Note, I didn't actually implement the countermeasure for Part 4 of this Project. This is just to describe what I would have implemented given the reading that was provided in the homework.

As stated in the paper that was given:

Lad, M., Oliveira, R., Zhang, B., & Zhang, L. (2007, June). Understanding resiliency of internet topology against prefix hijack attacks. In *37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07)*(pp. 368-377). IEEE.

The key to high resilience is to make the tier-1 nodes and other big ISPs always believe the true origin. The way to achieve this is to reach as many tier-1 nodes as possible using a provider route. In addition, when a node has to choose between two routes of the same preference, path length becomes a deciding factor, and thus the shorter the number of hops to reach the tier-1 nodes, the better the resilience. From our observations from simulation results, we found that the most resilient nodes are direct customers of many tier-1 nodes and other big ISPs.

Thus, in implementing a solution I would try to reach as many tier-1 nodes as possible using a provider route. Also I would design a topology with shorter number of hops to reach the tier-1 nodes.