A2D2-2

Autonomous Anti-DDOS Network V2.0
IDIP enhanced DDOS

Sarah Jelinek
University Of Colorado, Colorado Springs
sarah.jelinek@sun.com

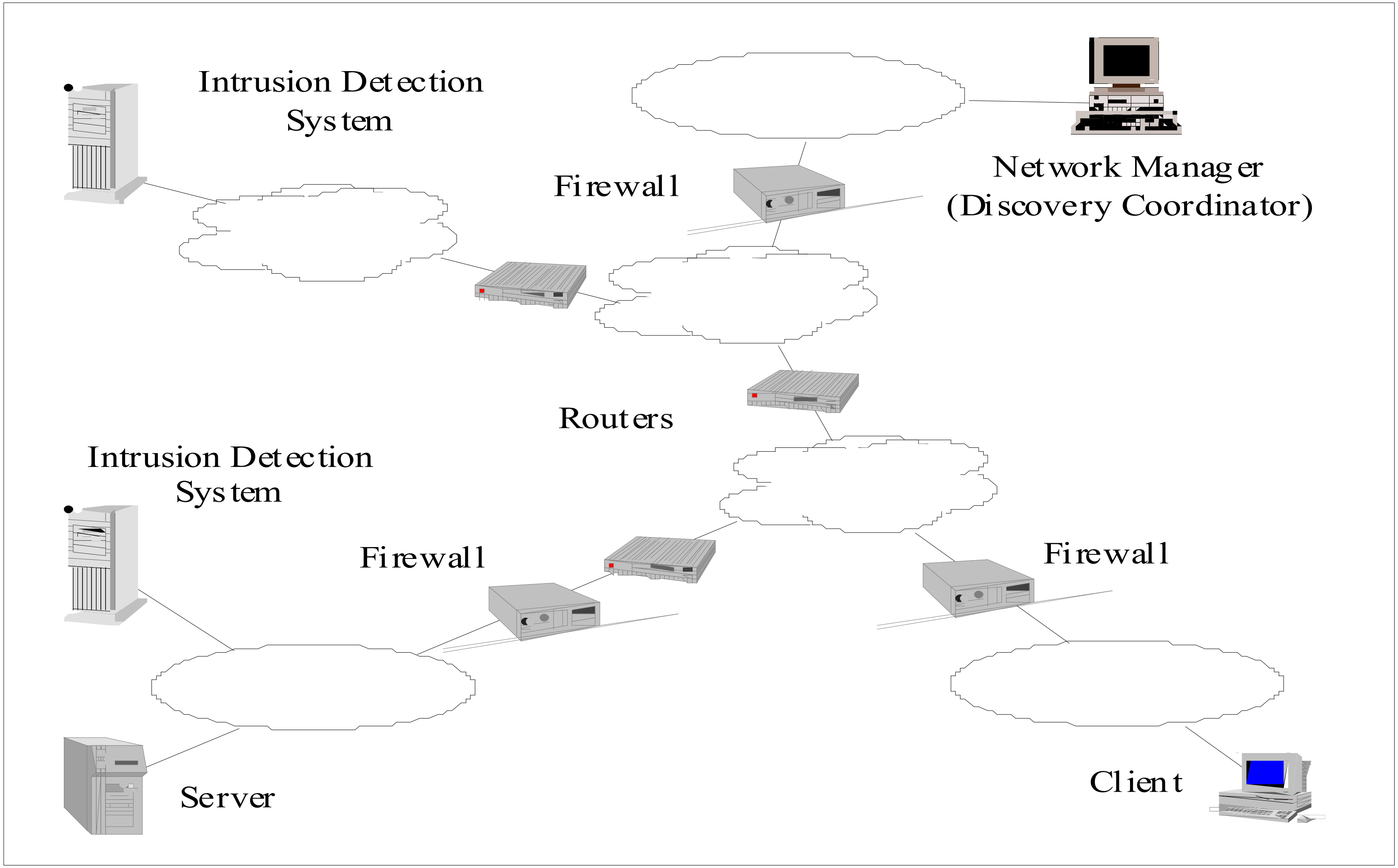
Project Goals

- To make DDoS technology more robust
- Enhancements to Angela Cearn's Masters thesis work, A2D2
  - DDoS Intrusion detection and response system
  - Uses Snort as main detection mechanism
  - Modifications to enable rate limiting
