The Crossfire Attack

Motivation
Cutting out organizations, cities or even regions from the Internet could be possible if we overflow a set of critical links that connect that entity to the Internet. This is in contrast from traditional DDoS attacks where the attacker targets a specific end host.

Methodology
The attack consists of three steps:

1. Constructing a link map towards the targeted entity.
2. Finding a set of decoy servers residing in the vicinity of a target.
3. Flooding the set of target links by coordinating a botnet to send low bitrate traffics towards the selected set of servers.

Dataset
The authors rely on 1K (PlanetLab + LG’s) vantage points to initiate traceroutes towards the target region (2 universities, 4 states, 2 regions) from a geographically diverse set of nodes. These nodes a representative of the bots in an actual attack. Each vantage point would initiate 6 traceroutes towards each of the selected IP addresses within the target region. Having the route towards a target the authors measure the degradation ratio which indicate the ratio of paths that would be effected if we cut out the given link. The authors observe a phenomena which they refer to as a narrow path waist for all of the selected targets, having the degradation ratio measure one could select a set of critical links for a link flooding attack.

Key Findings
- Large targets (states, regions) could be disconnected from the Internet by targeting a set of limited links.
- The crossfire attack could remain undetectable from due to the fact that it does not target end hosts but links that connect that entity to the Internet.
- Degradation ratio would vary depending on the size of a target. Targeting 15 links could affect 30%(90%) of the targets (university(region)) paths.
• Relatively low cost for conducting this attack (asymmetry between cost for attacker and victim).