Buddyguard+: An Adaptive IP Prefix Anomaly Monitor

Mingwei Zhang
University of Oregon

Jun Li
University of Oregon

What is Buddyguard+?

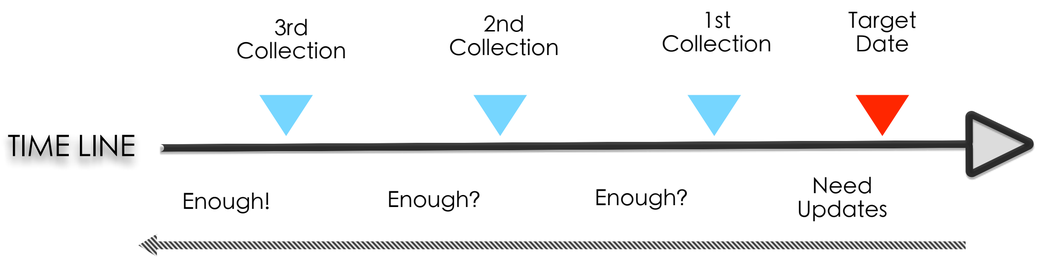
Buddyguard is a novel approach to detecting prefix anomalies including prefix hijacking and route leaks. Buddyguard compares the behavior of a monitored prefix with the behavior of numerous buddy prefixes. The system detects anomalies when the behavior of the monitored prefix significantly diverges from that of its buddies. Buddyguard provides fast, accurate and lightweight monitoring of IP prefix anomalies, and its introduction and use of buddy prefixes enables it to be resilient against resourceful attackers.

Buddyguard+ extends the original design by focusing on adaptively expanding the space of searching for buddies and adaptively including more BGP data for training. Buddygaurd+ monitors not only the target prefix, but also sub-prefixes and the minimal super-prefix of the target prefix in order to avoid false negatives.

Adaptive Updates Collection

Original Buddyguard applies 7 days as a training window, meaning all BGP updates in the 7-day window prior to the target date would be used to train buddies. The static 7-day window potentially contains an inadequate number of BGP updates which is a consequence of the dynamic nature of BGP.

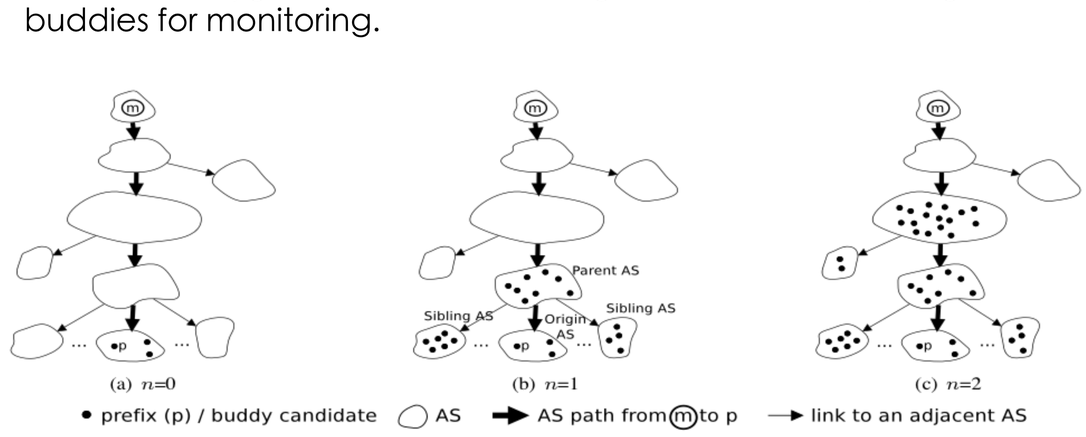
Buddyguard+ applies an adaptive updates collection mechanism to overcome this restriction. The size of training window is determined by the number of updates collected during the window. As soon as the number of updates reaching a sufficient threshold, meaning enough updates for finding buddies, the collecting procedure will stop.



Adaptive Candidate Search

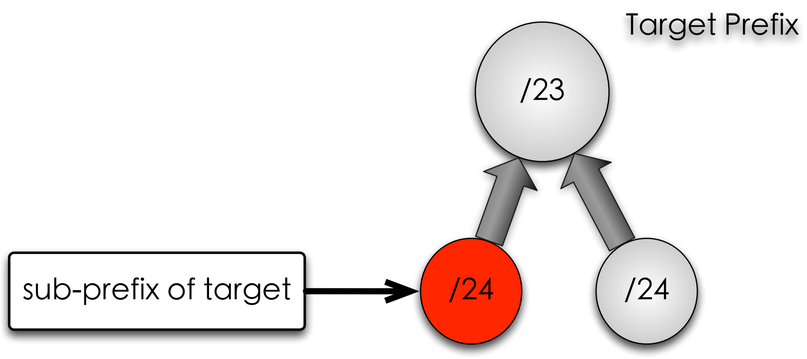
The original Buddyguard searches for Buddy candidates strictly within origin, parent and siblings ASes (Figure (a-b) below). Small ASes may result in lack of candidates.

Buddyguard+ will expand searching area when the number of candidates is less than threshold. The upper levels contain the "grandparent" AS and "uncles" ASes. The expanding procedure ensures Buddyguard+ will have enough candidates to pick good buddies for monitoring.



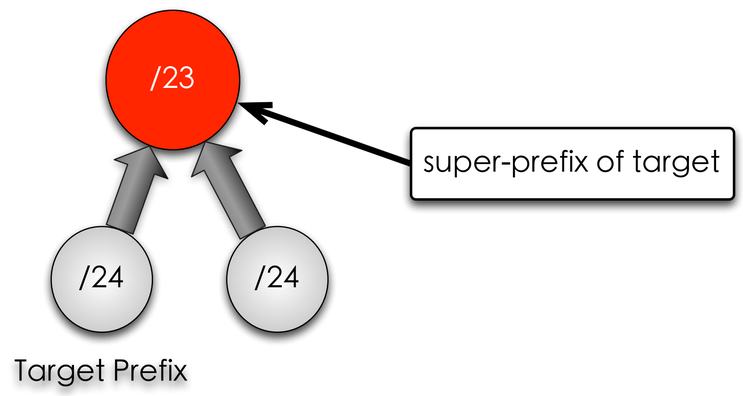
Sub-Prefix Monitoring

The longest matching prefix principle, which is used by a BGP router, dictates that the route to the destination associated the most specific prefix shall be used for forwarding. For example, 192.168.1.1/24 is preferred to 192.168.1.1/23. Buddyguard+ watches all updates that has target's sub-prefixes as their origin, in order to detect the sub-prefix hijacking. Buddyguard+ also learn buddies from the updates of both target and its sub-prefixes, enlarging the pool of buddy candidates.



Super-Prefix Monitoring

Prefix aggregation provides a challenge for the original Buddyguard by masking the specific prefixes that are used for route learning. The resulting super-prefixes need to be used for training buddies in addition to the target prefixes already used by the original Buddyguard. Buddyguard+ will monitor both the aggregated and target prefixes in order to avoid false negatives.



This research is supported by the National Science Foundation under Award No. CNS-1118101. Any opinions, findings, and conclusions or recommendations expressed in this research are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.