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)
- Use Service Locator Protocol(SLP) to find proxy servers

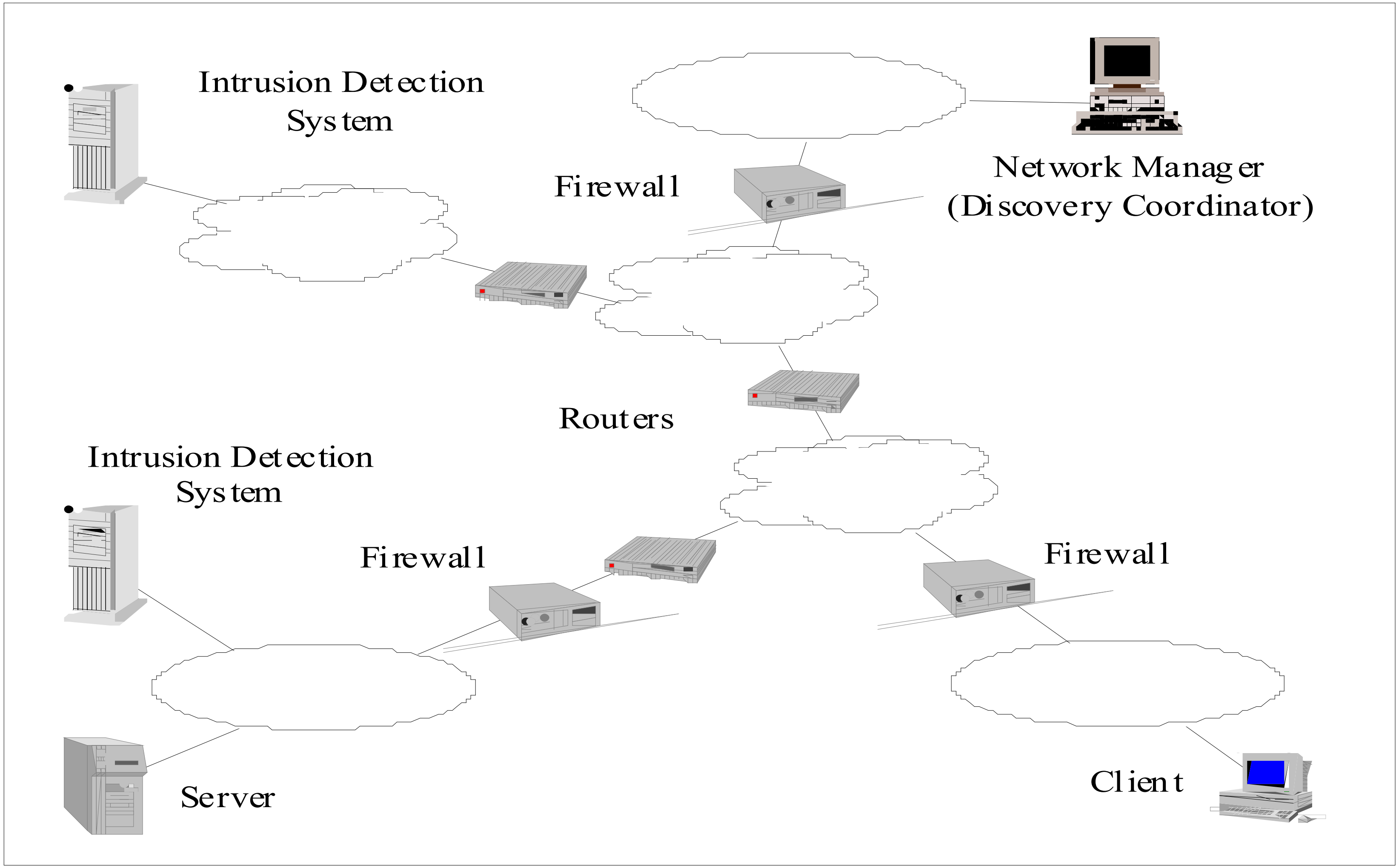
A2D2-2 Status

- 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
- Have downloaded and compiled OpenSLP (however not sure this piece is part of my project)
- Code is located at: ~sjjelinek/masters/project/src
- Plan for code complete by 11/03

