Understanding BGP Anomalies: Detection, Analysis, and Prevention

15-744 Class Project Report

Pratyusa Manadhata, Vyas Sekar
{pratyus,vyass}@cs.cmu.edu

***Abstract*— The Border Gateway Protocol is the de-facto inter-domain routing protocol in the Internet. Previous studies and various incidents have shown the vulnerability of the BGP infrastructure to a number of failures. In this paper we address a subset of the problem of BGP vulnerabilities we refer to as BGP anomalies, which can arise both as a result of mistakes by network operators and as a result of malicious attacks. Such incidents include routing loops, policy violations, incorrect export of routes between neighboring ASes, origin violations and address space hijacks, false announcements claiming non-existent connectivity, private AS announcements etc. We discuss a set of techniques for identifying these anomalies building on the existing work from [7], [17], and [4]. We present some results quantifying the occurrences of such anomalies in a recent dataset obtained from the RouteViews server, proving that the threat of routing failure due to anomalies still exists. We also discuss proposed solutions for prevention of such anomalies and outline a set of desirable properties for the inter-domain routing framework. The set of anomalies we present is by no means comprehensive, and it is also likely that most of them are likely to be harmless. However the problem of detecting, analyzing, and preventing these anomalies is non-trivial, and we believe such a framework is necessary to prevent routing failures in the future. We hope that our observations and suggestions are useful towards achieving long-term goals of secure and robust inter-domain routing.**

I. Introduction

The Internet depends on routing at two levels for successful operation: at the intra-domain level and at the inter-domain level. Intra-domain routing operates usually within an institution or an administrative domain, while inter-domain routing operates across Autonomous Systems (ASes), which are defined as a set of routers under a single technical administration using an exterior gateway protocol to route packets to other ASes. Inter-domain routing protocols have evolved over time, and in today's Internet the de-facto standard is BGP [16]. BGP operates as a path-vector protocol that strives to enable ASes to exchange the routing information to disseminate global reachability knowledge. It is quite evident that the correct operation of BGP is a necessary condition for wide area routing. Due to the inherent design of BGP it is possible for the entire Internet to observe and be affected by the misbehavior of one particular AS. The canonical incidents quoted in the literature include the AS7007 incident [15], and the AS3561 incident [14], which led to global connectivity disruption.

There has been work in the Internet community to develop threat models and identify vulnerabilities in the BGP framework [9], [10]. While these attempt to outline the set of possible attacks that a malicious attacker could launch against the infrastructure, a more plausible set of disruptions are caused by accidental mis-configurations in routers. [1] presented some of the earliest results in quantifying the occurrences of mis-configurations in inter-domain routing. From the perspective of network reliability it may be prudent to view misconfigurations and attacks to be identical, which we refer to as anomalies. We believe therefore that it is necessary to develop a comprehensive framework for detection, analysis, and prevention of BGP anomalies. In this paper we focus on a set of anomalies that are observed in the AS-paths, which is the single most important attribute of BGP messages. We do wish to state upfront that the anomalies we present are not exhaustive, and there may exist other kinds of anomalies, both in the AS-paths and in BGP announcements and messages (which is outside the scope of this paper).

The rest of this paper is organized as follows: In Section II we present some background on the operation of inter-domain routing, both with respect to the functioning of BGP, and also in terms of the relationships between ASes. We present some of the related work in the areas of BGP security, identifying AS relationships and the AS hierarchy, and detection of misconfigurations and false announcements in Section III. We attempt to outline a set of anomalies in the AS-paths that can be observed from routing tables in Section IV. Some of the preliminary results, and analysis are presented in Section V. We also analyze the existing proposals for securing the BGP infrastructure and detecting anomalies to enable the design of a more comprehensive framework for detection and prevention of anomalies. We discuss some desirable properties of a robust interdomain routing infrastructure in Section VI. Finally we conclude in Section VII, providing indications of the caveats of our work, and giving some directions for future work in this area.

II. Background: BGP and Inter-Domain Routing

In this section we describe some of the aspects of the operation of BGP and inter-domain routing in general. The Internet is divided into a large number of Autonomous Systems (AS) that represent an aggregation of a collection of hosts that are under a single administrative domain. Within an AS an intra-domain routing protocol such as OSPF or IS-IS is used to enable connectivity across hosts attached to the same domain.

ASes exchange routing information between each other to enable global connectivity. There are different categories of economic agreements between ASes, the predominant being a provider-customer relationship. A less common agreement is the peering relationship [19], where ASes carry traffic mutually between their customers for free. Another type of commercial agreement that is observed is one of mutual transit (sibling), that can occur either as a result of commercial mergers, or is implemented by small ISPs within the same region that try to provide better connectivity to its clients by sharing routes with each other.

BGP is the primary routing protocol that is intended for the purpose of achieving inter-domain routing. BGP is a path vector protocol in the sense that route announcements carry the AS-path to the destination (to prevent routing loops). A network operator can configure a router with a set of export and import policies. The export policies decide whether a route learned either from the intra-domain routing, or from neighboring ASes is announced to other neighbors. The import policies help to choose the best path over the learned paths. The common criterion is routes learned from customers are preferred over those learned from peers, and these are preferred over provider routes. The motivation for an inter-domain routing protocol such as BGP is the ability for ASes to implement independent policy decisions on which routes to choose, and which routes to export to the other ASes it is connected to. In a way it is the enormous flexibility in configuration to implement various economic agreements that leads to the frequent occurrence of misconfigurations [12]. With respect to the commercial agreements the export policies have the following constraints [20]: a. AS exports only routes learned from customers and siblings to its provider, b. AS exports all learned routes to its customers and to its siblings, and c. AS exports only customer routes to its peers.

