



EMIST
SPARTA DDoS Experimentation
June 2006

Alefiya Hussain

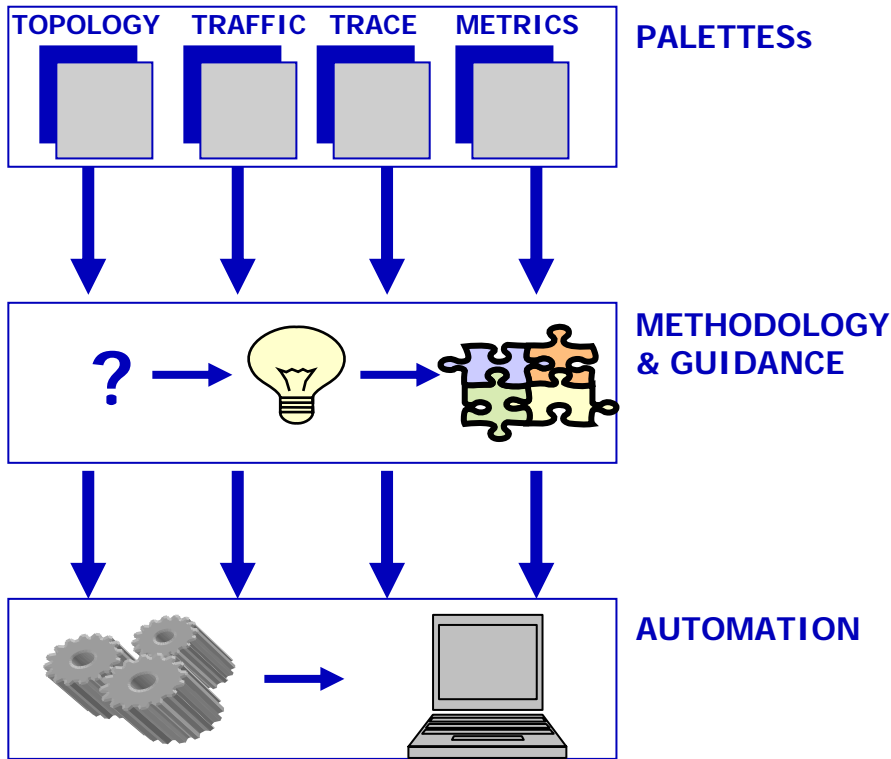
Calvin Ko, Brett Wilson, Steve Schwab,
Roshan Thomas, Dave Balenson



Objective of EMIST

- **Provide methodological guidance**
 - Recommendations for topologies, traffic generators, metrics,
 - Guidelines for interpreting results
- **Create prototypical experiments for conducting realistic, reproducible, impartial tests**
 - For assessing attack impact and defense effectiveness,
 - For analysis software, and experiment automation tools and configurations
- **Facilitate testing and evaluation of prototype and commercial defense systems**

DDoS Experiment Methodology



- *Experimenter selects from a palette of predefined elements: Topology, Background and attack traffic, trace capture and Metrics calculations*
- *Our Methodology frames standard, systematic questions that guide an experimenter in selecting and combining the right elements*
- *Experiment Automation increases repeatability and efficiency by integrating the process to the DETER testbed environment*



SPARTA Experiment Outline

- **Apply the EMIST methodology to evaluate three defense systems**
 - DWARD, COSSACK, and FloodWatch
- **Created reusable library of evaluation technology that allow quick configuration of different dimensions of the of the experiment:**
 - Topology, attack traffic, background traffic, defenses, metrics and measurements
- **SPARTA EMIST tools support automation of evaluation experiments on DETER**



Defense Systems

Requirement: Develop methodology to encompass a wide range of IDS technologies

UCLA D-WARD

Type:

- Source end

Detection Method:

- Collects anomaly stats for each destination at egress router

Evaluation Metrics:

- Legitimate traffic service level
- Per connection delay
- Failed connections

ISI COSSACK

Type:

- Cooperative

Detection Method:

- Signature based coordinated detection at watchdog locations

Evaluation Metrics:

- Percentage of dropped attack packets

SPARTA FloodWatch

Type:

- Core

Detection Method:

- Collects entropy and Chi-squared stats for src and dst IP addresses

Evaluation Metrics:

- Percentage of dropped attack packets

Jelena Mirkovic, D-WARD: Source End Defense Against Denial of Service Attacks. Ph.D Thesis 2003