IDIP and how it used

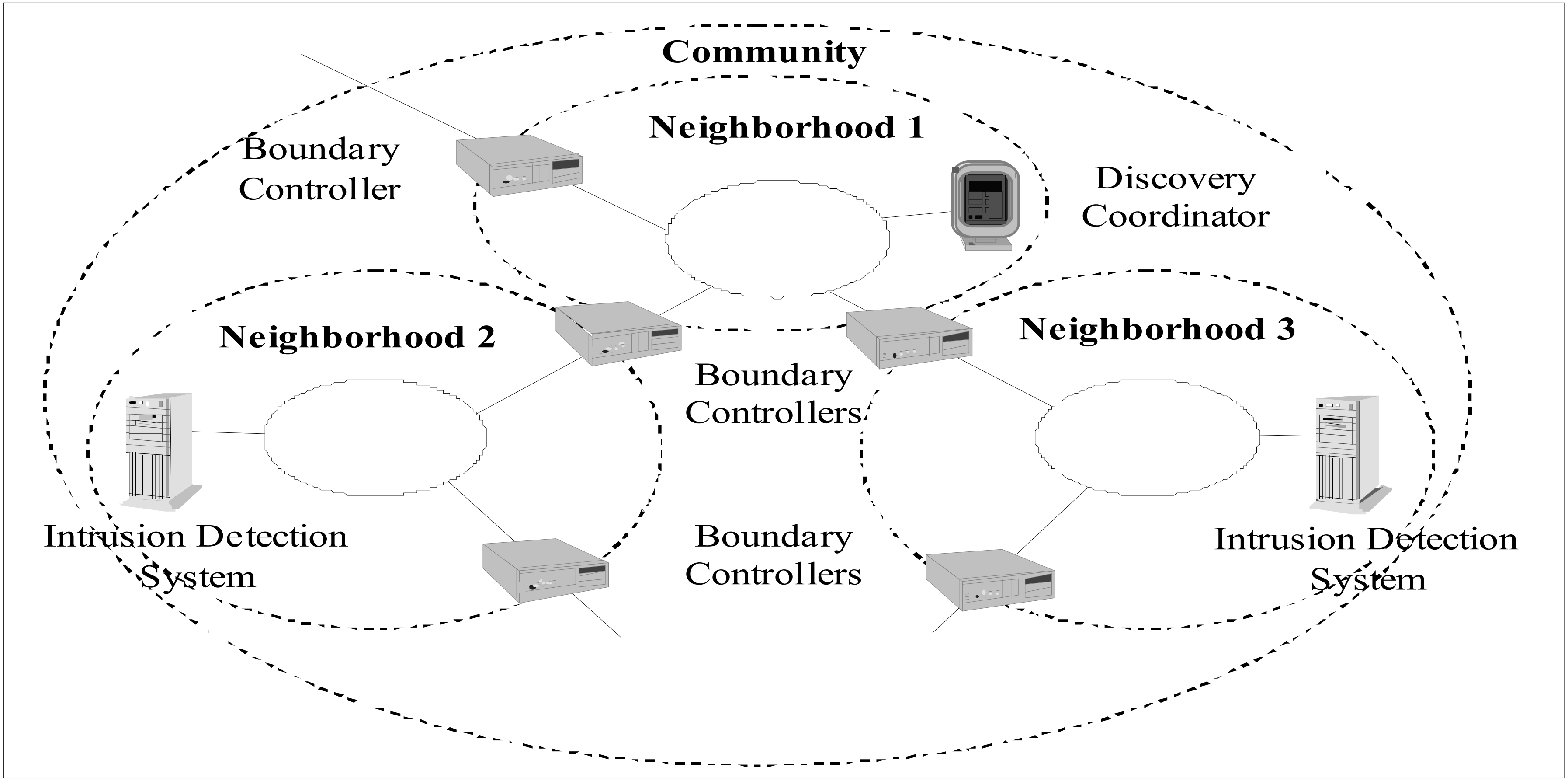
- IDIP protocol is split in to three components:
  - Message, Application and Discovery Coordinator
- Message layer is built on UDP and responsible for all communication to and from IDIP nodes
- Application layer is any application modified to talk to IDIP message layer. Can include more IDIP specific enhancements as well, including traceback, monitoring...
- Discovery Coordinator is responsible for maintaining IDIP neighborhood

IDIP Architecture


Intrusion Detection System
Network Manager (Discovery Coordinator)
Firewall
Routers
Intrusion Detection System
Firewall
Firewall
Server
Client