III. Related Work

We identify several categories of existing work that is related to the areas of BGP anomaly detection and prevention. One class of proposals suggest the use of cryptographic security architectures (with or without a PKI) that can be used for authenticating route announcements, and verifying the address ownership. These include the proposals for S-BGP, ASRAP, and the recently proposed Listen and Whisper mechanisms for BGP. We discuss these in III-A. Related work on identifying the hierarchy of ASes and identifying the relationships between ASes is discussed in Section III-B. Such a classification mechanism can be used for verifying the accuracy of export policies applied by ASes. Other work in identifying false announcements either in terms of address ownership or AS connectivity has been suggested, and we discuss these solutions in III-C. We present some of the analysis and results from one of the earliest attempts at quantifying the occurrences and impact of BGP misconfigurations in III-D. There has been recent work towards providing formal models of inter domain routing and verifying the configuration of routers to check if the configuration matches the desired policy. These are presented in III-E.

A. Security Mechanisms for BGP

Kent et. al. [5] describe S-BGP architecture which uses PKI infrastructure, a new path attribute containing attestation and IPSec to address most of the security vulnerabilities of BGP. Certificates are used for identifying an AS, identifying a BGP speaker, and identifying and authorizing a BGP peer. S-BGP uses attestations to establish the fact that the subject of the attestation (an AS) is authorized by the issuer of the attestation to advertise a route to a prefix. Address attestation, route attestation and certificates are used by the routers to validate the routes advertised in UPDATE messages i.e. the first AS in the route is authorized by the owner of the prefix to advertise the route and any AS in the route is authorized by the preceding AS to advertise the route to the prefix. These attestations protect BGP from misconfigurations in local policy and malicious BGP speakers. S-BGP does not address the issues of suppression of BGP messages by a misbehaving router, passive wiretapping to discover network connectivity, reasserting a route that was previously withdrawn, and verification that the BGP speakers have correctly applied the local policies.

Goodell et al. [24] propose ASRAP (autonomous system routing authority protocol) which does not require modifying the existing protocol and can be deployed incrementally. The proposed inter-domain routing validation (IRV) architecture allows ASes to acquire and validate both static (e.g. policy) and dynamic (UPDATE messages) routing information. Each participating AS runs an Interdomain Routing Validator which other ASes can query to acquire and validate routing information. Success of IRV depends on each AS running an IRV service without receiving any obvious benefits initially.

In a recent proposal, Lakshminarayanan et al. [6] describe the “Listen and Whisper” mechanisms that can be used to eliminate large number of misconfiguration problems and limit, though not completely eliminate, the damage caused by deliberate attacks on BGP infrastructure. Listen protocol passively monitors TCP flows to detect reachability problems in the data plane. Whisper protocol, which works in the control plane, introduces a signature field in UPDATE messages and can identify invalid route advertisements either due to misconfiguration or isolated adversary with either a fake AS path or tampered AS path. The proposal suggests a minor modification to BGP policy to include penalty based filtering of routes which in combination with Whisper can restrict the damage caused by colluding adversaries.

Ng et al. [25] propose secure origin BGP (soBGP) where the origin of any BGP advertisement can be verified and authenticated, preventing origin advertisement by unauthorized ASes. soBGP also ensures that the final destination in an advertised path is actually within the AS to which the packets are routed. soBGP uses certificates and a new SECURITY message to carry security information within the BGP protocol and ensure above properties.

B. Classification of AS relationships and AS hierarchy

In [7] Gao presents a novel heuristic for inferring the relationships between ASes, by identifying the transit characteristics of the routes obtained from the public RouteViews server. The technique involves a three-phase algorithm, where in the first stage the AS degrees are identified. In the second phase each AS path in the route dump is analyzed, and the "uphill" path identified as terminating with the AS number with the highest degree in that path. Transit relationships are assigned between adjacent AS numbers, where transit(A,B) implies that A acts as a transit point for traffic from B to some destination prefix. The final phase identifies peering relationships, assuming that the peering link in the path occurs at the AS with the maximum degree. The relationship between two ASes X and Y is determined to be one of the following:

- *Provider-to-Customer* relationship if transit(X,Y) = true and transit(Y,X) =false.
- *Sibling* relationship if transit(X,Y) = transit(Y,X) = true. The sibling relationship represents either the merger of AS domains, or mutual transit agreements between small ISPs to improve the customer performance.
- *Peer-to-Peer* if the degrees of the two ASes are not significantly different, and they transit traffic for each other.

Agarwal et al. present in [17] a different approach for classifying the relationships between ASes using data gathered from multiple vantage points. They present the notion of a graph theoretic problem they define as the TOR problem, which can be viewed as an optimization problem that minimizes the number of valley free anomalies, when the edges are labeled as (-1), (0), or (1). The key idea in their approach is that the uphill path from a given vantage point shows lesser variation than the downhill path. Therefore one can rank ASes by considering the position in the tree of AS paths as viewed from the vantage point. The relationship between ASes is identified based on the ranks observed from the different vantage points. The heuristic used to compare the ranks is based on identifying whether AS x dominates AS y, i.e., does AS x have a higher rank in a majority of the datasets. The paper also presents a five-level hierarchical decomposition of the Internet hierarchy based on the ranking methodology described above.

C. Detection of False Announcements

Zhao et al [8] propose an enhancement to BGP to detect invalid routing announcement involving multiple origin ASes (MOAS). If an IP prefix has multiple origin ASes, each origin AS attaches the MOAS list to BGP messages using the optional community attribute field. Any BGP router receiving multiple route advertisements with different origin ASes for same prefix can check the validity of the origin ASes by comparing them with the MOAS list. Routers can detect false and invalid origin ASes as the MOAS list of invalid announcement won't match the MOAS list from other valid announcements. Since the Internet AS graph is highly connected, most conflicts can be detected and contained efficiently.

Kruegel et al. [4] propose a passive monitoring bases approach to detect invalid BGP route announcements using AS topology information. The suggested approach divides the ASes into core and periphery ASes based on their degree of connectivity. The periphery ASes are subdivided in to clusters with the property that the geographic distance between any two ASes in a cluster is small. A valid AS path satisfies two constraints - (1) an AS path may contain at most a single subsequence of core ASes i.e. an AS path which enters and leaves the core must not enter the core again, and (2) any pair of consecutive ASes must either belong to same cluster or be in close geographic vicinity. Any route announcement violating either of the above constraints is considered invalid.