Christos Papadopoulos et al, OSSACK: Coordinated Suppression of Simultaneous Attacks, DISCEX 2003

L. Feinstein, D Kindred, Statistical Approaches to DDoS Attack Detection and Response, DISCEX 2003

Topology

Requirement: IDS should be evaluated on realistic, scaled-down topologies

Small Canonical Topology

End Systems: 9

Attackers: 4

Routers: 7

Delay Nodes: 25

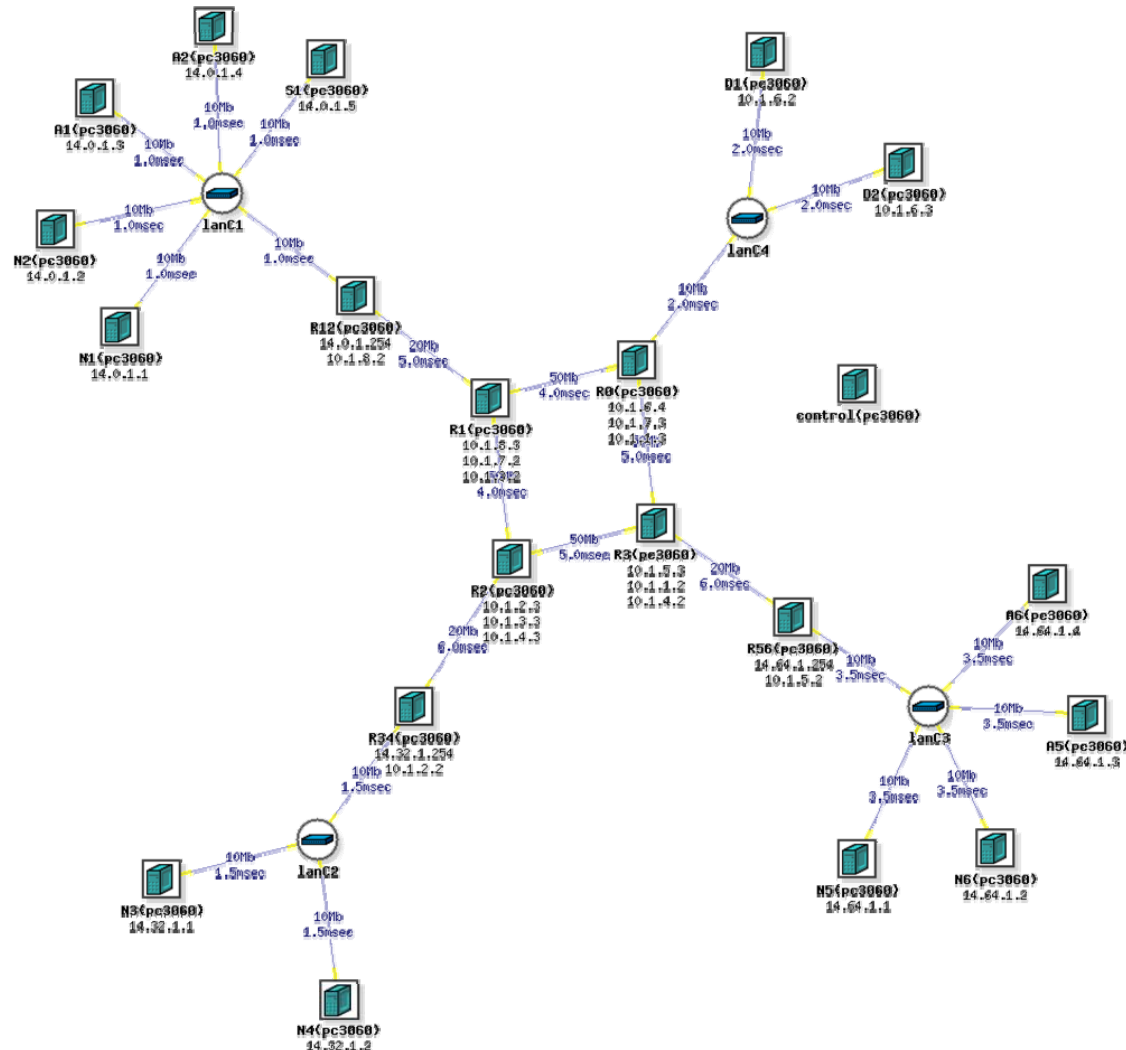
Total Nodes: 45

Range of bandwidth and delay configurations

Asymmetric Routes:

N1-R12-R0-R56-N5

N5-R56-R2-R12-N1





Background Traffic

Requirement: Detection and mitigation of attacks should to be evaluated against a mix of background traffic

TCP Harpoon (WAIL): generates IP flow-level traffic with byte, packet, temporal, and spatial diversity.

