Analysis of Propagation of Regular, Extended, and Large BGP Communities

Lilia Hannachi and Kotikalapudi Sriram, Fellow, IEEE
National Institute of Standards and Technology
Maryland, US
{lilia.hannachi; ksriram}@nist.gov

***Abstract*—This study focuses on the analysis of propagation of Regular, Extended, and Large Communities in the Border Gateway Protocol (BGP). Once added, these communities are often intended to be transitive by default meaning that they should be propagated transitively from one autonomous system (AS) to the next in the propagation path of BGP Update messages. There are evolving solutions in the IETF for route leak detection, DDoS mitigation, and other applications that use these Communities, and depend on the transitivity to work at least over a few AS hops. Relative to prior studies, this paper attempts to significantly advance the accuracy in measurement and analysis of the propagation behavior, especially for the Regular Communities. This is accomplished by performing the measurements against known applications. This work also provides measurements on the propagation of Extended and Large Communities which have not been studied before to the best of our knowledge. These propagation measurements and analyses throw light on whether these communities adequately propagate to benefit evolving applications and also whether they propagate beyond their intended scope thus reflecting poor hygiene and clutter on the Internet control plane.**

***Index Terms*—BGP, BGP Community, Measurement, Analysis, Regular Community, Extended Community, Large Community**

I. Introduction

Currently, three types of Border Gateway Protocol (BGP) communities have been standardized by the Internet Engineering Task Force (IETF). One is simply called Community [11] but we often refer to it as Regular Community (RC) in this paper to clearly distinguish it from the other two types. The other two are called Extended Community (EC) [7]-[10] and Large Community (LC) [12]. In the rest of this document, in many instances, the three types of communities will be simply referred to by their abbreviated names, i.e., RC, EC, and LC. These communities are used to share application-specific policy information between autonomous systems (ASes). For example, information about peering relations is encoded and signaled using the LCs in an evolving IETF standard for route-leak detection and mitigation [14]. ECs are proposed to be used in an evolving Flowspec 2.0 specification [15] that facilitates DoS/DDoS mitigation. These Internet security solutions depend on the transitivity of the LCs and ECs to work at least over a few AS hops.

This study focuses on the analysis of propagation characteristics of the communities of all three types. Once added, these communities are intended to be transitive by default meaning that they should be propagated transitively from one AS to the next in the propagation path of BGP Update messages. However, there are variations in how network operators view and treat BGP communities. Relative to prior studies [1] [2], this paper attempts to advance the accuracy in measurement and analysis of the propagation behavior, especially for the Regular Communities. This is accomplished by performing the measurements against specific known applications. The need for this was expressed in IETF working groups [18]. Focusing on those applications, it is possible to know the expected behavior of propagation and the measurements can be performed against that. There is strong interest in the IETF Inter-domain Routing (IDR) and Global Routing Operations (GROW) working groups about the propagation behaviors of LC and EC [16] [17]. So, our study also provides measurements on the propagation of Extended and Large Communities. (To the best of our knowledge, measurements of ECs and LCs have not been published before in existing literature except for our presentation of a very preliminary version of this work in an IETF meeting [17]; it was only a slide presentation.) These propagation measurements throw light on whether these communities propagate adequately to benefit the applications they serve. We study also whether they propagate beyond their intended scope thus possibly reflecting poor hygiene and clutter on the Internet control plane. For example, Blackhole Communities (which are examples of RC) used for remote triggered blackhole (RTBH) service must propagate up to the RTBH provider AS but not beyond that. The topic of Blackhole Community propagation was studied before in [1] [2] but our study probes further and aims to provide additional insights. The overall results in this paper should be helpful for people in R&D and standards development organizations (SDOs) working on future Internet routing protocols and applications that utilize BGP communities (RC, EC, or LC).