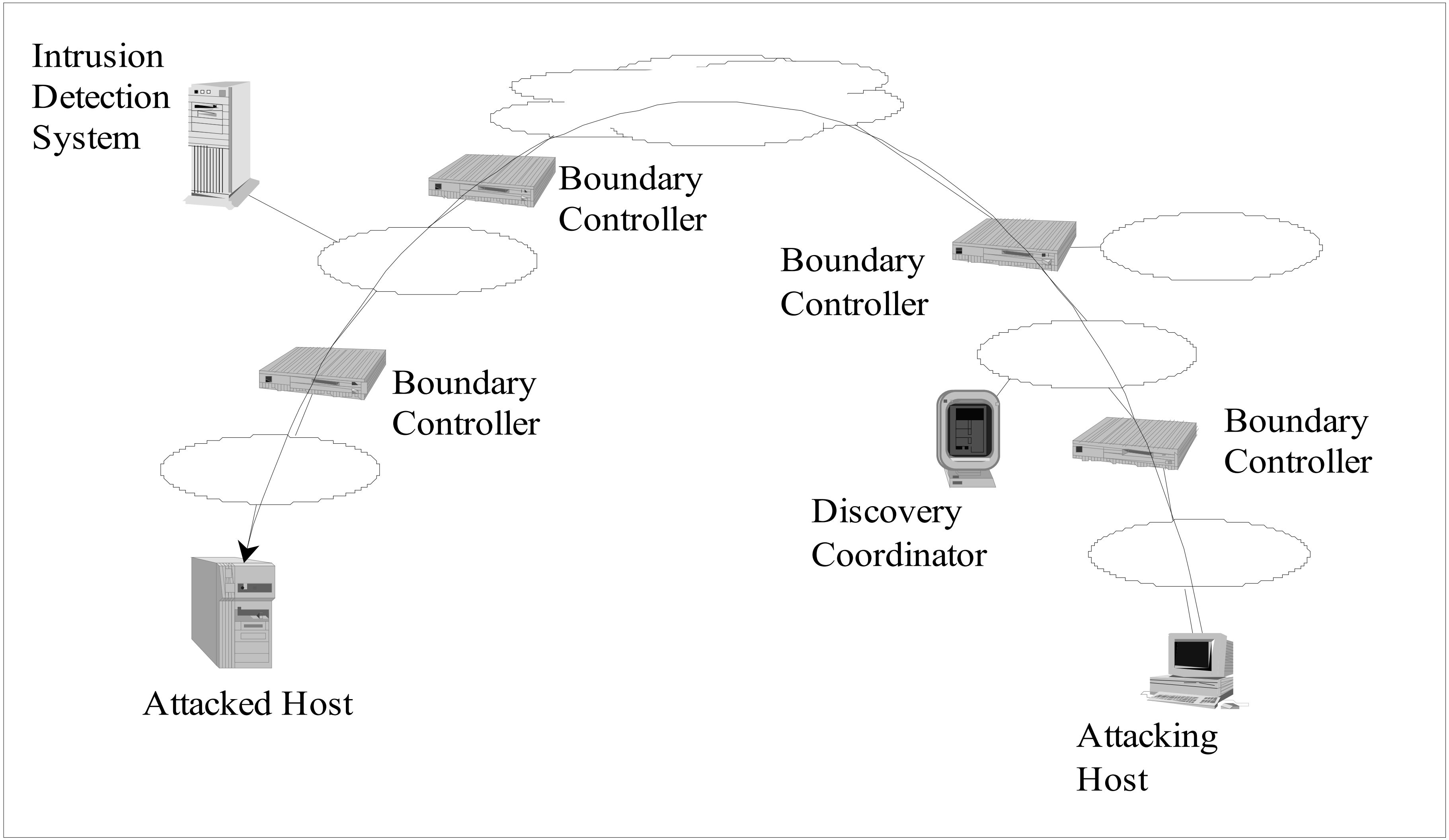
IDIP Nodes

IDIP Architecture cont.