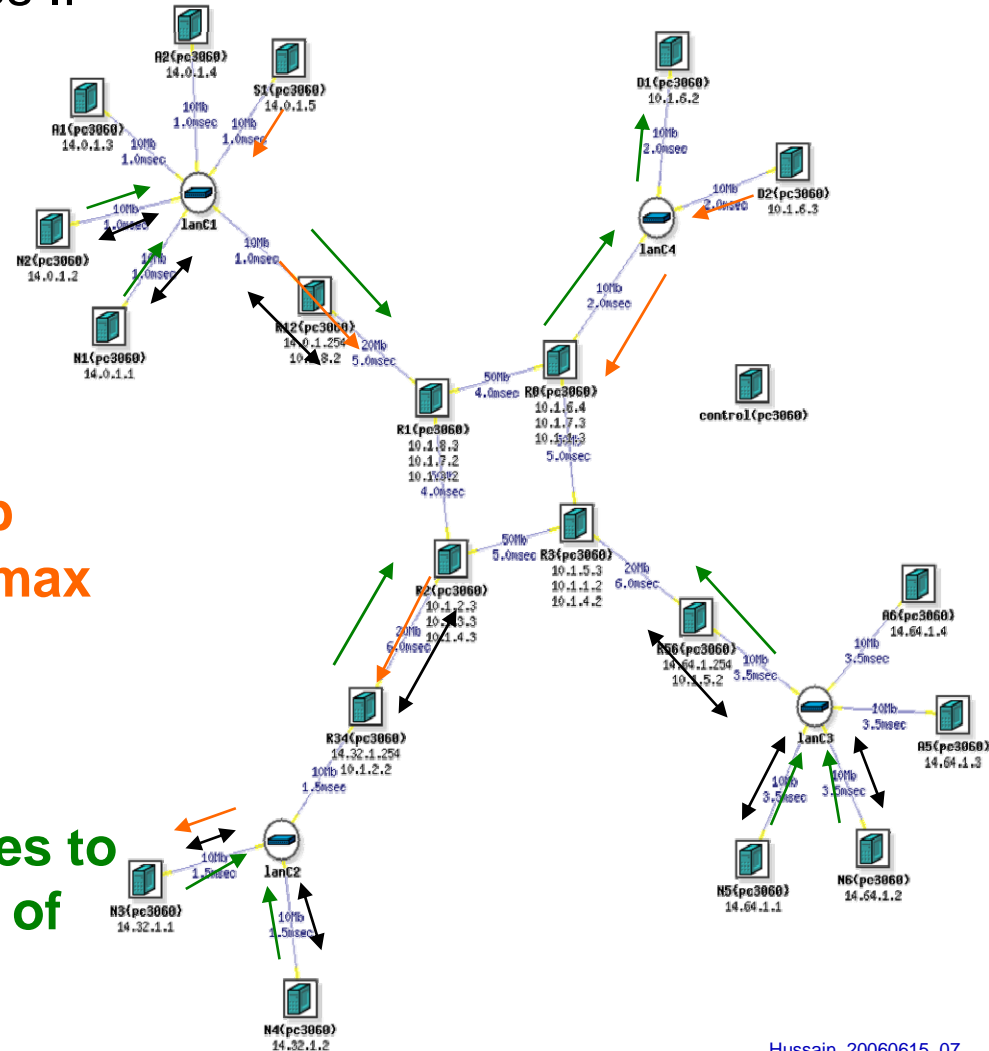
SPARTA Enhancement: IP address diversity where each end node can represent a subnet using Linux NAT.
Nodes: N1-N6

Wget (SPARTA): generates http requests to web servers with min-max thresholds.

Server: N3, Clients: S1,D2

UDP DNS (UDEL): generates queries to server every x sec with probability of request failure.