D. BGP Misconfigurations

Mahajan et al. [1] present a quantitative study of BGP misconfigurations after analyzing routing table advertisements collected at various vantage points. The study shows that 200-1200 prefixes, equivalent to 0.2-1.0% of the global BGP table size, suffer from misconfigurations every day. Misconfigurations increased the routing update load by at least 10% in 2% of the times. Surprisingly the connectivity of the internet is very robust in the face of misconfiguration, only 4% of the misconfigurations could disrupt connectivity. The causes of misconfiguration are diverse - involuntary slips by network operators, router initialization bugs and poor understanding of configuration semantics on the part of the operators etc. Based on the observations, they propose several modifications to router and protocol design such as better user interface, tools for checking router configuration, and maintaining database consistency to limit these misconfigurations.

E. Verifying Router Configuration

BGP's design, implementation, dependence on other routing protocols such as IGP, and inability to check the consistency of route advertisements makes the protocol very difficult to reason about. Feamster et al. [12] propose a routing logic which can be used to determine whether a routing protocol like BGP satisfies various properties. The different properties of interests are validity, visibility, safety, determinism, and information-flow control. For each of the property, they define a set of minimal rules that, when satisfied, imply that the protocol satisfies the property. This logic can be used to reason about BGP configurations and determine how router configuration affects each of the property. Feamster [13] has proposed techniques for verifying correctness of BGP operations, where the notion of correctness is based on the above described routing logic [12]. The proposal suggests combining static analysis of BGP configuration with simulation and emulation to verify the correctness of operation. In [12], Feamster et al. describe the difficulties of proving the correctness of AS path advertisements. The receiver of the advertisement can only prove that the advertiser has at least one known path to the destination advertised. The receiver can not prove that (1) the path taken by a packet to a destination is same as the path advertised, and (2) whether the chosen path is in accordance with policies of other ASes included in the path.

IV. BGP Anomalies

The disruption of wide area routing can occur either as a result of malicious route announcements or as a result of accidental misconfiguration/policy violations by network operators. Hence we believe that in the general case (assuming that the framework should be resistant to Byzantine failures) we should not distinguish between misconfiguration and malicious attacks. We can classify the set of anomalies that can occur in BGP into two broad categories: Path anomalies and Announcement anomalies. Path anomalies are the unexpected events that occur in the AS-PATH attributes, and these can be observed in the routing table dumps at BGP speakers. Such events include Path loops, Incorrect AS padding, private AS-announcements, origin AS conflicts etc. Announcement anomalies are incorrect UPDATE/WITHDRAWAL messages that can cause address de-aggregation, malformed updates, incorrect values advertised for the various BGP attributes etc. We now describe some of the possible anomalies.

- **Path Loops**: One of the fundamental motivations of a path vector protocol is the ability to prevent routing loops. The BGP specification suggests that each AS check whether its AS number is in the announced path before announcing the path to its neighbors (as defined by the policy). However it appears that a number of ASes do not implement the check either depending on upstream filtering or assuming that AS-loops do not occur. This is an explicit violation of the routing loop prevention technique. However one must note that loops in the AS path and in the actual router-level path may not have a one-to-one correspondence. There could be paths with AS loops that do not have routing loops at a forwarding level (BGP carries a next hop attribute and it is conceivable that the router next hop for the two occurrences of the same AS number are different). On a slightly different note other studies have shown that a number of routing loops are known to exist in the Internet, some as a result of transient conditions and others over longer time periods due to misconfiguration [22]. We should note that some of these loops may occur at an intra-domain level, and may not be observable as a loop in the AS-path directly.
- **Non origin AS padding** AS padding [21] is a well-known “hack” to achieve some control over the path selection of upstream domains. The basic idea is to inflate the AS-path with the AS number of the announcing AS repeated multiple times, so that the upstream ASes are led to believe that the number of AS hops to the destination is higher, and hence the preference for that path would be low. Usually origin ASes are known to implement AS padding especially when they are multi-homed to implement a primary-backup mechanism amongst the upstream providers. It is therefore unexpected that there would be AS padding at non-origin ASes in the AS-path.
- **Private AS announcements** Private AS numbers are used by large domains to divide the single AS into multiple smaller ASes connected through e-BGP, and each sub-AS is assigned a number from a designated private AS space to conserve the AS number space. As part of the specification, these private AS numbers must be removed before the route announcements are advertised to the outside world. The designated number range for private AS numbers lies between 64512 and 65535. The sheer complexity of router configurations may sometimes lead to address announcements with a private AS number.
- **Route Export Anomalies** The export policies for an AS were presented in Section II. These are necessary to ensure that the contractual obligations between domains are satisfied. Export anomalies often involve accidental leakage of routes, and incorrect announcements in violation of the policy. To recap, we note that a route learned from a provider cannot be exported to other providers or to peers, and routes learned from peers cannot be advertised to upstream providers.
- **Violations of the Valley Free property** A more general category of anomalies can be defined in terms of the “valley-free” properties of the AS-paths. The “valley-free” property arises as a result of the export configurations as stipulated by the relationships between ASes. We are aware of three notions of the valley-free property that may be observed in AS-paths.

  1) The most common notion of the valley-free property as reiterated in [17], is the fact that AS paths fall into one of two patterns $(-1)^m(1)^n$ or $(-1)^m(0)(1)^n$, with the understanding that a (-1) represents a customer-to-provider edge, (0) represents a peer-to-peer edge, and (1) represents a provider-to-customer edge.
  2) Gao [7] redefines the notion of valley free to accommodate the non-trivial number of sibling edges found in the AS-graph. The path is said to be valley-free if and only if the (1) a provider-to-customer edge is followed by only provider-to-customer or sibling-to-sibling edges, and (2) a peer-to-peer edge is followed by only provider-to-customer or sibling-to-sibling edges.
  3) In [4] the authors define another notion of valley-free routes in terms of a classification of ASes into core and periphery ASes. The observation is that any path cannot re-enter the “core” once it has left a “core” node into a “periphery” node.