II. Data Collection and Measurement Methodology

The results presented in this paper are derived from detailed analyses of the historic BGP Update datasets from the RIPE Routing Information Service (RIPE-RIS) [3]. The Routeviews [4] data was also used for additional analyses and cross-checking our results, but those results are not shared here due to limitation of space. We downloaded all Updates from RIPE-RIS generated on July 15, 2021, from collector RRC03 (one file every 5 minutes). In total, we have 288 files with more than 19 GBytes of data consisting of over 52 million BGP Updates (trace data). In this study, we focused on updates with community attributes. This includes all three BGP community types (RC, EC, and LC). The RC communities can be used for Blackholing services or other purposes. To identify Blackhole

Communities (BCs), we used a process similar to that presented in [2]. We started by generating the whole list of unique RCs from the BGP Update data. Then, for each ASN (i.e., Community ID) in each RC, we searched its record either from the well-documented communities in Internet Routing Registry (IRR) (we use the IRR records in Merit RADb [5]) or from AS's (or ISP's) Web page (e.g., [19] to [26]). BCs are identified by searching with keywords such as 'blackhole' or 'null route'. To identify other Regular Communities (RCs) that are not Blackhole, we searched with keywords such as 'customer', 'peer', 'non-customer', etc. In addition, we also searched for keywords that specifically indicate that the RCs are indeed propagated to customers. This allows us to identify RCs that are intentionally propagated to customers rather than used only internally within the AS. By making this extra effort (compared to previous studies [1] [2]), it is possible to measure the propagation of RCs against known applications where propagation is required. The measurement methods applied for EC and LC will be described in later sections while presenting the results.

III. High-Level Statistics of Regular, Extended, and Large Communities

Table I provides high-level statistics related to the measurements of RCs, ECs, and LCs. The reported results were obtained from the analysis of a total of over 52M Updates from RIPE-RIS (see Section II). The table is organized into seven parts. In the top four parts, the measurements are provided for each of the community types (RC, EC, LC) in terms of the #unique routes (i.e., {Prefix, Path, community} triples), #unique routes with Absent AS (i.e., ASN in the community (or global) ID is absent in the AS path), #unique{Prefix, community} pairs, and the #unique communities. Some distinctions are also made in the presented measurements, e.g., between transitive 2-octet AS EC and transitive 4-octet AS EC [9]. The non-transitive EC is not mentioned in the table because we observed zero such ECs. This transitive/non-transitive distinction does not exist for RCs and LCs at present (per IANA registrations). The table also shows that a total of 3,872 ASes (out of a total of about 70K ASes) propagate RC, EC, or LC. This is in the sense that these ASes appeared in a path segment in a BGP Update through which a community (of any type) has propagated. We also observe that 22 (out of a total of 24 [27]) Tier-1 ASes propagate RC, EC, or LC. Measurements on some miscellaneous RCs are reported as well. These include, for example, 0:0 which is known as 'Internet community' meant to signal that the RC should propagate without being stripped. The data reported in the last part of Table I related to Blackhole Communities will be discussed in more detail in Section IV-A.

TABLE I: High-Level Statistics of Regular, Extended, and Large Communities.

# Updates (raw)	52,765,351
RC, EC, LC Statistics	
Unique routes	
# Unique {Prefix, Path, RC}	69,643,850
# Unique {Prefix, Path, Transitive EC}	1,143,809
# Unique {Prefix, Path, Transitive 2-Octet AS EC}	826,575
# Unique {Prefix, Path, Transitive 4-Octet AS EC}	98,507
# Unique {Prefix, Path, LC}	12,802,541
# Unique {Prefix, Path, LC} LC with Global ID = 0	12
Absent: ASN in Comm. ID is Absent in AS path	
# Unique {Prefix, Transitive RC} with Absent AS	16,539,684
# Unique {Prefix, Transitive EC} with Absent AS	313,147
# Unique {Prefix, Transitive LC} with Absent AS	4,366,977
Unique {Prefix, community} pairs	
# Unique {Prefix, RC}	40,431,120
# Unique {Prefix, Transitive EC}	518,532
# Unique {Prefix, Transitive 2-Octet AS EC}	496,517
# Unique {Prefix, Transitive 4-Octet AS EC}	22,015
# Unique {Prefix, LC}	5,725,244
Unique community	
# Unique RC	49,782
# Unique Transitive EC	2,659
# Unique Non-Transitive EC	0
# Unique LC	2,363
Propagating Autonomous Systems	
# ASes that Propagate RC (at least once)	3,298
# ASes that Propagate LC (at least once)	262
# ASes that Propagate EC (at least once)	527
# ASes that Propagate RC or LC or EC	3,872
# Tier-1 ASes that Propagate RC or LC or EC	22
Miscellaneous	
# Unique {Prefix, Path, RC=Any:666}	264,557
# Unique {Prefix, Path, RC = 0:0}	18,583
# Unique {Prefix, Path, RC=0:Any}	10,293,308
# Unique {Prefix, Path, RC=Any:65535}	195,462
Blackhole Community (BC)	
# Unique BC	21
# Unique {Prefix, BC}	876
# Unique {Prefix, Path, BC}	2,512
# Unique {Prefix, Path, BC} 65535:666 WKC	21
# Unique BC (ASN:666 Blackhole)	9
# Unique BC (ASN:not-666 Blackhole)	12
# Unique RC (ASN:666 that are not Blackhole)	4

