Rhekter, DNS-based NLRI origin as verification in BGP, draft-bates-bgp4-nlri-orig-verif, 1998.

[80] D. Ward, Securing BGPv4 using IPsec, draft-ward-bgp-ipsec, 2000.

[81] X. Shi, Y. Xiang, Z. Wang, X. Yin, J. Wu, Detecting prefix hijackings in the internet with argus, in: Proceedings of the 2012 ACM Conference on Internet Measurement Conference, IMC '12, ACM, New York, NY, USA, 2012, pp. 15–28.

[82] Secure InterDomain Routing (SIDR) Working Group IETF, 2013 <http://datatracker.ietf.org/wg/sidr/>.

[83] Secure InterDomain Routing (SIDR) Working Group Charter, 2013 <https://datatracker.ietf.org/wg/sidr/charter/>.

[84] The Internet Engineering Task Force (IETF), 2013 <http://www.ietf.org/>.

[85] RIPE Network Coordination Center, 2013 <http://www.ripe.net/>.

[86] American Registry for Internet Numbers, 2013 <https://www.arin.net/>.

[87] M. Lepinski, S. Kent, An Infrastructure to Support Secure Internet Routing, RFC 6480, IETF, 2012.

[88] M. Lepinski, S. Kent, D. Kong, A Profile for Route Origin Authorizations (ROAs), RFC 6482, IETF, 2012.

[89] M. Lepinski, BGPSEC Protocol Specification, draft-ietf-sidr-bgpsec-protocol, 2013.

[90] Y. Song, A. Venkataramani, L. Gao, Identifying and addressing protocol manipulation attacks in secure BGP, in: IEEE 33rd International Conference on Distributed Computing Systems (ICDCS), 2013, pp. 550–559.

[91] G. Huston, M. Rossi, G. Armitage, Securing BGP – a literature survey, IEEE Commun. Surv. Tut. 13 (2011).

[92] K. Butler, T.R. Farley, P. McDaniel, J. Rexford, A survey of BGP security issues and solutions, Proc. IEEE 98 (2010) 100–122.

[93] G. Huston, Interconnection, peering, and settlements, in: Proceedings of the INET, June 1999.

[94] V. Giotsas, S. Zhou, Valley-free violation in Internet routing–analysis based on BGP community data, in: IEEE International Conference on Communications (ICC), 2012, pp. 1193–1197.

[95] P. Gill, S. Goldberg, M. Schapira, A Survey of Interdomain Routing Policies, Presented at NANOG'56, 2012 <http://www.cs.bu.edu/~goldbe/papers/survey.pdf>.

[96] J.W. Stewart, BGPv4: Inter-Domain Routing in the Internet, Addison-Wesley, 1999.

[97] S. Halabi, Internet Routing Architectures, Cisco Press, 2000.

[98] B. Dickson, Route Leaks – Requirements for Detection and Prevention thereof, draft-dickson-sidr-route-leak-reqts, 2012.

[99] B. Dickson, Route Leaks – Definitions, draft-dickson-sidr-route-leak-def, 2012.

[100] M. Nicholes, B. Mukherjee, A survey of security techniques for the border gateway protocol (BGP), IEEE Commun. Surv. Tut. 11 (2009) 52–65.

[101] A. Heffernan, Protection of BGP Sessions via the TCP MD5 Signature Option, RFC 2385, IETF, 1998.

[102] A. Boldyreva, R. Lychev, Provable Security of S-BGP and Other Path Vector Protocols: Model, Analysis and Extensions, in: Proceedings of the 2012 ACM Conference on Computer and Communications Security, CCS '12, ACM, New York, NY, USA, 2012, pp. 541–552.

[103] Internet Assigned Numbers Authority (IANA), 2013 <http://www.iana.org/>.

[104] R. Bush, R. Austein, The Resource Public Key Infrastructure (RPKI) to Router Protocol, RFC 6810, IETF, 2013.

[105] Open Networking Foundation (ONF), 2013 <https://www.opennetworking.org/>.

[106] G. Huston, G. Michaelson, Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs), RFC 6483, IETF, 2012.

[107] R. Bush, BGPSEC Operational Considerations, draft-ietf-sidr-bgpsec-ops, 2012.

[108] K. Sriram, BGPSEC Design Choices and Summary of Supporting Discussions, draft-sriram-bgpsec-design-choices, 2013.

[109] K. Sriram, R. Bush, Estimating CPU Cost of BGPSEC on a Router, IETF 82 SIDR WG Meeting, 2012.

