Classification of UDP Traffic for DDoS Detection

Alexandru G. Bardas, Loai Zomlot, Sathya Chandran, Xinming Ou
Kansas State University
{bardasag, xou, lzomlot, sathya}@ksu.edu

S. Raj Rajagopalan, Marc R. Eisenbarth
HP Labs, HP TippingPoint
{raj.rajagopalan, marc.r.eisenbarth}@hp.com

VISA MasterCard PayPal™

FBI DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION POLICE

DEPARTMENT OF JUSTICE QUI PRO DOMINA JUSTITIA SEQUITUR

UNIVERSAL®

UNIVERSAL MUSIC GROUP

2010

2012

Why UDP based DoS/DDoS?

- Reportedly a significant part of the recent effective DDoS attack traffic was based on UDP
- Our work is focused on detecting DoS/DDoS **flooding attacks** leveraging **UDP** packets
- **Free tools** that perform flooding attacks: Low Orbit Ion Canon (LOIC), Stacheldraht, Trin00 *etc.*
- Despite past research, we still lack practical solutions to deal with UDP DoS/DDoS attacks

User **D**atagram **P**rotocol

- UDP is a **transport protocol** that offers **minimal** transport service
- UDP Packet:

16 bits	16 bits
Source Port (optional)	Destination Port
Length	Checksum (optional)
Payload	

- UDP does **NOT** provide **reliability**, **datagram ordering** and **data integrity**

UDP DoS/DDoS Characteristics

- Usual UDP flooding packets properties:
  - Every packet has the **same payload**
  - The **source IP** address may or may **NOT** be **spoofed** (more effective if it's not randomized)
- In case of a **flooding attack** there is a one-way flood of packets

UDP DoS/DDoS Detection Challenges

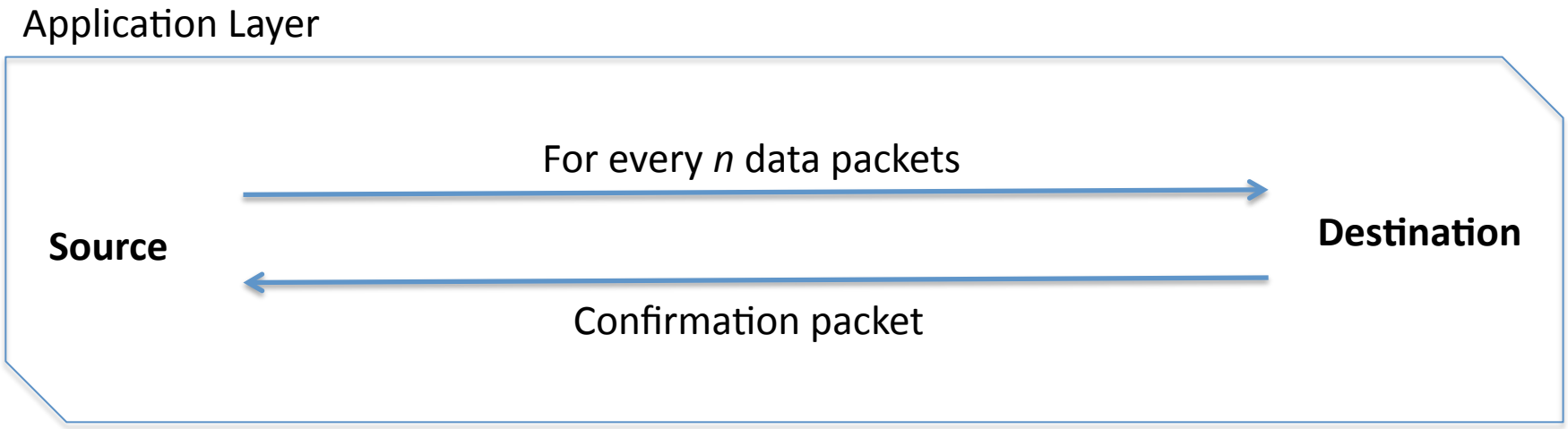
- **Unique payloads** can be generated for every single UDP packet
- **Replay attacks** – attackers may send previously recorded benign UDP traffic
- **UDP is stateless –** DoS/DDoS prevention methods based on connection state are not applicable