    - More info:http://cs.uccs.edu/~chow/pub/master/acearns/doc/angThesis-final.pdf
- Incorporate the use of Intrusion Detection and Isolation Protocol(IDIP)
- Setup IDIP Neighborhood and Community and test DDoS response with A2D2-2

What is IDIP?

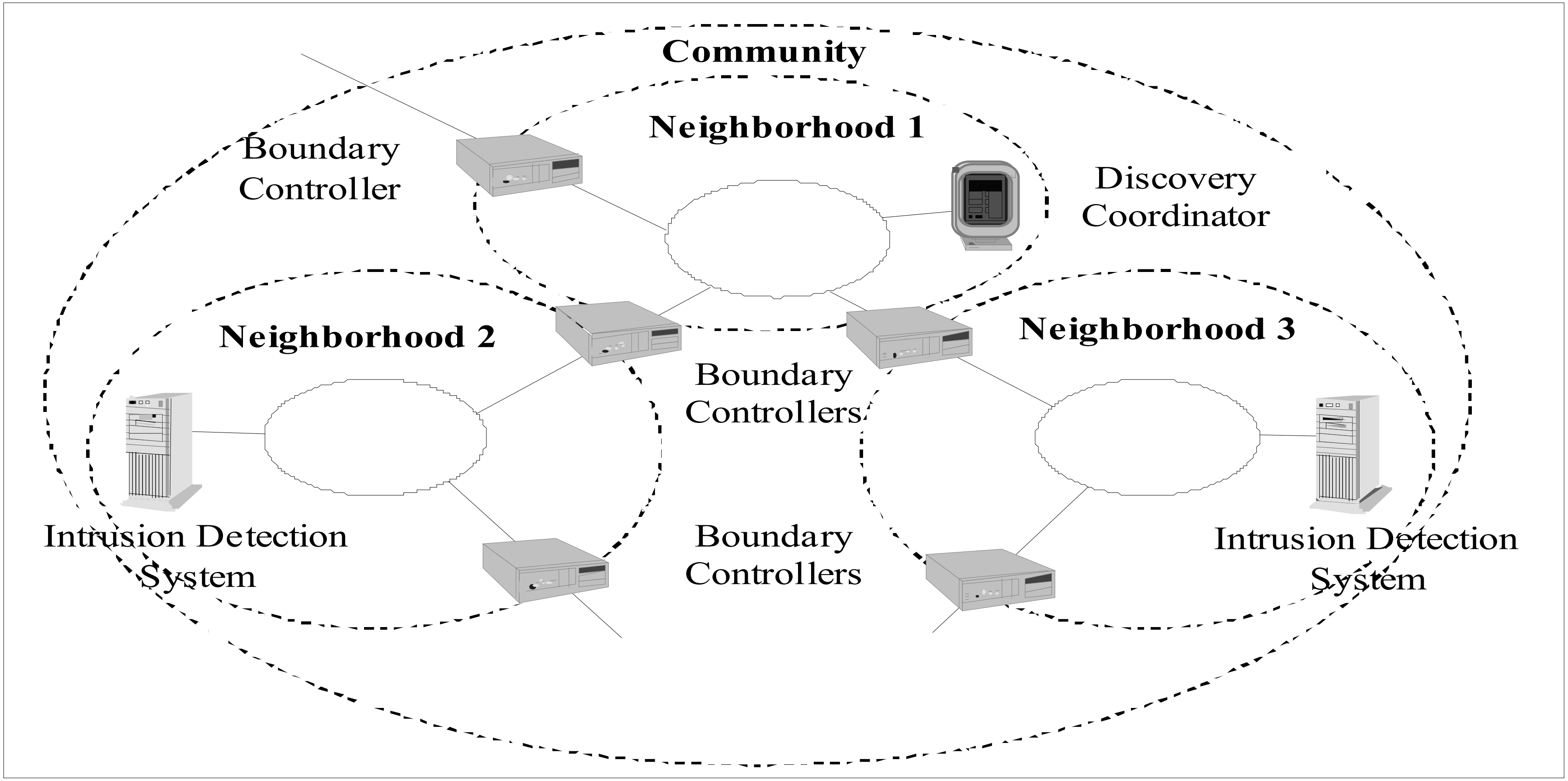
- IDIP is a set of protocols
  - Hello
  - Message
  - Application
- IDIP Objective is to share information
  - Enables intrusion tracking and containment
- IDIP relies on neighborhoods and communities