[110] S. Goldberg, M. Schapira, P. Hummon, J. Rexford, How secure are secure interdomain routing protocols?, Comput Netw. 70 (2014) 260–287.

[111] CloudFlare, Why Google Went Offline Today and a Bit about How the Internet Works, 2012 <http://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about>.

[112] S. Kent, A. Chi, Threat Model for BGP Path Security, RFC 7132, IETF, 2014.

[113] Global Routing Operations (GROW) Working Group IETF, 2013 <http://datatracker.ietf.org/wg/grow/>.

[114] D. McPherson, S. Amante, E. Osterweil, D. Mitchell, Route-Leaks & MITM Attacks Against BGPSEC, draft-ietf-grow-simple-leak-attack-bgpsec-no-help-04, 2014.

[115] K. Sriram, D. Montgomery, Enhancement to BGPSEC for Protection against Route Leaks, draft-sriram-route-leak-protection-00, 2014.

[116] S. Sundaresan, R. Lychev, V. Valancius, Preventing attacks on bgp policies: One bit is enough, 2011.

[117] B. Dickson, Route Leaks – Proposed Solutions, draft-dickson-sidr-route-leak-solns, 2012.

[118] K. Sriram, D. Montgomery, Design Discussions and Comaparison of Replay-Attack Protection Mechanisms for BGPSEC, draft-sriram-replay-protection-design-discussion, 2012.

[119] R. Gagliano, K. Patel, B. Weis, BGPSEC router key rollover as an alternative to beaconing, draft-ietf-sidr-bgpsec-rollover, 2013.

[120] Q. Li, X. Zhang, X. Zhang, P. Su, Invalidating idealized BGP security proposals and countermeasures, dependable and secure computing, IEEE Trans. PP (2014) 1–1.

[121] S. Bellovin, R. Bush, D. Ward, Security Requirements for BGP Path Validation, RFC 7353, IETF, 2014.

[122] R. Lychev, S. Gol dberg, M. Schapira, BGP security in partial deployment: is the juice worth the squeeze? in: Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM, ACM, pp. 171–182.

[123] D. Cooper, E. Heilman, K. Brogle, L. Reyzin, S. Goldberg, On the Risk of Misbehaving RPKI Authorities, in: Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks, HotNets-XII, ACM, New York, NY, USA, 2013, pp. 16:1–16:7.

[124] E. Heilman, D. Cooper, L. Reyzin, S. Goldberg, From the consent of the routed: Improving the transparency of the rpki, in: Proceedings of the 2014 ACM Conference on SIGCOMM, SIGCOMM '14, ACM, New York, NY, USA, 2014, pp. 51–62.

[125] E. Osterweil, T. Manderson, R. White, D. McPherson, Sizing Estimates for a Fully Deployed RPKI, Technical Report 1120005 version 2, Verisign, 2012.

[126] S. Kent, K. Sriram, RPKI rsync Download Delay Modeling, IETF 86 SIDR WG Meeting, 2013.

[127] T. Bruijnzeels, O. Muravskiy, B. Weber, RPKI Repository Analysis and Requirements, draft-tbruijnzeels-sidr-repo-analysis-00, 2013.

[128] R. Bush, [sidr] Scaling Properties of Caching in a Globally Deployed RPKI/BGPSEC System, 2012 <http://www.ietf.org/mail-archive/web/sidr/current/msg05351.html>.

[129] K. Sriram, O. Borchert, O. Kim, D. Cooper, D. Montgomery, RIB Size Estimation for BGPSEC, 2011 <http://www.nist.gov/itl/antd/upload/BGPSEC_RIB_Estimation.pdf>.

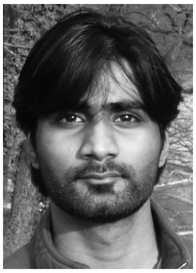
[130] P. Gill, M. Schapira, S. Goldberg, Let the market drive deployment: a strategy for transitioning to bgp security, in: Proceedings of the ACM SIGCOMM 2011 Conference, SIGCOMM '11, ACM, New York, USA, 2011, pp. 14–25.

[131] F. Mejia, R. Gagliano, C. Martinez, G. Rada, Implementing rpki-based origin validation one country at a time. the ecuadorian case study, draft-fmejia-origin-a-country, 2014.

[132] M. Yannuzzi, Path-State Protocol (PSP), 2012 <http://www.craax.upc.edu/psp.html>.

[133] LACNOG, LACNOG 2012, Montevideo, Uruguay, October/November 2012 <http://www2.lacnic.net/sp/eventos/lacnicxviii/index.html>.