IDIP Communities

DDoS Attack Scenario with IDIP



How IDIP works

- IDIP nodes register their participation in IDIP Neighborhood and community
- On detection of an attack, IDIP node determines if a response is indicated
- IDIP node notifies neighbors, via IDIP message layer of this attack
- Local nodes (IDIP Applications) determine response based on severity, type, rules and components involved

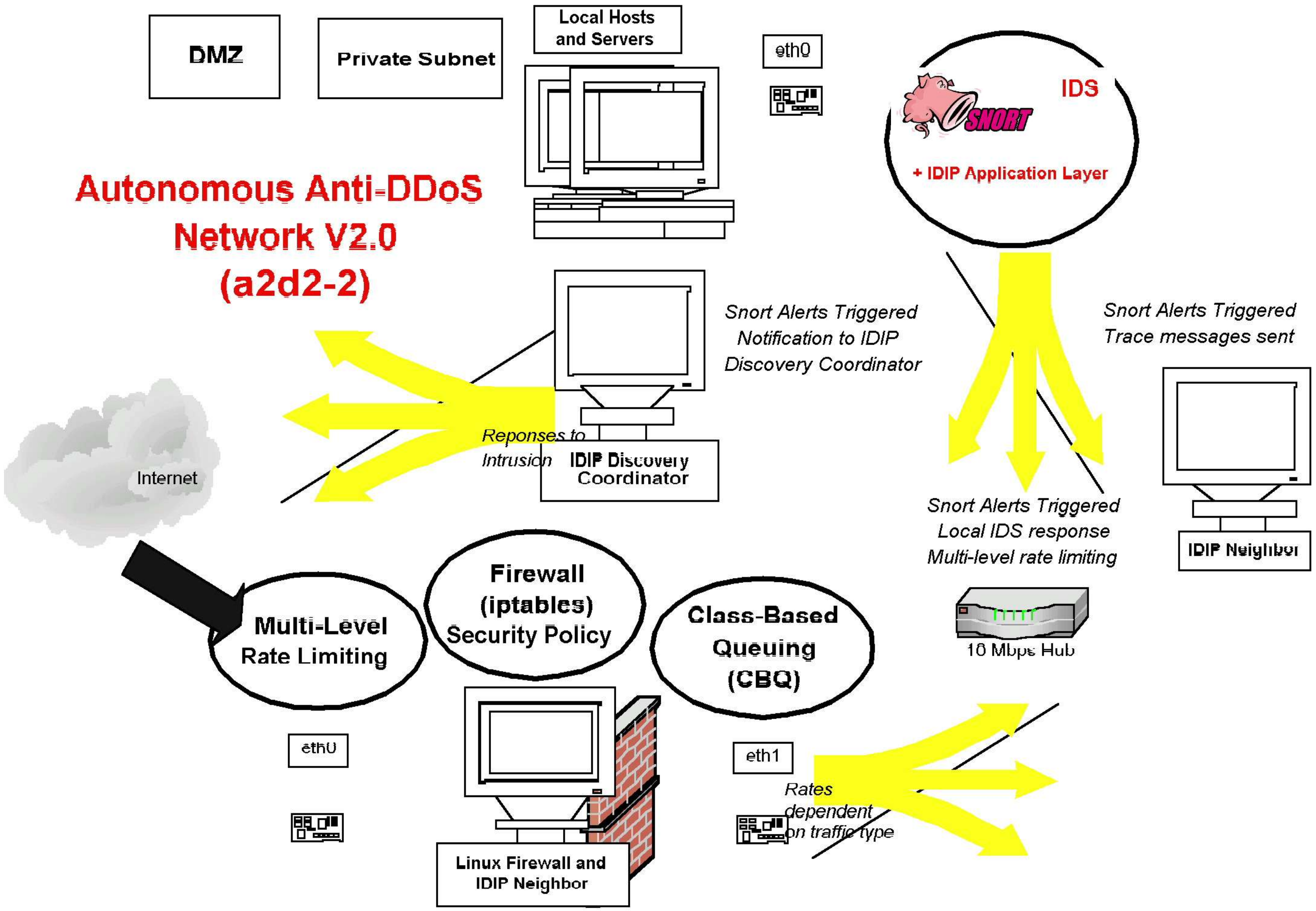
How IDIP works , cont.