- **Address Space hijacks/ Origin AS conflicts** A serious problem where malicious agents can cause Denial of Service attacks on a particular portion of the address space by announcing ownership of that address space. The problem is aggravated by the fact that many organizations employ some form of multi-homing for traffic engineering and resilience, and such arrangements are often not known to the outside world, unless the primary link fails. It is also common practice for providers to aggregate address prefixes from customers, and announce it as a single aggregated prefix to the outside world, while the customer may itself announce a subset either independently or through a backup link. It is not easy therefore to distinguish between the multi-homed customers and incorrect origin ASes for specific prefixes in the routing updates.

- **Malformed Updates** The BGP protocol specification has numerous attributes, each used to implement some policy or traffic engineering operation. It is extremely likely that a number of BGP update messages, both announcements and withdrawals are configured with incorrect values, not intended by the network operator, and some of these can actually cause routers to crash. The other type of update anomalies that can occur include address de-aggregation, which can inflate the routing tables of upstream providers unnecessarily. Certain previous studies [26] had shown that many routers do not conform to the specification and may send redundant updates.
- **Non-existent connectivity** An easy way for a malicious AS domain to cause either blackhole, DoS, or eavesdropping attacks is to advertise some false connectivity to the outside world, so that all or some traffic intended for the final destination transits through it. For example if origin A has a provider P, and if malicious attacker M wants to ensure that traffic for A transits itself, it can announce a malicious route with the path from A to P appearing to go through M.

V. Results and Analysis

In this section, we present some of the results from our analysis of the route table dumps from the RouteViews project [2], which proves that a non-trivial number of anomalies occur on a almost regular basis. We draw on the methodologies described in the existing literature and present a framework for detecting BGP anomalies in V-A. We also present some of our initial efforts at understanding why these anomalies occur. We should however note that these are mere conjectures, unless one manually queries the network operators concerned, there is no precise method to identify the root causes of such problems (even in this case some of the information may be proprietary, and in some cases as noted [1] it is often the case that the operators may be unaware of the cause of the problems themselves).

The data set we have used involves a set of routing table dumps collected from the public RouteViews server [2]. The routing tables were obtained for a week in Feb 2004. The motivation for picking a relatively new set of routing dumps was to prove that anomalies do exist even today, despite several attempts at improving the accuracy of router configurations and multiple independent studies to observe routing anomalies and the susceptibility of the BGP infrastructure. To put the observed anomalies in perspective of the extent of damage they can cause in terms of routing disruption and affecting BGP stability, we discuss some issues in Section V-H.

A. Methodology

We have implemented the analysis scripts for extracting the AS paths and advertised prefixes from the routing table dumps. We parse the AS-paths to remove any AS-padding which makes the analysis for valley free routing and identifying AS edges, and AS degrees tractable. The AS-paths are subsequently parsed to identify AS loops. We have also obtained from the CAIDA NetGeo database [1] the mapping of AS numbers to the enterprise that owns that AS number and the location (latitude, longitude, city etc) of the operations center of that AS. We have also obtained the AS-relationships classification and the AS edges from [23] for the corresponding period [2]. We implemented the *basic* algorithm defined in [7], and the AS classification strategy discussed in [4]. Based on the classification of either the ASes or the AS edges, we then encode the AS paths and identify the violations of valley-free routes as described earlier. The other components of our analysis toolkit involve extracting the directed AS-AS edges from the AS-paths, identifying the degree of each AS, identifying the distances between the ASes when they have a direct edge, identifying the edge type on which non-origin padding occurs, and identifying private AS number announcements. We present a summary of the overall findings in I.

TABLE I
Summary of main observations

Day	Total-paths	Loops	Prepending
24	7611257	9049	380623
25	7622968	9068	379256
26	7755401	8743	391656
27	7764638	5858	393241
28	7762127	5622	387191

B. AS-loops

A fairly surprising observation we found was that there were a non-trivial number of AS-path loops that were present in the route dumps. Further these loops seem to occur over fairly long durations and are present in a significant number of paths. We tried to analyze the reason why AS-loops occurred and we have the following conjectures. Table II presents a summary of the loop patterns we observed, our conjectures on why these occur and the persistence of the patterns across routing tables on different days.

1) A domain attempts to do AS padding, but the operator has mistyped the AS number and the AS path appears to contain a loop. A fair number of AS-loops fall under this category. We believe they are typos, because the lexical distance between the AS numbers is often less than 2, and there doesn't appear to be any scope of a commercial agreement between the AS numbers involved [3]. Examples include 12390-21390-12390, 22894-22849-22894, and 30495-30405-30495. These typos may not cause significant route disruption as the next hop attribute is usually well defined in this case to be a unique router IP.

[1] We independently implemented tools to automatically extract the AS information from the whois databases, but found this dataset later. We also note that whois entries tend to be unstructured and hard to parse, it may be worth an effort to standardize the outputs of the different whois servers.

[2] The actual results for Feb. 2004 were not available, so we approximate using the Jan. 2004 dataset

[3] Typically these are small ASes (identified by their degree) which are geographically very far apart

TABLE II

SUMMARY OF LOOP PATTERNS AND THEIR CONJECTURED CAUSES

Pattern	Day 24	25	26	27	28	Cause
30284 68 30284	6	6	9	9	9	Customer
11423 2152 11423	152	157	157	157	156	Unknown
30495 30405 30495	15	15	16	16	16	Typo
22894 22849 22894	7	7	7	7	7	Typo
4802 1221 4802	20	20	20	6	20	Unknown
16631 174 174 174 16631	5479	5440	5135	3218	3217	Sibling
7927 6505 7927	180	183	186	201	0	Sibling
30285 68 30285	23	23	23	23	23	Customer
16631 174 174 16631	2869	2916	2897	2077	2082	Sibling
1 3356 1	196	193	183	14	20	Sibling
17184 17814 17184	57	57	58	58	0	Typo
12390 21390 12390	8	8	8	10	10	Typo
766 288 766	53	54	55	55	55	Unknown
21390 12390 12390 12390 21390	4	4	4	5	5	Typo
21287 21278 21287	0	0	5	12	12	Typo