Server: D1, Clients: N1-N6

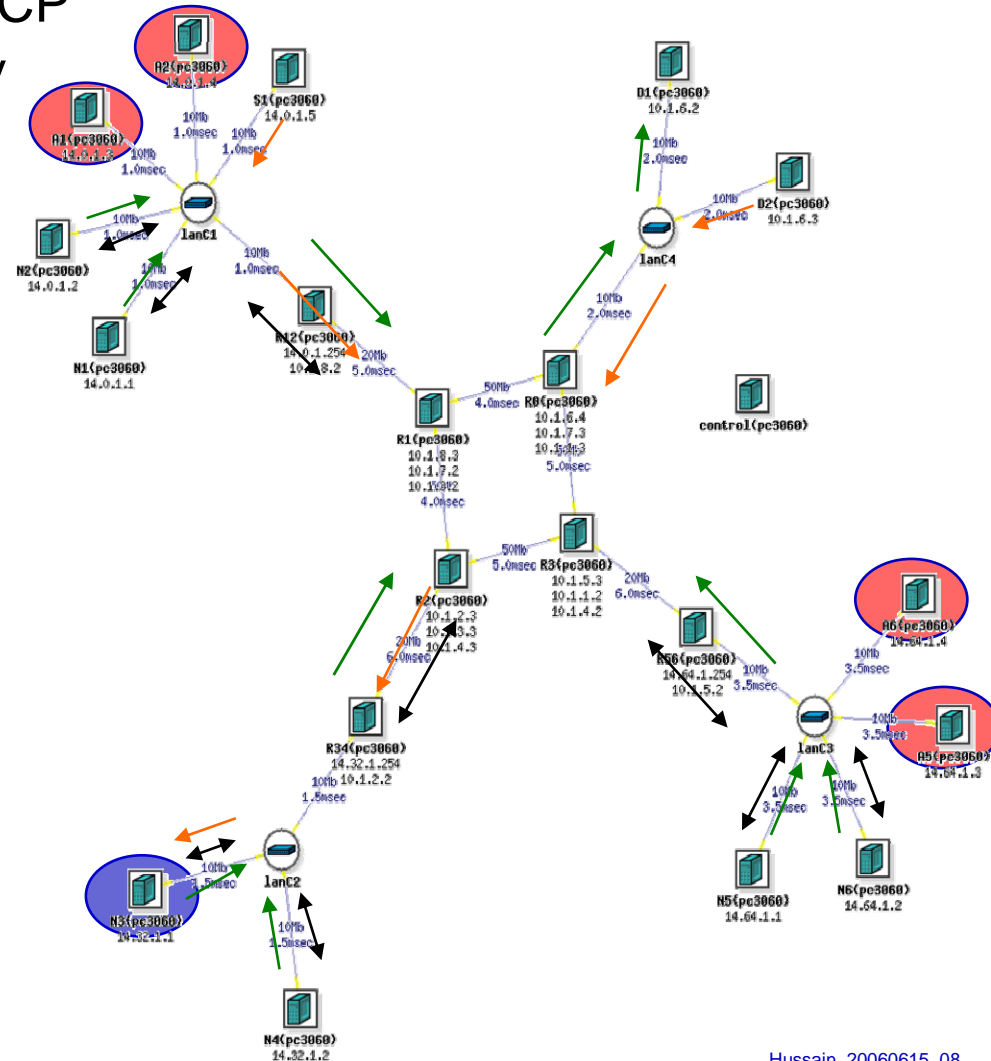
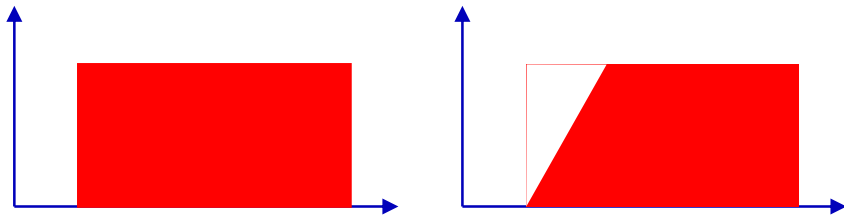