IDIP Architecture



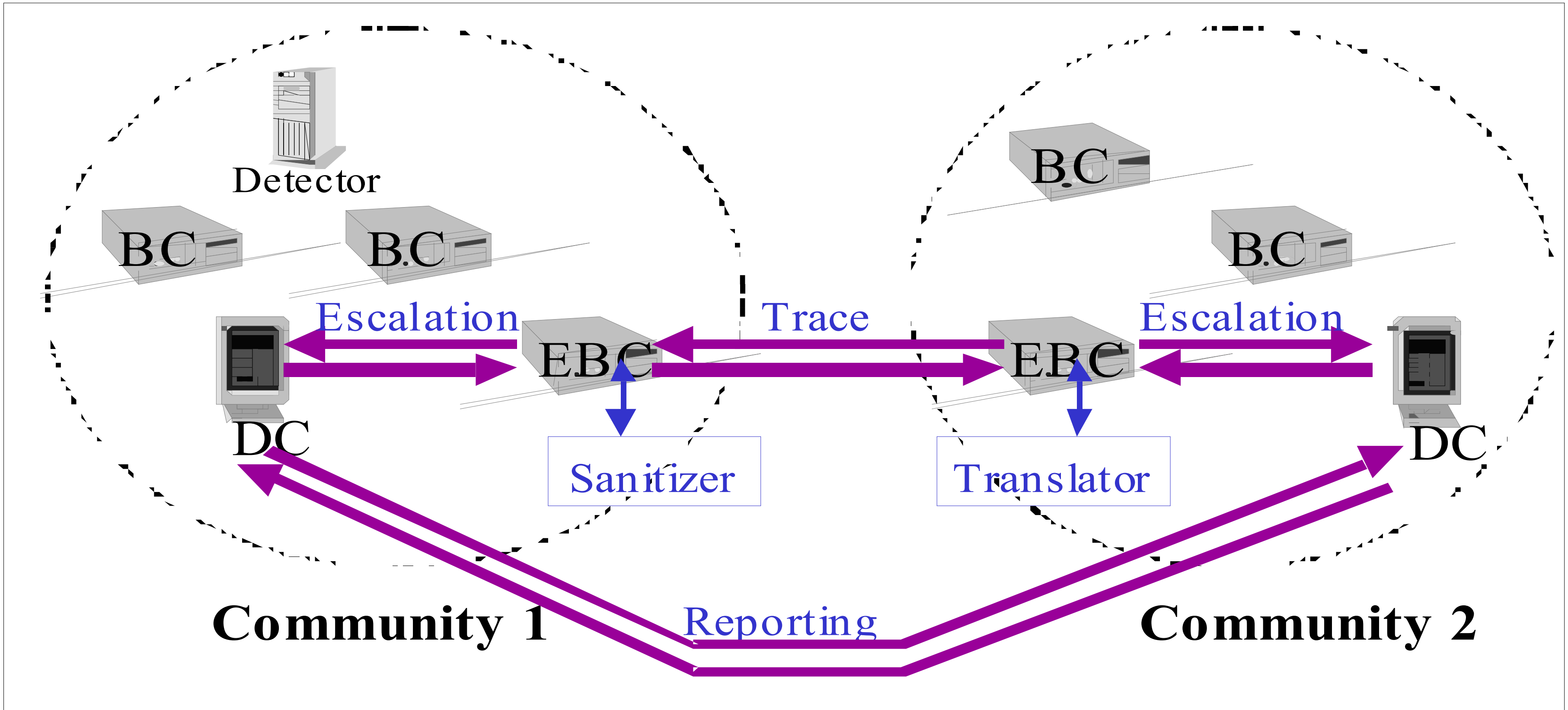
IDIP Nodes

IDIP Architecture cont.