- Each IDIP node sends copy of report to IDIP Discovery Coordinator for correlation and updated response actions
- IDIP Discovery Coordinator (part of message layer) notifies other neighborhoods in IDIP community about attack

IDIP Security

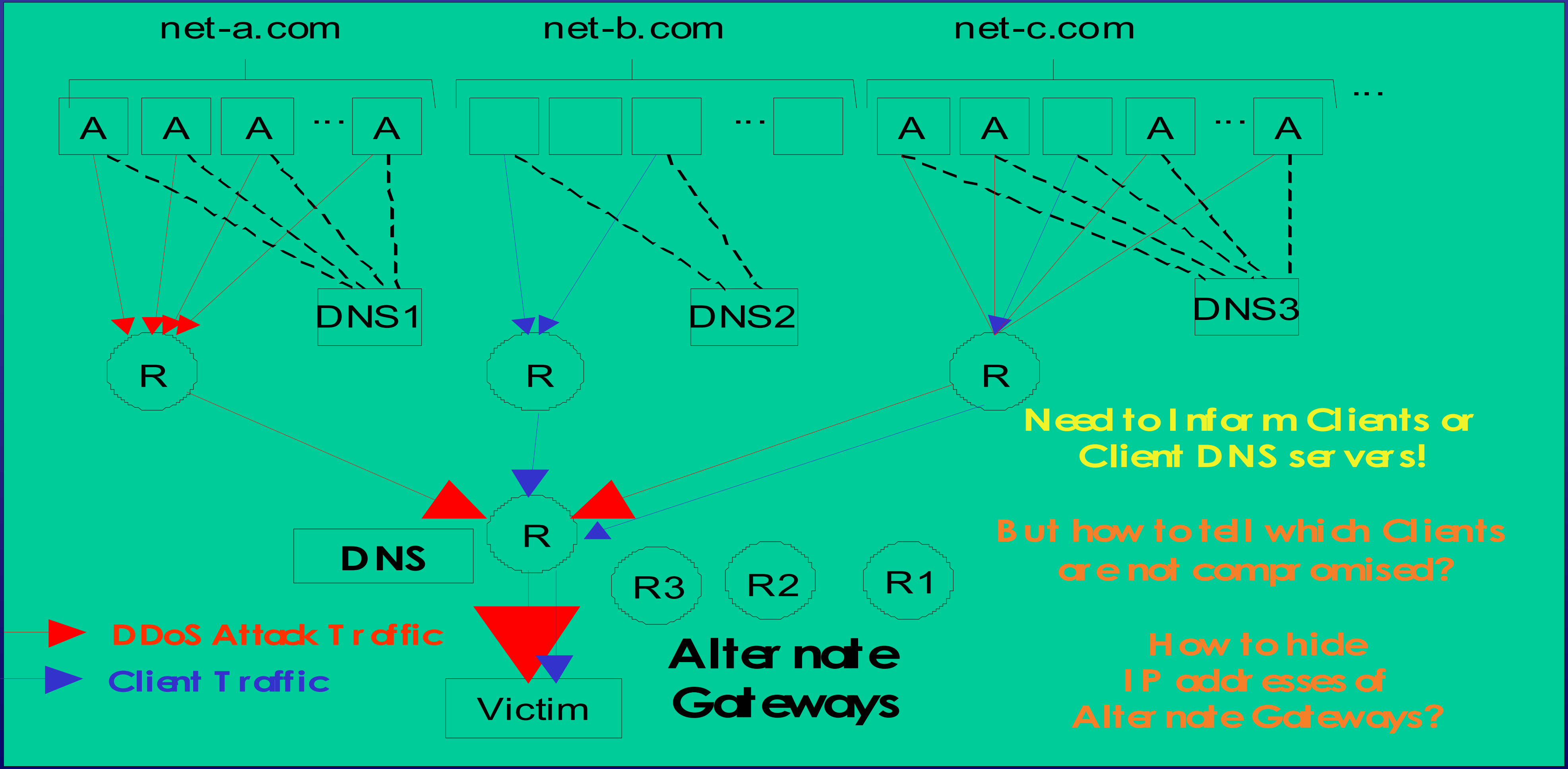
- Security holes:
  - IDIP Message node spoofing
  - Eavesdropping
  - Falsification of data
- How IDIP handles security:
  - Will only forward certain messages
  - Any NKID (Network Key Information Distribution) data is never forwarded
  - Specific NKID protocol handles all validation and verification
  - Supports cryptographic extensions in message layer
  - Each node generates the keys it will use for transmission. Responsible for distribution of these keys
  - Multicast key distribution
  - Provides for both authentication and privacy. Modeled after IPSec

