Reading Report #7
Paper: A study of prefix hijacking and interception in the Internet
Student: Shuo Yang

In the paper the authors briefly mentioned two other possibilities an AS could use for hijacking traffic to a prefix: 1) advertise a more specific prefix (sub-prefix); 2) advertise a less specific prefix (super-prefix). Then they stopped right here saying that "the impact of such advertisements can be trivially predicated, we don't study them here". However, it seems to me not convincing. Although the intermediate consequence of these kind of hijackings are obvious, their deep impact to the Internet routing system may be far from being trivially predicated. In addition, an AS can also advertise an unused prefix or unallocated prefix. These types of hijacking seem more suspicious (could be done intentionally) than the regular one (advertisement of the same prefix as the one being advertised by the owner) the paper focused on.

It is a pity the paper does not cover different types of prefix hijacking. In order to get a big picture of the degree of prefix hijacking and the impact it has imposed on the Internet, it is very important for us to understand characteristics of different types of prefix hijacking in deep. We should be interested in knowing:

1. What is the frequency distribution of different types of prefix hijacking? Which one is more frequently happened and which is less frequently happened?
2. What is the fraction of traffic that can be hijacked for different types of prefix hijacking?
3. What are the possible root causes for different types of prefix hijacking? Are they different by type? For example, mis-configuration might cause more exact-prefix hijacking while malicious attack might cause more sub-prefix hijacking.
4. Does the type of prefix hijacking correlate with the level of tier ASes belong to?
5. How does the BGP routing policy influence the different kind of prefix hijacking? For example, the longest match rule causes all traffic be routed to sub-prefix hijacking ASes. BGP routing policy might have more subtle influences on all kinds of prefix hijacking.

Trying to answer these questions are important because:

1. It helps us to better understand the global impact of prefix hijacking to the entire Internet routing system.
2. It helps us to better detect or prevent prefix hijacking. If we know characteristics of different types of prefix hijacking, we can devise and deploy different detection or prevent strategies. For example, we may adopt more aggressive strategy on sub-prefix hijacking, and employ less aggressive strategy on super-prefix hijacking due to different level of impact each has.