2) Another common loop pattern occurs when there is a sibling relationship between two AS numbers. An interesting example is the 16631-174-16631 case, which predominantly occurs in a number of loops. It appeared to be two different ASes 16631 (Cogent) and 174(Psinet), but the *whois* entries were subsequently updated to indicate that 174 was indeed merged with Cogent, and the loop occurs as a result of some traffic engineering within the merged domain. Another example that falls under this category is 1-3356-1, which appears to be between Level3 and Genuity, but we came across a press release that announced the merger of the two providers.
3) A third case where loops occurred was due to some enterprise using BGP to ensure reachability across locations. An example of this is 30285-68-30285, but it is still unclear why this route was being announced if it was meant to ensure connectivity across enterprise locations.
4) There are still quite a few AS loops that are unexplained. One possible explanation as suggested in [18] is the fact that may ASes seem to artificially inject loops by picking an AS already seen in the path and appending it to the AS-path (possibly for some traffic engineering or to prevent upstream ASes from using the route).

A disturbing fact we learned [4] is that most routers have mechanisms to avoid paths with AS-loops, while selecting the best paths. The very fact that the RouteViews learns many routes with AS-loops implies that the loop-checking mechanism failed at some downstream router, and went unnoticed through multiple domains. We learned that since it is a costly operation to check for loops while accepting route UPDATES, most router implementations postpone the route-loop check until the best-path selection process, and use only loop-free paths. While this is understandable, our observations indicate that the loop-checking during path selection is either turned off by some operators or the implementation is itself faulty.

C. AS-padding

We observed that many ASes in fact perform non-origin AS padding to affect the route selection process of the upstream ASes. We analyzed these occurrences of non-origin AS padding further to analyze the set of ASes and the type of AS-AS edges on which the padding occurs. A summary of the number of ASes that are involved in non-origin prepending, and the relative frequency with which this phenomenon was observed is presented in Table III. It appears that most of the padding by non-origin ASes occurs on a customer-to-provider edge [5], which seems acceptable assuming that this is an extension of a multi-homed customer trying to implement a primary-backup association amongst its upstream providers. Also padding on a sibling edge seems acceptable as it provides a simple means of implementing some forms of traffic engineering. Another common case of an AS exhibiting non-origin padding was the case of InterNAP, which provides connectivity to enterprises by peering with Tier-1 providers. The surprising fact was that there were a number of cases where the prepending occurred at peer-to-peer edges and among provider-to-customer edges [6], and this requires further investigation.

TABLE III

NON-ORIGIN AS PADDING

Day	Prepending	P2C	C2P	P2P	SIBLING	Last-hop
24	380623	39839	295797	8330	30282	6375
25	379256	39740	293631	8448	31079	6358
26	391656	40282	295979	8483	40472	6440
27	393241	43093	297481	8913	37193	6561
28	387191	39432	294524	8943	38312	5980

D. Private AS-announcements

As per the specification private AS numbers should not be exported to the outside world, but due to router mis-

[4] We thank Jibin Zhan for providing useful information on common practices

[5] Since we believe that Gao's analysis yields the most accurate AS relationship we used the inferred relationship from this analysis model

[6] Though the classification mechanism may itself be faulty, we believe that some of these edges are provider-to-customer edges with very high probability for example when a Tier-1 provider like ATT (7018) is involved

configuration this seems to be a fairly common occurrence. We analyzed the number of private addresses present, the relative frequencies with which the announcements occur, and the number of ASes that are involved in such accidental misconfiguration. Surprisingly many of these announcements are found to persist across all the five days. We believe that these do not hold significant potential for exploits by malicious attackers or causing route disruption, but it is a definite anomaly that is in violation of the specifications and could allow leakage of otherwise proprietary information. Over the route-dumps that we analyzed, we found that between 38-45 directed AS-AS edges involved private AS numbers. There were 34 distinct private AS numbers that were observed, out of which 28 were observed over all 5 days, and 2 each were observed for 1, 2, and 4 days.

E. Violations of Valley Free Routing

A large category of anomalies can be observed by considering the valley-free property of BGP routes. Most of the violations of the valley free property are artifacts of export misconfiguration at routers, that causes accidental leakage of routes, and subsequent violation of the valley free property. We presented the three models for identifying the valley-free violations in AS paths as suggested by [7], [17], and [4]. Table IV presents a comparison of the number of AS paths that violate the valley free property as defined by the three independent studies. According to the analysis in [7] and [17], there are four distinct patterns that can cause violations of the valley-free property:

1) A peer-to-peer edge followed by another peer-to-peer edge (*P2P-P2P*). This indicates an AS incorrectly exports routes learned from one peer to another. The definition of peering from [19] suggests that the routes learned from peers can only be exported to customers.
2) A provider-to-customer edge followed by a customer-to-provider edge (*P2C-C2P*). This can arise when a multi-homed AS starts to transit traffic between its upstream providers, as it exports routes learned from one provider to another.
3) A peer-to-peer edge followed by a customer-to-provider edge (*P2P-C2P*). Here the AS exports routes learned from its peer to its provider.
4) A provider-to-customer edge followed by a peer-to-peer edge (*P2C-P2P*), where the AS leaks routes learned from a provider to its peer.

We observe that Gao's analysis finds the least number of violations, and we believe this is because of two main reasons 1. the notion of a sibling relationship, and 2. the fact that Gao's analysis tends to do some form of data-fitting better than the other two. We also performed a breakup of the types of anomalies for Gao's and Agarwal's analysis, which is instructive as we can observe the common cases of import-export misconfiguration and also understand the weaknesses of each classification mechanism. The breakdown of the anomalies into the 4 categories described above indicates that in Agarwal's analysis a major portion (greater than 70%) arises from the P2P-P2P pattern, mostly because the notion of sibling relationship is absent, while in Gao's analysis a major portion (greater than 90%) arises from the P2C-P2P pattern.