IV. Analysis of Regular Communities

Signaling a Blackhole request using a Blackhole Community (BC) is an application of the Regular Community (RC). Other applications of RC include signaling customer or peer routes in Update messages sent to customers. Here "customer routes" and "peer routes" mean the routes learned from customers and those learned from lateral (i.e., non-transit) peers, respectively. Here, we report on the measurement and analysis of BCs (Section IV-A) as well as other RCs corresponding to applications such as signaling a customer or peer (Section IV-B).

A. Blackhole Communities

Blackhole Community (BC) of the form ASN:x is used to request Remote Triggered Blackholing (RTBH) service. Here, the ASN field (2-octets size) is called the Community ID and is typically the ASN that offers the Blackholing service, and the value of x denotes Blackholing request. Many operators use x = 666 for BC. However, some operators use an x value different from 666 for BC. Examples of this are 3356:9999 (Level 3) [22], 1299:999 (Telia) [20], and 3257:2666 (GTT)[1]. Some operators use the ASN:666 community for an application other than Blackholing. For example, AS 3356 uses 3356:666 to signal a peer route [22]. So, care is needed to prepare an

[1]Certain commercial network services or operational practices are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by NIST.

accurate list of BCs. Sometimes the Well-Known Community (WKC) 65535:666 [6] is also used for BC. In such cases, when the ASN offering the RTBH is not used as the Community ID, it is not possible to determine which AS in the AS path (in the BGP Update) is the RTBH service provider. The Updates in such cases are ignored in performing the measurements on BC propagation. However, such BCs are counted and reported as 'Absent' meaning that the ASN in the Community ID of the BC is absent from the AS path (see Table I).

We assume that the origin AS in the BGP Update message attaches the BC since it originates the prefix that is under a Denial of Service (DoS) attack. (Note: Discussions on the IETF GROW list [18] have clarified that it is unusual or rare for an AS other than the origin AS to request Blackholing.) We measure the number of hops (excluding prepends) from the origin AS to the AS offering RTBH service and this metric is called #hops propagated to RTBH provider. We also measure the total number of hops propagated from the AS offering RTBH service to the last AS in the AS path. This metric is called the #hops propagated beyond the RTBH provider. When a server (or servers) in a subnet is under DoS/DDoS attack, the AS which announces the prefix can originate a route with a Blackhole Community attached. This route is usually for a more specific prefix (subsumed under the normally announced prefix) and contains the address(es) of the server(s) under attack. The route is intended to transitively propagate to an AS one or multiple hops away that offers the RTBH service. Sometimes the route only needs to propagate in iBGP within the originating AS if the egress router(s) in the originating AS happens to be the RTBH provider. In this case, the ASN in the BC matches the origin AS and the #hops to RTBH provider is counted as zero.

We believe that the distinction of the metrics '#hops propagated to RTBH provider' and '#hops propagated beyond the RTBH provider' (see above) is useful and novel (relative to [1] [2]). Note: AS prepends are eliminated in our study as well as other cited studies [1] [2] so the AS path consists of only the unique ASNs.