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

Alternate Routes

Implement Alternate Routes



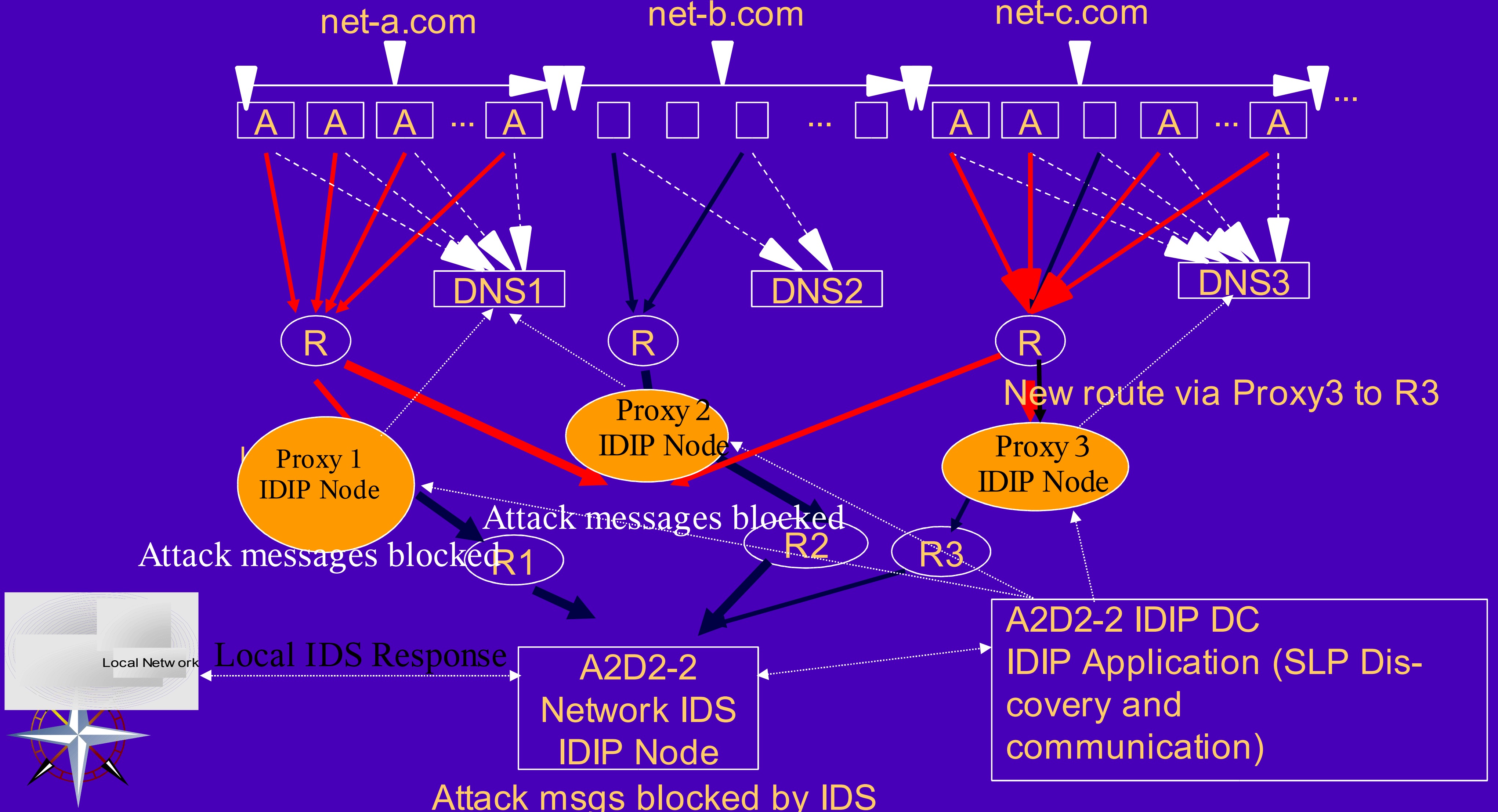
Need to Inform Clients or Client DNS servers!

But how to tell which Clients are not compromised?

How to hide IP addresses of Alternate Gateways?

Alternate Routes, cont.

A2D2-2 & SLP -> Alternate Routes



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