We investigated the valley-free violations further using the fact that (1) Gao's analysis is heavily dependent on accurate estimates of AS degree to assign transit relationships, (2) the core-periphery classification can benefit from more accurate AS topology information, and (3) the three classification and valley free violation detection mechanisms are fairly independent. For (1) we tried to repeat Gao's analysis using the degree distribution from the data set from [23] [7], but we observed that the number of violations did not change significantly (we do not present these results here for brevity). As in (1), we used the set of edges observed from [23] to infer the AS topology, and perform the classification to identify anomalies. The number of violations observed were similar to the RouteViews data set and we do not present these here [8]. A corollary of (3) yields the observation that valley free violations that occur in two or more of the analysis methodologies are likely to be more accurate estimators of actual export violations. Table IV also presents the number of anomalous paths that occurred in at least two of the detection mechanisms. We believe that it is useful to further investigate these anomalous patterns [9].

TABLE IV
VALLEY FREE ANOMALIES

Day	Distinct Paths	Gao	Agarwal	Kruegel	Common
24	998280	2280	91814	8082	812
25	998471	2259	91276	8184	816
26	1004860	1395	91708	8256	801
27	1004320	1257	89905	8181	757
28	1002524	1167	89926	8142	760

F. Identifying false links in the AS graph

It is a common observation that small ISPs or enterprises, have one or two upstream providers, and do not generally peer or have a forwarding agreement with other providers. When they do peer with other small ISPs or enterprises it is extremely unlikely that these ISPs are geographically very far apart. We have modified the methodology presented in [4] to identify the periphery ASes and consider any directed edge between periphery ASes that are geographically distant to be invalid. Table V presents the number of invalid links found in the route dumps for different values of a threshold distance in kilometers (beyond which the connectivity is deemed invalid). This method has a number of drawbacks as 1. it does not identify anomalous links between core nodes, or between core and periphery nodes, 2. it is tightly coupled to the classification methodology, 3. it does not take into account the geographical spread of the AS, rather we consider only the central office

[7] We believed that the data from the multiple vantage points would yield a more accurate degree distribution than the RouteViews data which is heavily biased towards North American providers.

[8] As an aside, these observations seem to indicate that either RouteViews "sees" a significant number of ASes and their interconnection or the data set from the multiple vantage points is not diverse enough

[9] A preliminary investigation suggests many of the common anomalies arise from a few common patterns

location information from the *whois* registries. Having noted the drawbacks we feel that this method can however be used to corroborate any anomalous events that we observe, and is a useful tool for confirming observations (for example to convince ourselves that the "typo" loops were actually typos we investigated the geographical distance between the AS numbers part of the loop, and found that in a majority of the cases the link was declared as invalid by this methodology). For example for the pattern 22894-22849, the distance between the two ASes is greater than 5000 km, and in the 21278-21287 pattern the ASes belong to vastly distant places (Moscow and Algeria) [10].

TABLE V
GEOGRAPHICALLY INVALID LINKS

Day	300	400	500
24	1343	1302	1285
25	1341	1298	1280
26	1341	1298	1280
27	1339	1297	1279
28	1300	1300	1282

G. *Origin AS conflicts*

Previous work [8] has analyzed the extent of origin AS conflicts and suggested mechanisms to distinguish multi-homed ASes from hijack attempts. Table VI confirms the findings, and we observe that a number of prefixes are multi-homed. However one caveat is that a number of these prefixes actually appear to be part of a larger address block that was de-aggregated for some reason, so these results may be an overestimate of the actual extent of origin-AS conflicts.

TABLE VI
ORIGIN AS CONFLICTS

Day	Number of prefixes
24	1455
25	1456
26	1481
27	1467
28	1475

H. *Impact of Anomalies on Routing and Stability*

To analyze the extent of disruption that the anomalies could cause we analyzed then number of prepending, loop, and valley-free anomalies that occur among the best-paths in the routing table. While the fact remains that the only reason these paths are found in the routedumps are because some router decided that this was the best path it possessed to some prefix, it is quite possible that many of the anomalous routes get filtered out upstream. As observed in Table VII we see that many of the observed anomalies occur only in non-optimal paths, and the best path to any prefix does not appear to have any significant number of loops or violations of the valley-free property. The extent of non-origin AS-prepending is also significantly less, when all paths were considered 50% of the paths had non-origin AS prepending while less than 2% seem to have AS-padding in the best paths. [11]

TABLE VII
ANOMALIES IN THE BEST PATHS

Day	Number of prefixes	Loops	Prepending	Valley-Free (Gao)
24	151700	4	1582	11
25	151940	5	1712	11
26	152071	5	1771	11
27	152240	5	1272	1
28	152195	1	1230	1

VI. TOWARDS A BETTER BGP

If one were to design a new interdomain routing infrastructure, what properties should the new framework have? In this Section, we attempt to answer this question based on our observation and quantification of BGP anomalies as described in the previous Sections.

- The receiver of a routing advertisement should be able to verify the ownership of the IP prefix advertised i.e. the origin AS in the advertisement is authorized to advertise the prefix by the owner. This would prevent the problems of address hijacking and origin AS conflicts. Both S-BGP [5] and soBGP [25] proposals guarantee this property through the use of PKI. Zhao et al.'s proposal [8] uses the community attribute of BGP to attach the MOAS list to BGP announcements, which the receiver can use to detect invalid announcements.
- The receiver of the routing advertisement should be able to verify that (1) the AS advertising the path does actually have a path to the destination , (2) the path taken by packets to the destination is same as the advertised path, and (3) the advertised path is in accordance with the local policies of the ASes included in the path. The first and second properties would prevent blackhole attacks and traffic hijacking, whereas the third property would help identify policy violation such as detection of the violation of valley free routing. These properties would also help in detecting anomalies arising out of misconfiguration. The soBGP [25] proposal guarantees the first property. Feamster et al. [11] show that a path vector protocol like BGP can not guarantee the last two of the desired properties, hence we need to look beyond BGP in order to achieve them.
- The routing framework should include a high-level language for specifying router policies and configuration files. Currently the router configuration files have no standardized format and language, which makes it difficult to extract and analyze information from the router

[10] Some of these were verified manually as the latitude-longitude database from NetGeo has inherent flaws, as some entries were missing or had wrong locations reported

[11] We should note however that the best paths are considered from the perspective of the RouteViews peering router, which observes a much richer topology than most points on the Internet, and is likely to have a much wider range of routing choices for each destination.

configuration files in an efficient and accurate manner. A standard language for configuration files would make the life of network operators lot more easier. The framework should also include a better human interface (GUI, analysis tools etc) to routers and router configuration files, as suggested by Mahajan et al. [1] in their analysis of BGP misconfiguration.