We created a listing of Blackhole Communities (BCs) using the Whois information from the Merit RADb [5] as well as websites maintained by networks (e.g., [19] to [26]). These websites describe the Communities that the networks use or require their customers or peers to use to facilitate various applications or services. From this search, we found a total of 214 unique BCs having the form ASN:x that fall into one of two types: (1) x is 666, and (2) x is not 666. We created lists of 96 BCs that are of Type 1 and 118 BCs that are of Type 2. As noted earlier, some networks do not use their ASN value in the BC; examples are 65535:666 (WKC per [6]), 0:666, and 0:66. These are included in our results obtained from searching Merit RADb and the web. The number of unique BCs that we found are higher than those obtained in [2]. That is expected in part because the number of networks using BCs increases over time. We looked for the presence of the BCs from the lists mentioned above in the RIPE-RIS Update data. Tables II and III list (for Type 1 and Type 2, respectively) the BCs that were observed in the RIPE-RIS Update data and the number of unique routes observed for each BC. A majority of the BCs from our Type 1 and Type 2 lists mentioned above were not observed in RIPE-RIS. Only 21 (out of the 214) were observed as listed in Tables II and III. That is considered to be good because BCs should not be quite visible to RIPE-RIS or Routeviews in large numbers. The reasons behind this are: (1) BCs are short-lived (lasting only for the DDoS mitigation period), (2) they typically propagate very few AS hops to reach RTBH provider, and (3) most BCs are associated with highly specific prefix announcements that get blocked by eBGP routers unless appropriate Blackhole route policies are in place.

TABLE II: ASN:666 that are Blackhole Communities

ASN:666 that are BC	#Unique routes
9002:666	883
8595:666	24
49544:666	24
65535:666	21
0:666	7
12714:666	2
13101:666	1
41722:666	1
21056:666	1

TABLE III: ASN:x (x $\neq$ 666) that are Blackhole Communities

ASN:x (x $\neq$ 666) that are BC	#Unique routes
0:66	724
3491:999	716
43267:9999	24
25478:9999	24
50384:6666	24
3356:9999	10
1299:999	8
3257:2666	6
33891:33890	5
31133:999	3
12389:55555	2
20485:65535	2

Table IV lists the RCs found from the IRR and websites in which ASN:666 is used for purposes other than BC, and also shows the number of unique routes observed for each. There RCs are not included in the BC analyses, and are instead included in the RC (non-Blackhole) analyses in Section IV-B. In our study of BCs, we consider only the BCs that have been declared to be BCs by the network operators (as described

TABLE IV: ASN:666 that are not Blackhole Communities

ASN:666 that are not BC	#Unique routes
3356:666	208,308
2603:666	39,170
5511:666	6,983
34145:666	1
5650:666	0
6128:666	0
7385:666	0

above). By doing so we accurately measure the propagation against the known (declared) RTBH application instances.

Fig. 1 shows the distribution (in raw numbers) of the #hops to the RTBH provider, and Fig. 2 shows the corresponding empirical cumulative density function (ECDF). The two figures also show the plots for the #hops propagated beyond the RTBH provider. The figures show that a fairly large fraction (69%) of unique routes with BCs is associated with BCs for which the ASN in the BC is absent from the AS path in the Update message. This data point is represented by 'Absent' in the plots. 'Absent' also includes the cases where the ASN in the BC is 65535 or 0. These key observations can be made about Figs. 1 and 2: (1) The number of routes with BCs seen in the wild is minuscule compared to the number of routes seen with other types of RCs (also see Table I). This bodes well because BCs are meant to propagate only to the RTBH provider(s) which are generally either zero or one hop away from the AS requesting RTBH service. Hence, collectors (of Routeviews or RIPE-RIS) should rarely catch them in the wild; (2) The distribution of #hops propagated to RTBH provider has most of its mass at either zero or one hop; and (3) The distribution of #hops propagated beyond RTBH provider has most of its mass at one and two. All three observations indicate reasonably satisfactory results that are consistent with good hygiene about BCs. ASes should not normally allow BCs to propagate beyond the RTBH provider(s). In some cases, a primary RTBH provider forwards the Blackhole Update to some immediate peers for their help in making RTBH even more effective.

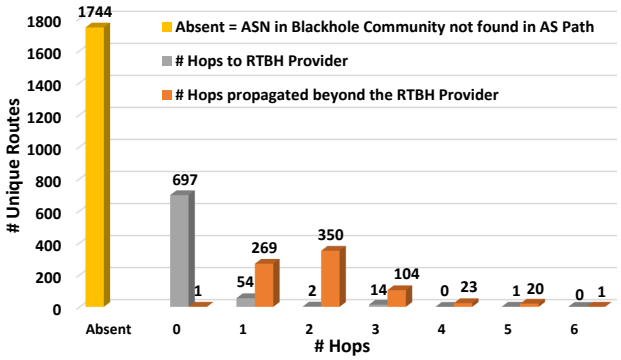

Fig. 1: Distributions of #hops propagated for BCs.