IDIP Communities

DDoS Attack Scenario with IDIP

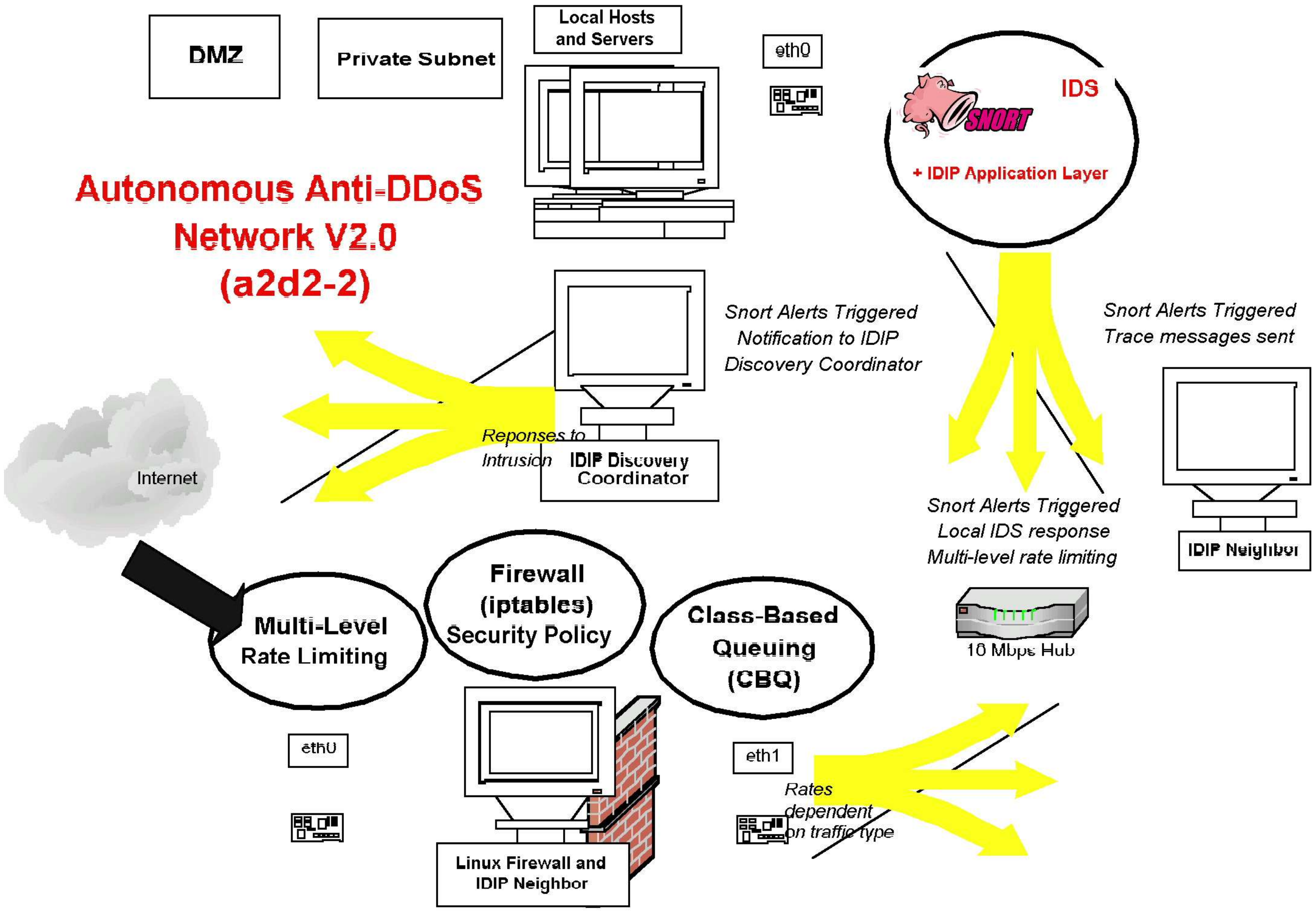


DC - Discovery Coordinator (Management Console)

BC - Boundary Controller (Firewalls, Routers, etc.)

EBC - Edge Boundary Controller (e.g., Corporate Firewall)

Proposed A2D2-2 Architecture


DMZ
Private Subnet
Local Hosts and Servers
eth0
IDS
SNORT
+ IDIP Application Layer
Autonomous Anti-DDoS Network V2.0 (a2d2-2)
Snort Alerts Triggered Notification to IDIP Discovery Coordinator
Snort Alerts Triggered Trace messages sent
Reponses to Intrusion
IDIP Discovery Coordinator
Internet
Snort Alerts Triggered Local IDS response Multi-level rate limiting
IDIP Neighbor
Firewall (iptables) Security Policy
Multi-Level Rate Limiting
Class-Based Queuing (CBQ)
10 Mbps Hub
eth0
eth1
Rates dependent on traffic type
Linux Firewall and IDIP Neighbor

A2D2-2 Status

- Still working on code
- Have IDIP receiver, IDIP sender and IDIP hello protocol implemented
  - Am limiting my project to implementation of the IDIP message layer(receiver, sender and hello protocol) as well as Snort enhancements for Application layer node
- Need to modify A2D2 snort code to act as IDIP application
- Code is located at: ~sjjelinek/masters/project/src
- Plan for code complete by 11/03

Future Work

- IDIP Redundant/Cooperative Discovery Coordinators
- Discovery Coordinator and Application layer response enhancements