- The network operator should be able to verify the correctness of router configuration and local policies. This would prevent many of the misconfiguration problem seen in BGP today. BGP's distributed nature can cause small misconfigurations to give rise to complex errors affecting global connectivity. The state-of-the-art in reasoning about BGP's behavior is to observe the effect of the configuration on a live network. The routing framework should include a formal model to reason about BGP's behavior on different router configurations. Feamster et al [12] propose a routing logic to reason about BGP configurations. Feamster [13] proposes a way of verifying router configuration files by combining static analysis techniques with simulation and emulation.
- The routing framework should include standardized "best practices" guidelines for router configuration and traffic engineering. From our observations it appears that AS-padding seems to be a predominant method to achieve traffic engineering even if there are other BGP attributes to achieve the same. A good understanding of practices would enable faster detection and also help lower false alarms in anomaly detectors.
- Every participating entity in the routing infrastructure should have the full knowledge of AS connectivity. This knowledge would enable them in detecting invalid route announcements. In soBGP [25] every AS publishes the list of its peers, which is used to build a topology map of the paths of the entire network. In the absence of such information in the current infrastructure, that have been attempts ([7], [17], [2] etc.) to understand the AS connectivity graph.
- The framework should have provisions for authenticating and authorizing every participating entity. Every participating entity should be able to identify who the other participants are and what information they are authorized to advertise. The framework should also guarantee the integrity of messages exchanged between these entities. The S-BGP [5] and soBGP [25] proposals include steps in this direction.
- The participating entities should be able to contain suspicious behavior of malicious and misconfigured entities i.e. the entities should not propagate any routing advertisement to their neighbors if they suspect the advertiser to be misconfigured or malicious. This would limit the amount of damage caused by misconfiguration and malicious attacks. The Listen-Whisper protocol [6] and the IRV protocol [24] include mechanisms which the BGP speakers can use to prevent the propagation of suspicious routing announcements.
- In the current BGP framework, the BGP speakers have non-trivial amount of trust on their neighbors. Every router trusts its neighboring routers to apply their local policy correctly, and accepts routing advertisements from them without suspecting misconfiguration or malicious nature. The new framework should reduce the amount of trust on upstream filtering and introduce local filtering to detect anomalies. Various anomaly detection techniques ([7], [17], [4], [8]) can be used locally to filter out invalid and malicious routing announcements.
- The routing infrastructure should be physically secure to prevent the compromise of participating entities. Many of the proposals of securing BGP would fail to work if the router is compromised.
- The routing framework should include financial models for cost distribution across multiple service providers. Economic considerations such as transit relationship, peering relationship and customer-provider relationship are fundamental part of the infrastructure and hence should be included in the specification of the framework. Also temporary arrangements between service providers and customers, and per-prefix arrangements between ASes need to be modeled in the policy specification framework.

VII. Conclusions

We have identified some of the BGP AS-path level anomalies and quantified them by looking at the routing table data available at the RouteViews [2] project. We have suggested a set of required properties of a robust routing infrastructure in order to prevent these anomalies. Most of the anomalies identified appear to be benign, nevertheless they have the potential for malicious exploits. More work needs to be done in order to understand the root cause of the anomalies and to prevent them from happening. We hope to obtain some more information on some of our observations from network operators and the NANOG mailing list. Below we describe the caveats of our work and suggest some directions for future work in this area.

A. Caveats

- In quantifying the BGP anomalies, we looked at the information available in the route table and not the route announcements. Hence it is quite likely that we underestimated the anomalies. Our work looks at only path level anomalies and not malformed updates or anomalies in route announcements. Another possible source of routing anomalies can occur as a result of mismatches in the policy in the control plane (AS-path), and the actual data forwarding path [18], we do not have techniques for identifying these.
- The routing table dumps at RouteViews are collected every two hours. We looked at one set of routing table dumps for each of the five days. All misconfigurations may not have showed up due to the insufficiency and granularity of the dataset we have looked at and we may have missed longer term anomalies (and in particular notion of persistence of the anomalies, which gives some

idea of how long it took the network operator to have observed and fixed the problem).

- The anomalies identified may be benign in nature and may have very little impact on actual routing performance, and this is to a certain extent confirmed by the observations in Section V-H. Also a study by Rexford et al. [27] shows that the routes to most popular destinations are stable, and as a result a majority of Internet traffic may not be affected by route fluctuations and misconfigurations.
- The classification methodologies used for identifying the different types of AS relationship possess inherent inaccuracies, and are incapable of modeling AS relationships at finer granularity. It appears that the Internet community is moving towards an economic relationship model that is based on the address prefix ranges as opposed to on a AS-level, and new work needs to be done to understand these fine-grained relationships.
- We have not been able to accurately point out the root causes of various anomalies. We have not correlated various observed events with routing changes, policy changes, real events (e.g. merger of ISPs) etc.

B. Future Work

Even though there is a lot of existing literature in the areas of BGP, routing security, and the development of better interfaces for operators to routers and configuration languages, we feel that there are multiple avenues for future work. One dimension would be to persist with the data analysis for a longer term, and observe a wider range of anomalies, and also evaluate the remedy times for the mistakes to be fixed. It would also be interesting to further analyze the risks presented by the observed anomalies. A very interesting direction of research in the routing community is towards "root-cause analysis", which aims at identifying the true source of an anomalous event, which can help in precluding future events of a similar kind. We also believe that there is promise in the area of topology inference either using the geographical properties of Internet routing [28], [30] or by observing the update dynamics [29], that can help to understand the relationships between ASes better. We also feel that there are two components that are missing in the current framework for policy specification and implementation: the need to integrate an economic model into BGP policy specification, and the need for formal verification tools to automate the process of policy setting and validation.