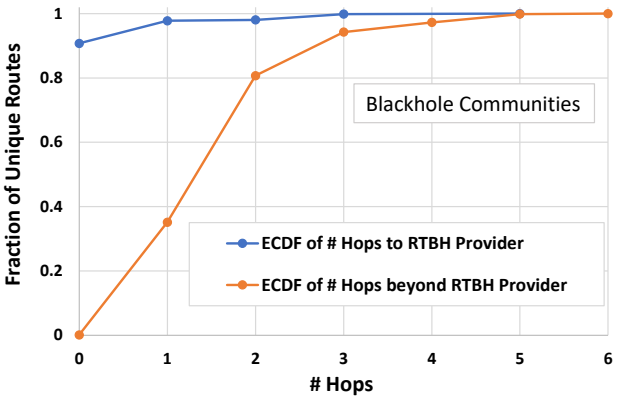

Fig. 2: ECDFs of hop counts to RTBH provider and beyond.

Fig. 3 shows the distributions of # unique routes with BCs and # unique BCs vs. the prefix length of the Blackhole prefix for IPv4. The # unique routes measure is in the sense of unique {Prefix, Path, BC}. It is instructive that the bulk of the routes (or BCs) occur at prefix length 24. A few routes even have /32 IPv4 prefixes. BCs are expected to be associated with prefixes with large prefix lengths. Prefixes more specific than /24 will be generally blocked by ASes along the way because of their route filtering policies. Hence, the highly specific routes with BCs are not likely to be detected at the collectors. Thus, the low measured numbers, as well as the distributions in Fig. 3, appear consistent with the expected behavior of routes with BCs.

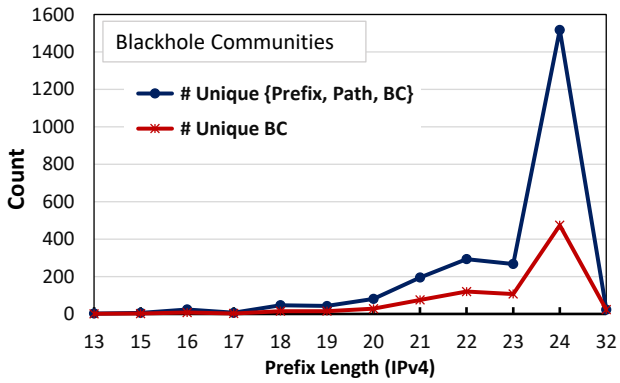

Fig. 3: Distribution of prefix lengths in BCs

B. *Other Regular Communities (Non-Blackhole)*

Some high-level statistics about RCs, in general, were stated and described earlier (Section III, Table I). Now, we turn our attention to Regular Communities (RCs) that are not Blackhole Communities (BCs) but belong to other known applications. For this, our strategy in this paper is to find the RCs that are unambiguously declared to belong in an application category with certain expected propagation behavior. In particular, we focus on RCs that are used by some major ISPs to signal peer and customer routes and are propagated to customers. The IRR data search reveals that at least these three major ISPs, namely, AS 174, AS 2914, and AS 1299 unambiguously declare that they propagate a variety of RCs to signal peer and customer routes to their customers, including encoding of region/country/city information [19] [20] [21]. For example, AS 2914 states, "Communities marked on routes sent to customers" and lists them all. Likewise, AS 1299 declares, "Telia Carrier offers origin BGP communities to all IP Transit customers as a standard service feature." And similarly, AS 174 declares, "Routes announced to customers by Cogent will have one of the following communities associated with them." AS 174 lists four Community strings under the above declaration as shown in Table V. AS 2914 and AS 1299 list dozens of Community strings under their declarations stated above; we include all of them and AS 174's (Table V) in our analysis of RCs. The direct customers of these ISPs should transitively propagate said RCs to their customers and the propagation should continue down the entire customer cone (note that RC is a transitive BGP attribute per RFC specification [11]). Thus, the propagation of said RCs over multiple hops from the respective ISPs' ASes would be the expected behavior.

TABLE V: AS 174 RCs in routes announced to customers.