[134] M. Yannuzzi, R. Serral-Graci, S. Siddiqui, E. Serra, X. Masip-Bruin, BGP Path-State Overlays as an Alternative to BGPSEC, 2012 <http://www.craax.upc.edu/pdf/PSP_Demo_LACNOG.pdf>.
[135] O. Borchert, S. Spies, K. Lee, D. Montgomery, K. Sriram, O. Kim, NIST BGP-SRx and BRITE Implementations, 2011 <https://www.nanog.org/meetings/nanog53/presentations/Monday/SRxAndBRITE_NANOG53.pdf>.
[136] OpenDaylight—A Linux Foundation Collaborative Project, 2014 <http://www.opendaylight.org/>.
[137] Cisco, Cisco OnePK, 2014 <https://developer.cisco.com/web/onepk>.
[138] JUNIPER, JUNIPER's JUNOS SDK, 2014 <https://developer.juniper.net/content/develop-overview/junos-sdk/getting-started.page>.
[139] Locator/ID Separation Protocol (LISP) Working Group IETF, 2013 <http://tools.ietf.org/wg/lisp/>.
[140] G. Farinacci, V. Fuller, D. Meyer, D. Lewis, The Locator/ID Separation Protocol (LISP), RFC 6830, IETF, 2013.
[141] D. Montero, M.S. Siddiqui, R. Serral, X. Masip, Y. Yannuzzi, Securing the LISP Map Registration Process, to be published in Globecom 2013 – Next Generation Networking Symposium (GC13 NGN), 2013.
[142] V. Fuller, G. Farinacci, D. Meyer, D. Lewis, Locator/ID Separation Protocol Alternative Logical Topology (LISP+ALT), RFC 6836, IETF, 2013.



Muhammad Shuaib Siddiqui is a research associate as well as a Ph.D. candidate at Technical University of Catalonia (UPC), Spain. He received his B.Sc in Computer Engineering from King Fahd University of Petroleum & Minerals (KFUPM), Saudi Arabia, and M.Sc in Communication Systems Engineering from École Polytechnique Fédérale de Lausanne (EPFL), Switzerland. Currently, he is a PhD candidate working both with the Networking and Information Technology Lab (NetITLab), and the Advanced Network Architectures Lab (CRAAX) at UPC. His research interests include Network Security, Inter-Domain Routing Protocols, and Performance Evaluation.

Diego Montero received his B.Sc. in Computer Engineering from University of Cuenca (UDC), Ecuador. He completed his M.Sc. in Computer Architecture, Networks and Systems (CANS) from Technical University of Catalonia (UPC), Spain. He is currently a Ph.D. candidate at the Networking and Information Technology Lab (NetITLab), where his research interests include Network Security, Software Defined Networking (SDN) and Cloud Computing.

René Serral-Gracià received his degree in computer science (2003) and a Ph.D. (2009) from the Technical University of Catalunya (UPC). He is the R&D head of the Networking and Information Technology Lab (NetITLab) at UPC, where he is leading different research initiatives, including projects under the European FP7 Research Framework as well as with industry. He is also an Associate Professor at the Department of Computer Architecture at UPC. His research interests are focused on Software Defined Networks (SDNs), overlay networks, network security, routing optimization, and QoE assessment of multimedia traffic.

Xavi Masip-Bruin, Ph.D. in Telecommunications Engineering from the Technical University of Catalonia (2003) is serving from its creation in 2008 as Director of the Advanced Network Architectures Lab (CRAAX), where he has been involved in several research initiatives funded by both the public and private sectors. Xavi has a large track record of participation in FP6 and FP7 EU research projects and he has been engaged in initiatives in close collaboration with industry including Cisco Systems, IBM, etc. His current R&D activities are in the areas of network programmability and adaptability, network management, protocolar network architectures design, IoT, and smart cities and novel services.

Marcelo Yannuzzi received a degree in Electrical Engineering from the University of the Republic, Uruguay, and the MSc. and Ph.D. degrees in Computer Science from the Department of Computer Architecture (DAC), Technical University of Catalonia (UPC), Spain. He is the head of the Networking and Information Technology Lab (NetITLab) at UPC, as well as the head of the Advanced Network Architectures (ANA) research group at UPC. He is involved in several research initiatives and projects in close interaction with European and US companies and research centers. His research interests lie on Software Defined Networks (SDNs), Network-based Intelligence (NBI), outsourced computation and control of network functions, security, network management, smart orchestrations, and mobility.