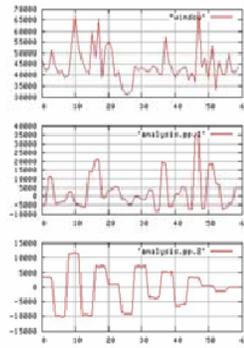
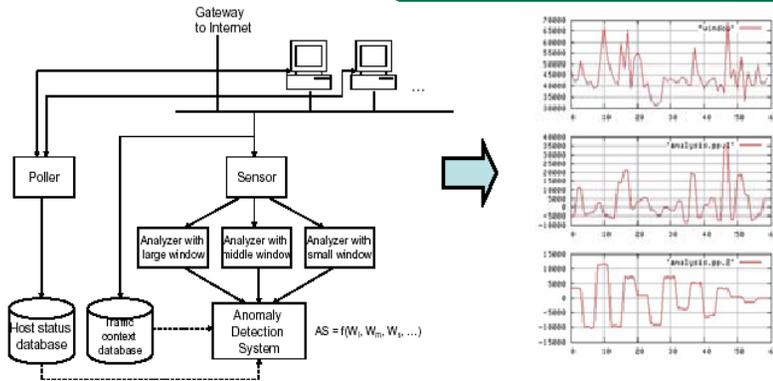


DEFT: Dynamic Early Filtering of Internet Traffic

Cyberspace Sciences & Information
Intelligence (CSIIR) Group



Problem Statement:

Increasing numbers of unwanted, unsolicited “garbage” packets mainly generated by DDoS attacks, worm attacks, and spam. These packets traverse the Internet before getting filtered at their destination, and cause severe traffic burdens, waste communication resources, and disrupt the normal functions of networked infrastructure.

Technical Approach:

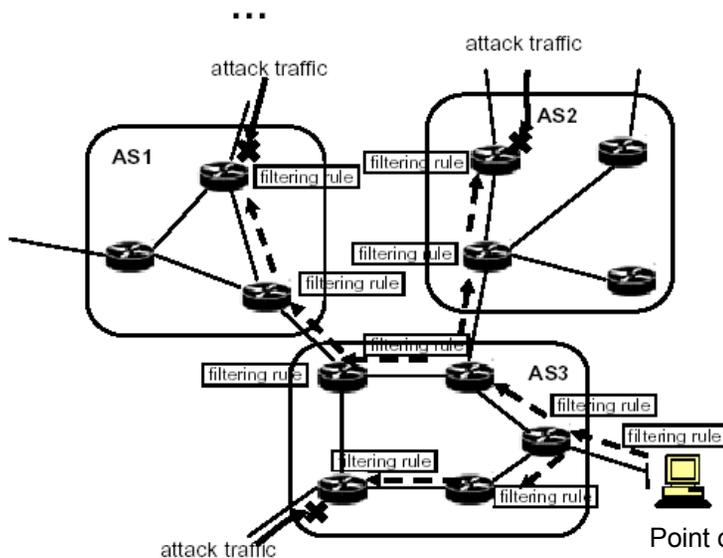
DEFT will coordinate routers to filter and discard garbage packets soon after they enter the Internet. DEFT has four major components:

- **Rule generation:** quickly identify streams of garbage packets and generate appropriate filtering rules automatically.
- **Rule dissemination:** combine BGP routing mechanism to disseminate filtering rules to routers closer to the attack source.
- **Rule management:** install filtering rules in a scalable manner by using only reasonable amount of router’s resources.
- **Rule security:** provide authentication of dynamic filtering rules.

destination	protocol	port
01 18 0a 00 01	03 81 06	04 81 19



destination	source	port
01 18 0a 00 02	02 10 c0 0a	04 81 50



Benefit:

Limit the damages caused by large-scale Internet attacks, increase the reliability of critical national infrastructures, reduce ISP operational costs, enhance the performance of many online services and applications. DEFT will also benefit a broad range of disciplines that require intensive Internet communications (e.g., computational physics, astronomy, medical science, and biology).

Point of Contacts: Dr. Frederick Sheldon (865-576-1339) sheldonft@ornl.gov
Dr. Chin-Tser Huang, Univ. of South Carolina huangct@cse.sc.edu