RC string	Description	#Unique routes
174:21100	Route is learned from Europe (EU) non-customer	396,799
174:21001	Route is North America internal or customer route	254,368
174:21101	Route is a EU internal or customer route	156,994
174:21000	Route is learned from North America non-customer	134,276

Other major ISPs or enterprise ASes also list the RCs that they use to signal peer and customer routes but often do not make it explicitly clear whether they use them only internally or propagate in eBGP to their customers. So, for now, we have decided not to include them in the analysis. But in reality, often the RCs that belong to them are observed in the Routeviews/RIPE-RIS data to propagate multiple hops in large numbers of routes. Chances are that these RCs are purposely propagated to customers and/or peers, but to be conservative we focus on measuring and analyzing only RCs that are unambiguously declared to be announced to customer ASes. Thus, we consider the three major ISPs – AS 174, AS 2914, and AS 1299 – as mentioned above. This enables us to adhere to our strategy of measuring RCs against known applications.

Fig. 4 shows the distribution of #hops propagated (from the AS that matches the RC) for the RCs identified above corresponding to AS 174, AS 2914, and AS 1299 applications combined. These RCs should propagate down the respective customer cones and that would be correct behavior. The distribution in Fig. 4 can be trusted to be generally true considering the applications for which the RCs are intended. The #hops propagated range from 0 to 7. The ASes 174, 2914, and 1299 are major ISPs and they tend to have multiple levels (or Tiers) in the hierarchy in their customer cone. That explains why the #hops propagated can be easily 2 or 3. The message from this plot is that RCs do seem to propagate per what is needed for the applications. The distribution offers evidence that ASes do propagate RCs rather than strip them off. This is not meant to imply that RCs are always propagated when they need transitivity. ASes are known to have different policies or hygiene about propagation or blocking of Communities.

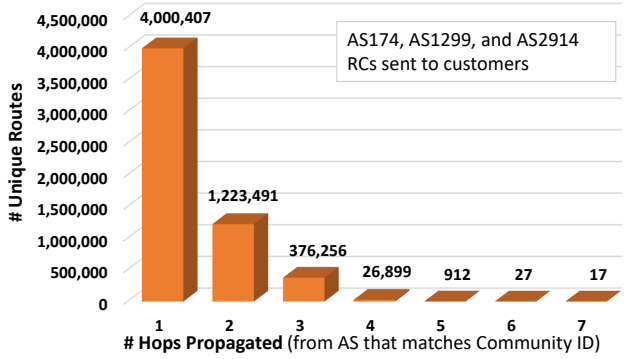

Fig. 4: Distribution of #hops propagated for {AS174, AS1299, AS2914} RCs sent to customers.

Fig. 5 compares the ECDFs of #hops propagated for {AS174, AS1299, AS2914} RCs sent to customers vs. all RCs (excluding BCs). In the latter case, the measurement is naturally not against specific known applications. However, we thought the comparison may be of interest. The figure shows that 'all RCs' propagate farther than the selected application-specific RCs. This seems intuitively explainable as follows. Higher tier ASes may be more likely to accord transitivity to communities. The application-specific RCs are only expected to propagate down (provider-to-customer hops) from the Tier-1 ASes while 'all RCs' may be added downstream from a transit provider, then propagate up (customer-to-provider hops) to a Tier-1 AS and may continue to propagate down.

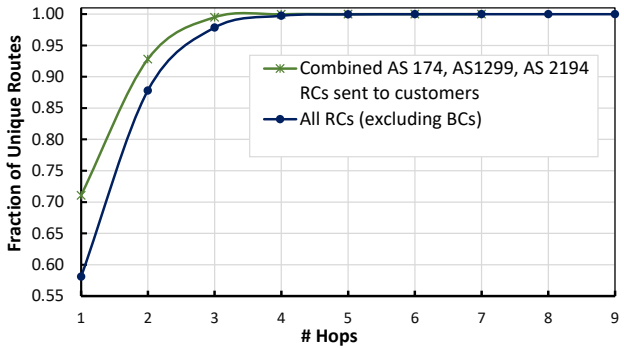

Fig. 5: Comparison of ECDFs of #hops propagated for {AS174, AS1299, AS2914} RCs sent to customers vs. all RCs (non-BC).