Attack Traffic

Requirement: Evaluate against both existing and future attack strategies

Flooder (SPARTA): generates TCP or UDP attack with ramp-up capability



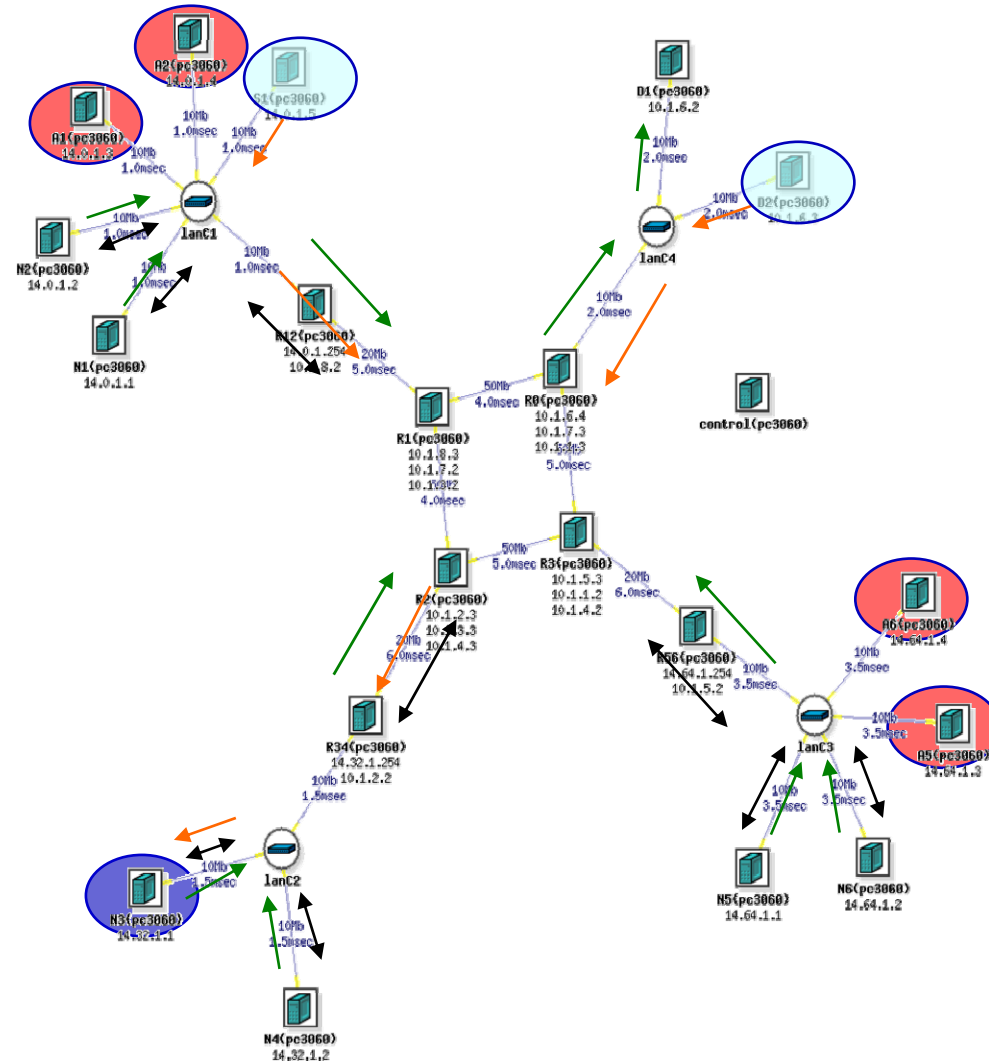
TCP Attack: Attackers: A1-2,A5-6
Victim: N3, Rate: 2Kpps, Size:1KB

UDP Attack: Attackers: A1-2,A5-6,
Victim:N3, Rate:15Kpps,Size:1KB

Measurement

Requirement: Collection of packet traces and host-based logs to support metrics calculation and visualization

- **Full automation to collect**
 - packet traces at each node (end host and router) in the network
 - system log files, IDS log files, attacker logfiles
 - instrumentation to record aggregate packet counts at each router for rapid visualization
- **Compute metrics on packet traces of Wget traffic captured at S1 and D2**





Metrics

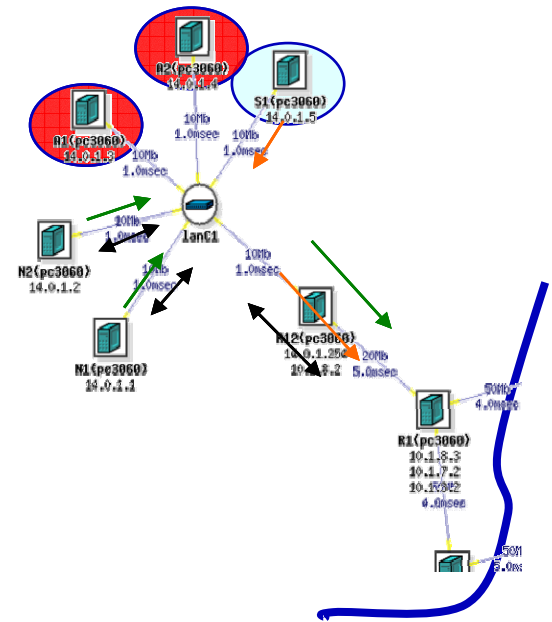
Requirement: Defense metric should encompass the quality of network service perceived by the end user