ACKNOWLEDGMENTS

We would like to thank the RouteViews project and Sharad Agarwal for making their data available, without which this project would have been infeasible. We thank Jennifer Rexford, Albert Greenberg and Hui Zhang for suggesting the problem. Finally we would like to thank Aditya Akella for the insightful discussions and guidance throughout this project.

REFERENCES

[1] Ratul Mahajan, David Wetherall, and Tom Anderson. "Understanding BGP Misconfiguration ", *In Proceedings of ACM SIGCOMM 2002.*

[2] RouteViews University of Oregon *www.routeviews.org*

[3] NetGeo, CAIDA *http://www.caida.org/tools/utilities/netgeo/*

[4] Christopher Kruegel, Darren Mutz, William Robertson and Fredrik Valeur. "Topology-based Detection of Anomalous BGP Messages", *In 6th Symposium on Recent Advances in Intrusion Detection (RAID), Lecture Notes in Computer Science, Springer Verlag, USA, September 2003.*

[5] S. Kent, C. Lynn, K. Seo. "Secure Border Gateway Protocol (S-BGP)", *In IEEE JSAC, Vol. 18 No. 4, April 2000, pp. 582–592.*

[6] Lakshminarayanan Subramanian, Volker Roth, Ion Stoica, Scott Shenker and Randy H. Katz. "Listen and Whisper: Security Mechanisms for BGP" , *In First Symposium on Networked Systems Design and Implementation (NSDI'04), March, 2004.*

[7] Lixin Gao, " On Inferring Autonomous System Relationships in the Internet " , in IEEE Global Internet, Nov 2000.

[8] Xiaoliang Zhao, Dan Pei, Lan Wang, Dan Massey, Allison Mankin, S. Felix Wu, Lixia Zhang. " Detection of Invalid Routing Announcement in the Internet ",*In International Conference on Dependable Systems and Networks (DSN'02).*

[9] S. Convery, D. Cook, M. Franz. "An Attack Tree for the Border Gateway Protocol" IETF Draft. *http://www.cs.unt.edu/ rdantu/An Attack Tree for the Border Gateway Protocol.htm*

[10] Sandra Murphy. "BGP Security Vulnerabilities Analysis" *http://www.ietf.org/internet-drafts/draft-ietf-idr-bgp-vuln-00.txt*

[11] R. White, B. Akyol, and N. Feamster. "Considerations in Validating the Path in Routing Protocols", *http://ietfreport.isoc.org/ids/draft-white-pathconsiderations-02.txt, IETF Draft, April 2004.*

[12] N. Feamster and H. Balakrishnan. "Towards a Logic for Wide-Area Internet Routing " *Proc. ACM SIGCOMM Workshop on Future Directions in Network Architecture 2003.*

[13] N. Feamster. "Practical Verification Techniques for Wide-Area Routing " *ACM SIGCOMM Workshop on Hot Topics in Networks (HotNets-II), November 2003.*

[14] J. Farrar. "C&W Routing Instability", *http://www.merit.edu/mail.archives/nanog/2001-04/msg00209.html*

[15] V. J. Bono. "7007 Explanation and apology" *http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html*

[16] Y. Rekhter and T. Li. "A Border Gateway Protocol 4 (BGP-4)", *RFC 1771, March 1995.*

[17] Lakshminarayanan Subramanian, Sharad Agarwal, Jennifer Rexford and Randy H.Katz. "Characterizing the Internet Hierarchy from Multiple Vantage Points." *In IEEE INFOCOM 2002 , New York, June 2002.*

[18] Zhouqing Morley Mao, Jennifer Rexford, Jia Wang, and Randy Katz. " Towards an Accurate AS-Level Traceroute Tool, " ,*In Proceedings of ACM SIGCOMM 2003.*

[19] W. B. Norton. "Internet Service Providers and Peering ", *http://www.equinix.com/press/whtppr.htm*

[20] G. Houston. "Interconnection, Peering, and Settlements", *In Proceedings of INET, June 1999.*

[21] Timothy G. Griffin, "An Introduction to Interdomain Routing and BGP", *ACM SIGCOMM 2001 Tutorial Session.*

[22] V. Paxson. "End-to-End Routing Behavior in the Internet", *In Proceedings of ACM SIGCOMM '96, August 1996.*

[23] *http://www.cs.berkeley.edu/ sagarwal/research/BGP-hierarchy/*

[24] Geoffrey Goodell, William Aiello, Timothy Griffin, John Ioannidis, Patrick McDaniel, and Aviel Rubin. "Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing", *In Symposium on Network and Distributed Systems Security, February 2003.*

[25] James Ng(editor). "Extensions to BGP to Support Secure Origin BGP (soBGP)", *http://ietfreport.isoc.org/ids/draft-ng-sobgp-bgp-extensions-02.txt, IETF Draft, April 2004.*

[26] C. Labovitz, G. R. Malan, and F. Jahanian. "Internet Routing Instability", *Proceedings of SIGCOMM'97, September 1997.*

[27] Jennifer Rexford, Jia Wang, Zhen Xiao, Yin Zhang, "BGP Routing Stability of Popular Destinations " in *ACM SIGCOMM IMW (Internet Measurement Workshop) 2002.*

[28] Lakshminarayanan Subramanian, Venkata N. Padmanabhan and Randy H. Katz. " Geographic Properties of Internet Routing ", *USENIX Annual Technical Conference, Monterey , CA, June 2002.*

[29] D. Andersen, N. Feamster, S. Bauer, and H. Balakrishnan. "Topology Inference from BGP Routing Dynamics", *In Proceedings of SIGCOMM Internet Measurement Workshop 2002, Marseille, France, November 2002.*

[30] T. S. Eugene Ng and Hui Zhang. "Predicting Internet Network Distance with Coordinates-Based Approaches", *INFOCOM'02, New York, NY, June 2002.*