V. Analysis of Extended Communities

Some high-level statistics about ECs, in general, were stated and described earlier (Section III, Table I). Here, we present additional details. Fig. 6 shows the distribution of #hops propagated for Extended Communities (ECs) in terms of #unique routes. The #hops propagated measure is from the ASN in the

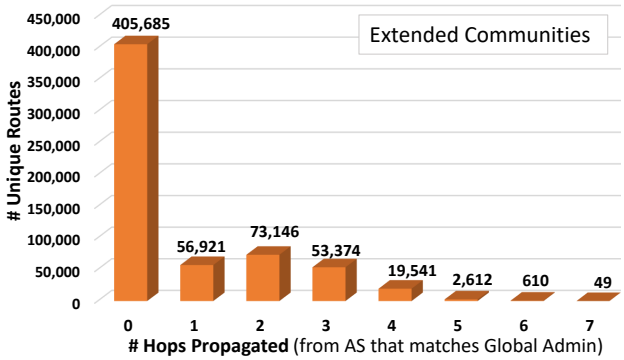

Fig. 6: Distribution of #hops propagated for ECs.

path that matches the ASN in the EC. Here we assume that the AS in the EC is the AS that added the EC. This provides a conservative estimate of the propagation distance. The spike at zero hops is contributed by one single AS and it corresponds to a transitive EC of type 00. The first 0 indicates 'transitive' but the second 0 (subtype for applications) is currently unassigned by IANA [9]. The figure shows that ECs do transitively propagate multiple hops, even up to 7 hops. Fig. 7 shows the distribution of EC types in terms of #unique routes. EC types 00, 01, 02, and 03 are all Transitive Two-Octet AS-Specific ECs [9] and

they have the highest values in terms of #unique routes seen. All ECs observed in the wild and shown in Fig. 7 are of the transitive type. No non-transitive ECs [9] are seen in the wild. ASes (or network operators) seem correctly restrained about not propagating non-transitive ECs.

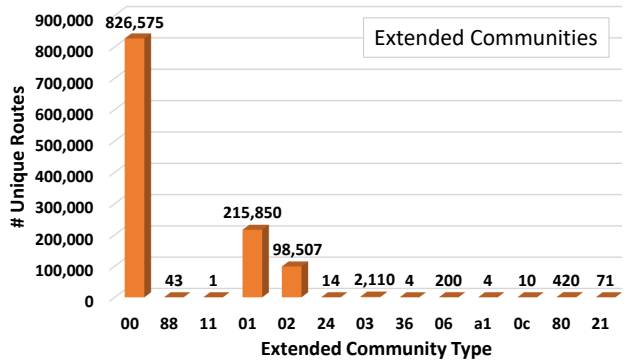

Fig. 7: Extended Community frequency distribution by Type.

VI. Analysis of Large Communities

Some high-level statistics about LCs, in general, were stated and described earlier (Section III, Table I). Here, we present additional details. Fig. 8 shows the distribution of #hops propagated for Large Communities (LCs) in terms of # unique routes. The #hops propagated measure is similar to that described for ECs above, i.e., from the ASN in the path that matches the ASN in the LC. Here again, we assume that the AS in the LC is the AS that added the LC to obtain a conservative estimate of the propagation distance. Unlike that for ECs, there is no IANA registration of LCs, let alone those for transitive and non-transitive applications. LCs are transitive per RFC specification [12]. From Fig. 8, it can be observed that LCs propagate in substantial numbers up to 5 hops. And at higher numbers of hops, LCs propagate in much smaller proportions, even reaching up to 10 hops. The applications associated with LCs do not seem published openly at this time, although the route-leak mitigation draft [14] requests well-known LCs to be allocated by IANA. Measuring LC propagation against known applications is planned as part of future studies.

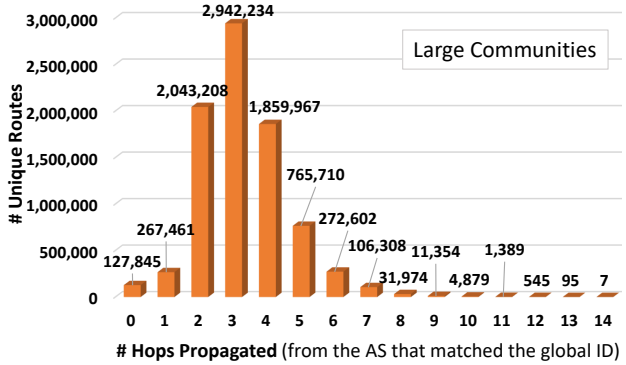

Fig. 8: Distribution of #hops propagated for LCs.

