Alarms Validation via Pattern Matching

In our paper, we define four anomalous route change patterns that represent typical routing anomalies. Namely,

- P1 (Unauthorized Route Change): The origin ASes before and after the route change belong to different organizations and have different RPKI validation states, *i.e.,* one in the *invalid_ASN* state and the other in the *valid* state [1].
- P2 (Route Leak): The routing path before or after the route change violates the valley-free criterion [2].
- P3 (Path Manipulation): The routing path before or after the route change contains reserved ASNs or adjacent ASes that have no business relationship records between them [3].
- P4 (ROA Misconfiguration): The origin ASes before and after the change are from the same organization but have different RPKI validation states, *i.e.,* one in the *invalid_length* or *invalid_ASN* state and the other in the *valid* state [4].

Here, we discuss the rationale of P1-P4, which are confirmed by domain experts. Each pattern represents one typical kind of Internet routing anomalies. Specifically, P1 tracks the change of RPKI validity states, which indicates the legitimacy of AS-Prefix bindings [1], during a route change to detect the unauthorized prefix announcements caused by misconfiguration or hijacking attacks. P2 tracks the violation of the valley-free criterion during a route change. This criterion describes an inherent attribute of normal routing paths in terms of business relationships [2]. According to RFC 7908 [5], the violation of this criterion indicates a route leak. P3 tracks the appearance of suspicious path segments during a route change, including private ASNs and adjacent ASes that do not have business relationship records in the CAIDA dataset. In particular, the private ASNs [6] only appear in the global routing paths when adversaries tamper with the routing path or misconfigurations happen. Besides, considering CAIDA maintains a relatively comprehensive knowledge base of the business relationships among global ASes, the adjacent ASes that have no relationship records in the CAIDA dataset typically represent nonexistent routing connections and are very likely to be forged by sophisticated attacks, *e.g.,* the Type-N hijacking [3]. Lastly, P4 tracks the conflicts between route announcements and Route Origin Authorization (ROA) objects where the conflicting ASes belong to the same organization. Since the ASes in the same organization usually share the same interests, these conflicts indicate the ROA object misconfigurations.

Table 1: **Anomalous patterns of the routing anomaly events reported by our detection system.**

Name	**H.C.**					**L.C.**	**Avg.EP**
	P1	**P2**	**P3**	**P4**	**Any**		
$SP_{backcon\_5}$	0	25	30	2	32	2	0.6478
$SP_{backcon\_4}$	2	20	19	1	21	0	0.8163
$SP_{backcon\_2}$	1	29	31	3	36	1	0.7628
$SP_{bitcanal\_1}$	1	10	16	0	16	0	0.7473
$SP_{petersburg}$	2	18	24	3	24	0	0.8912
SP_{defcon}	3	3	3	1	6	1	0.9624
SO_{iran}	5	21	27	2	29	2	0.8190
$SO_{bitcanal\_3}$	8	36	38	2	39	1	0.8966
$SO_{backcon\_3}$	3	24	25	2	30	5	0.7520
$SO_{backcon\_1}$	0	15	12	1	15	3	0.8691
$SO_{bitcanal\_2}$	4	19	24	2	24	0	0.8798
SO_{h3s}	1	13	12	1	14	0	0.8444
$SO_{pakistan}$	2	8	5	0	9	1	0.7058
PO_{brazil}	4	34	50	2	50	1	0.5878
PO_{sprint}	1	26	28	3	29	0	0.9262
RL_{jtl}	1	30	34	0	41	5	0.7072
$RL_{stelkom}$	3	32	37	0	40	3	0.7644
$RL_{itregion}$	5	33	38	1	40	4	0.8187

We explain how to use these patterns to analyze the alarms. For each reported routing anomaly event, we calculate the fraction of suspicious route changes in the event that match each pattern (*i.e.,* P1-P4) as the explanatory power (EP) of each pattern. Then, if the EP of any pattern is higher than 50% (*i.e.,* an absolute majority), we consider the event an anomaly with high confidence (H.C.), otherwise with low confidence (L.C.). Specifically, we use the RIPEstat web API[1] to query

[1] https://stat.ripe.net/ui2013/

RPKI validation states and the CAIDA AS-to-organization mapping dataset [7] to identify the organizations of ASes. We show the number of H.C. and L.C. events detected by our system in each dataset and the average EP of the H.C. events in Table 1. We report the L.C. events as false alarms in §5.2 in our paper.

Note that, when we investigate which country an AS belongs to, we treat European countries as a whole since they are close by and well connected by many non-BGP links [8]. Besides, given that some route change events occurred long ago, before their corresponding prefixes had registered ROA objects, we use the most recent RPKI validation results to identify the RPKI-related patterns P1 and P4. Further, to reduce the negative impact of the inconsistency between historical and current ROA objects, we double-check each event matching P1 and P4 based on the RIPEstat database and only regard those with unchanged authorized AS-prefix bindings as H.C.

References

[1] P. Mohapatra, J. Scudder, D. Ward, R. Bush, and R. Austein, "Bgp prefix origin validation," in *IETF RFC 6811*, 2013.

[2] L. Gao, "On inferring autonomous system relationships in the internet," *TON*, vol. 9, no. 6, pp. 733–745, 2001.

[3] P. Sermpezis, V. Kotronis, P. Gigis, X. Dimitropoulos, D. Cicalese, A. King, and A. Dainotti, "Artemis: Neutralizing bgp hijacking within a minute," *TON*, vol. 26, no. 6, pp. 2471–2486, 2018.

[4] Y. Gilad, A. Cohen, A. Herzberg, M. Schapira, and H. Shulman, "Are we there yet? on rpki's deployment and security," *Cryptology ePrint Archive*, 2016.

[5] K. Sriram, D. Montgomery, D. McPherson, E. Osterweil, and B. Dickson, "Problem definition and classification of bgp route leaks," *RFC 7908, IETF*, 2016.

[6] J. Mitchell, "Autonomous system (as) reservation for private use," *RFC 6996, IETF*, 2013.

[7] CAIDA. AS-to-Organization Mapping Dataset. Accessed May. 25, 2023. [Online]. Available: https://www.caida.org/catalog/datasets/as-organizations/

[8] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, "An analysis of bgp multiple origin as (moas) conflicts," in *SIGCOMM WS*, 2001, pp. 31–35.