- More updates to SNORT for DDoS pushback
- Security protocol implementation
- More Application protocol implementation
- OpenSLP proxy server work

References

- [C02] Cearns, Angela. 2002. Autonomous Anti-DDoS Network http://cs.uccs.edu/~chow/pub/master/acearns/doc/angThesis-final.doc
- [T02] Toplayer.com. 2002. Intrusion Protection Systems http://www.toplayer.com/bitpipe/IPS_Whitepaper_112602.pdf
- [NB02] Network Associates Labs. Boeing Phantom Works. 2002. http://zen.ece.ohiou.edu/~inbounds/DOCS/reldocs/IDIP_Architecture.doc
- [NB02-1] Network Associates Labs. Boeing Phantom Works. 2002. http://zen.ece.ohiou.edu/~inbounds/DOCS/reldocs/IDIP_Application_Layer.doc
- [NB02-2] Network Associates Labs. Boeing Phantom Works. 2002. http://zen.ece.ohiou.edu/~inbounds/DOCS/reldocs/IDIP_Message_Layer.doc
- [T02] Tanase, Matt. 2002. Barbarians at the Gate: An Introduction to Distributed Denial of Service Attacks
- http://www.securityfocus.com/infocus/1647
- [C03] Chow, Edward C. Security Related Research Projects at UCCS Network Research Lab, January 10, 2003
- [DAR02] DARPA. 2002. Common Intrusion Detection Framework.
- http://www.isi.edu/gost/cidf/
- [OpenSLP] Open SLP Project. 2003.
- http://www.openslp.org/
- [B02] Brindley, Adrian. Denial of Service Attacks and the Emergence of “Intrusion Prevention Systems”, November 2002.
- http://www.sans.org/rr/firewall/prevention.php