- **IDS defense should prevent degradation or restore end user application behavior to as before attack**
 - Delay, loss, and jitter based on application type
- **Current focus on only web applications at S1 and D2**
- **Calculate three metrics (Tool by J. Mirkovic, UDel)**
 - *goodput*: transaction transfer rate
 - *delay*: maximum one-way delay
 - *%success*: number of successfully completed transactions

Results: Metrics at S1

Type	Goodput	Delay	%Success
B-No Attack	49K	0.06s	98
B-TCP	45K	0.05s	77
B-UDP	na	na	0
D-TCP	28K	0.31s	58
D-UDP	na	na	0
C-TCP	31K	0.19s	58
C-UDP	na	na	0
F-TCP	32K	0.27s	81
F-UDP	6.5	3.7	14

Metrics such as dropped attack packets do not provide insight to protection offered by IDS

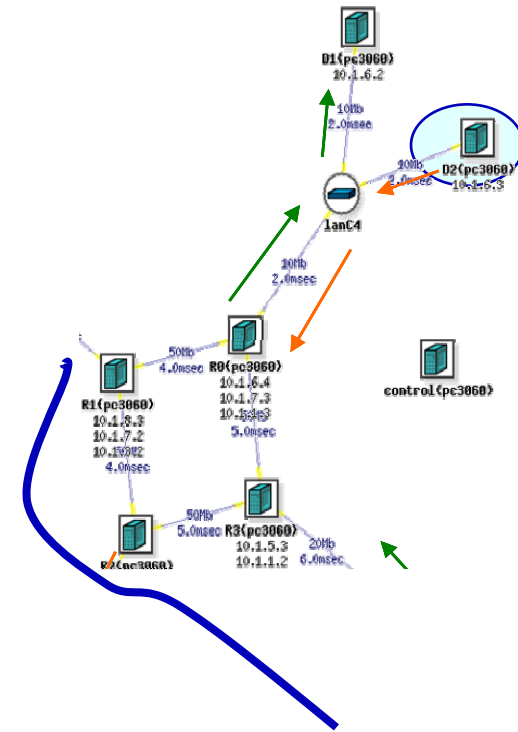


- S1 on same subnet as attackers
- D-WARD and FloodWatch filter 90% of TCP and UDP attack packets however 40% of TCP transactions fail
- COSSACK does not filter UDP attack



Results: Metrics at D2

Type	Goodput	Delay	%Success
B-No Attack	45K	0.06s	98
B-TCP	48K	0.05s	99
B-UDP	na	na	0
D-TCP	50K	0.06s	100
D-UDP	50K	0.06s	100
C-TCP	38K	0.12s	89
C-UDP	na	na	0
F-TCP	37K	0.11s	95
F-UDP	24K	0.06s	26



- **D2 on different subnet**
- **D-WARD and FloodWatch filter 90% of TCP and UDP attack packets**
- **COSSACK does not filter UDP attack**

Significantly higher completed connections and lower latencies for all IDS



Conclusions

- Created a *reusable* library of technologies that can be used for conducting realistic, rigorous, and reproducible IDS evaluations
- Provided *usage examples* and *methodological guidance* for selecting various experiment elements and interpreting results
- Support for *automation* allowing repeatability, efficiency and ease-of-use
- Extensive *collaboration* with bi-weekly meetings with the DDoS Working group and UDel to converge on common methodology and metrics for DDoS benchmarking



Ongoing and Future Work

- **Enrich and improve tool set**
 - ICMP traffic generator, TCP Replay
 - Additional attack tools, Cleo (UDEL)
- **Evaluate against additional methodology elements**
 - Deployment and testing on complex rocketfuel topologies (Purdue)
 - Working to acquiring AT&T Pushback IDS implementation
 - Developing Click-based RED-PD implementation in-house
- **Develop additional metrics and benchmarks through synergies with other projects**