VII. Conclusions and Future Work

In this paper, we studied the propagation behaviors of Blackhole Communities and Regular (non-Blackhole) Communities used for signaling customer/peer routes in Updates sent to customers. These communities have specific known applications. In that sense, the measurements are performed against known applications; this need was expressed in IETF working group discussions. The measurements of propagation of Extended Communities indeed show that only the transitive ECs propagate on the Internet and the non-transitive ECs do not. That is rationally expected behavior for ECs. Our study provides some evidence of good hygiene being practiced by network operators about propagating (or discarding) of at least some of the community types (e.g., BCs, ECs, and RCs of known applications). There is more information needed about the emerging applications of LCs and ECs. More measurements of the EC and LC propagation against known applications are planned as part of future work.

References

[1] F. Streibelt et al., "BGP Communities: Even more Worms in the Routing Can," Proceedings of ACM IMC, October 2018.
[2] V. Giotsas et al., "Inferring BGP Blackholing Activity in the Internet," Proceedings of ACM IMC, November 2017.
[3] RIPE Routing Information Service. http://www.ripe.net/ris/
[4] University of Oregon Route Views Project. http://www.routeviews.org/
[5] Merit RADb, Merit Network, Inc. http://radb.net/
[6] T. King, C. Dietzel, J. Snijders, G. Doering, and G. Hankins, "BLACKHOLE Community," IETF RFC 7999, October 2016.
[7] S. Sangli, D. Tappan, and Y. Rekhter, "BGP Extended Communities Attribute," IETF RFC 4360, February 2006.
[8] E. Rosen and Y. Rekhter, "IANA Registries for BGP Extended Communities," IETF RFC 7153, March 2014.
[9] IANA Assignments for BGP Extended Communities. https://www.iana.org/assignments/bgp-extended-communities/bgp-extended-communities.xhtml
[10] D. Meyer, "BGP Communities for Data Collection," RFC 4384 (2006).
[11] R. Chandra, P. Traina, and T. Li, "BGP Communities Attribute," IETF RFC 1997, August 1996.
[12] J. Heitz, J. Snijders, K. Patel, I. Bagdonas, and N. Hilliard, "BGP Large Communities Attribute," IETF RFC 8092, February 2017.
[13] J. Snijders, J. Heasley, and M. Schmidt, "Use of BGP Large Communities," IETF RFC 8195, June 2017.
[14] K. Sriram and A. Azimov, "Methods for Detection and Mitigation of BGP Route Leaks," IETF I-D, October 2021. https://datatracker.ietf.org/doc/draft-ietf-grow-route-leak-detection-mitigation/
[15] S. Hares et al., "BGP Flow Specification Version 2," IETF Internet-Draft, October 2021. https://datatracker.ietf.org/doc/draft-hares-idr-flowspec-v2/
[16] IETF GROW WG discussion on "Choice of Large vs. Extended Community for Route Leaks Solution," March 2021. https://mailarchive.ietf.org/arch/browse/grow/?gbt=1&index=152EJ38HSvfapwg4F0SqFii69RM
[17] L. Hannachi and K. Sriram, "Analysis of Propagation of Regular, Extended, and Large BGP Communities," Presentation at the IETF GROW WG Meeting, IETF 111 Proceedings, July 2021. https://datatracker.ietf.org/meeting/111/materials/slides-111-grow-bgp-regularextendedlarge-community-analysis-01
[18] IETF GROW WG discussion on BGP communities, August 2021. https://mailarchive.ietf.org/arch/msg/grow/MvydwLtpb01dzsK-bX7EVrl6VeY/
[19] AS 174 Communities: https://onestep.net/communities/as174/
[20] AS 1299 Communities. https://www.teliacarrier.com/our-network/bgp-routing/bgp-communities.html
[21] AS 2914 Communities. https://www.gin.ntt.net/support-center/policies-procedures/routing/
[22] AS 3356 Communities. https://onestep.net/communities/as3356/ https://www.robtex.com/as/AS3356.html
[23] AS 2603 Communities. https://www.nordu.net/content/nordunet-ip-and-mpls-network-0
[24] AS 5511 Communities. https://bgp.he.net/AS5511 (IRR tab)
[25] AS 6939 Communities. https://www.he.net/adm/blackhole.html
[26] AS 3491 Communities. https://www.robtex.com/as/AS3491.html
[27] Tier-1 networks. https://en.wikipedia.org/wiki/Tier_1_network