The Proportional Packet Rate Assumption

"During normal operation, the packet rate of traffic going to an address is proportional to the packet rate of traffic going from that address"

[T.M. Gil, M. Poletto, ***MULTOPS: a data-structure for bandwidth attack detection,*** 2001]

Packet-Ratio Intuition



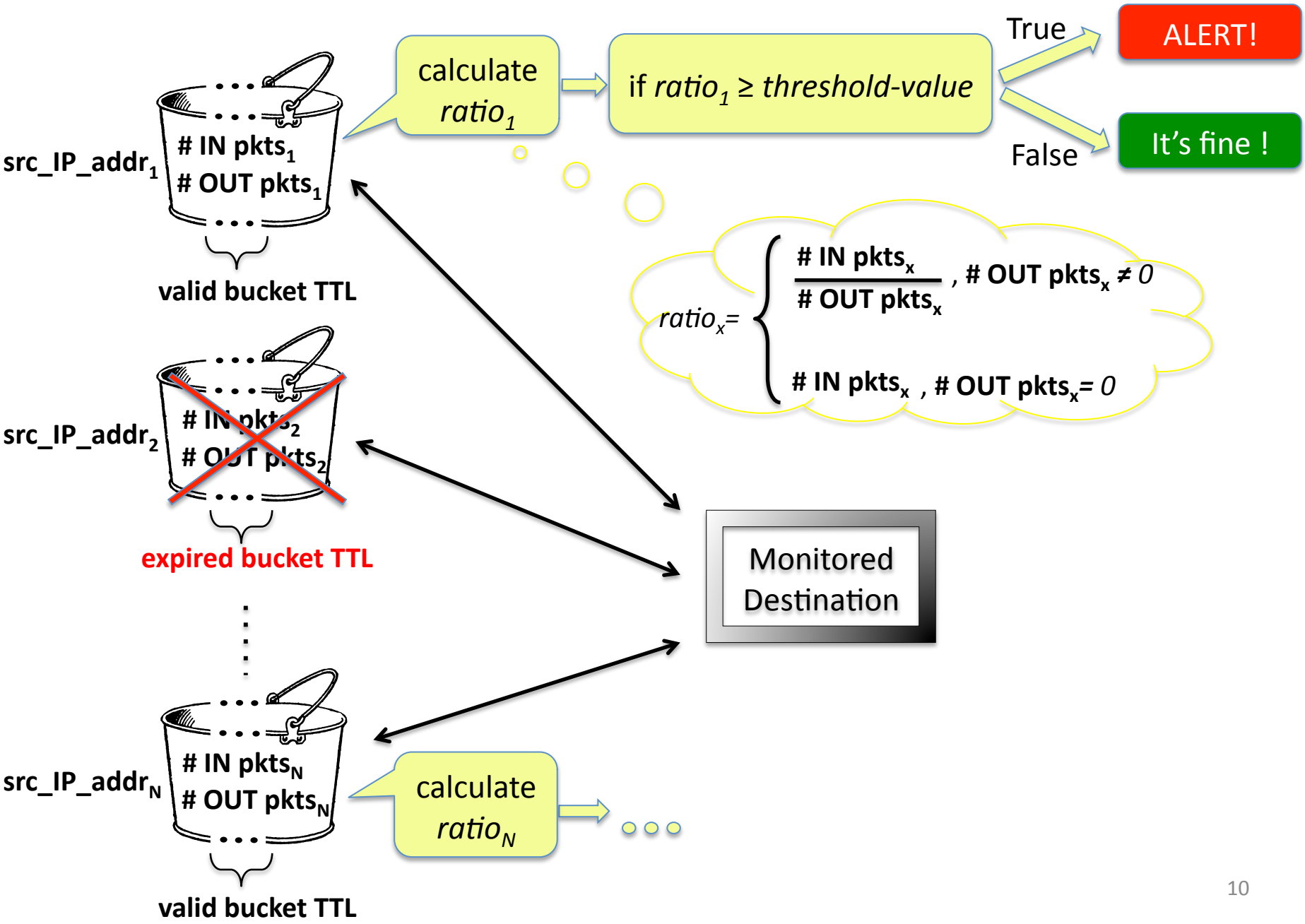
Hypotheses:

- Under normal operation the ratio will be less than a predefined allowed maximum threshold value
- Ratio can be used to separate benign traffic from attack traffic

Using the Proportional Packet Rate Assumption in a Classifier

- DoS/DDoS flooding attacks can be detected early at the victims side by calculating the ratios for every single sender
- We developed a classifier based on the proportionality assumption
- Classifier monitors an enterprise network to detect possible DDoS flooding attacks targeted at it

Classifier – Basic Approach



Experimentation

- **Hypotheses**:
  - Under normal operation the ratio will be less than a predefined allowed maximum threshold value
  - Ratio can be used to separate benign traffic from attack traffic
- Measured the ratio for benign and attack traffic on:
  - **Synthetic Data**:
    - Own testbed at Kansas State (Argus CyberSecurity Lab)
    - DeterLab
  - **Production Networks**:
    - Our departmental network (**CIS** - Computing and Information Sciences)
    - Non-DNS UDP packet captures from **twelve distinct networks**

argus
Kansas State University

CyberSecurity Lab

CyberSecurity Education at CIS

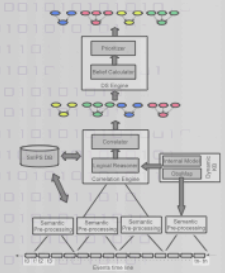
We provide rigorous training for our students on cyber defense capabilities in the real world. The CIS department offers a series of undergraduate and graduate courses in cybersecurity.

- CIS 490/798: Cyber Defense Basics
- CIS 551/751: Introduction to Computer and Information Security
- CIS 553/753: Applied Cryptography
- CIS 590/798: Secure Networks and Distributed Systems
- CIS 890: Research Topics in Security

Scholarship Opportunities

The CIS Center for Information and Systems Assurance (CISA) at Kansas State University is a National Center of Academic Excellence in Information Assurance Research (CAE-R) designated by National Security Agency (NSA) and Department of Homeland Security (DHS). CISA provides scholarship opportunities for both undergraduate and graduate students through the DoD Information Assurance Scholarship Program (IASP) and other federal agencies.

Start from REAL problems, Create solutions that LAST



SnIPS Intrusion Analysis System

Snort Intrusion Analysis using Proof Strengthening is an advanced intrusion analysis framework that utilizes both logical and probabilistic reasoning techniques to handle the inherent uncertainty ubiquitous in all intrusion detection alerts. We have close collaboration with our industrial partners --- ArcSight, CABEM, HP-ES, and TippingPoint, to deploy this technology on production networks, and further our research to tackle the grand challenge of reasoning under uncertainty for cybersecurity..

MulVAL Attack Graph System

Multi-host, muli-stage Vulnerability Analysis Language adopts Datalog to express generic security knowledge about cyber attacks, and can find all possible intrusion paths in a network automatically. MulVAL has been successfully used by the North Atlantic Treaty Organization (NATO), Defence Research & Development Canada, National Institute of Standards and Technology (NIST), Idaho National Laboratory, and a number of academic institutions.

Cyber Defense Club

We provide facilities and trainings for students interested in hacking and counter-hacking. Please come join us in the club activities, competitions,and other fun stuff!

We do research that helps cyber defenders. We believe effective defense must utilize collective intelligence, connect the dots from multiple vantage points, and reason about them under the inherent uncertainty in the observations.

Funding

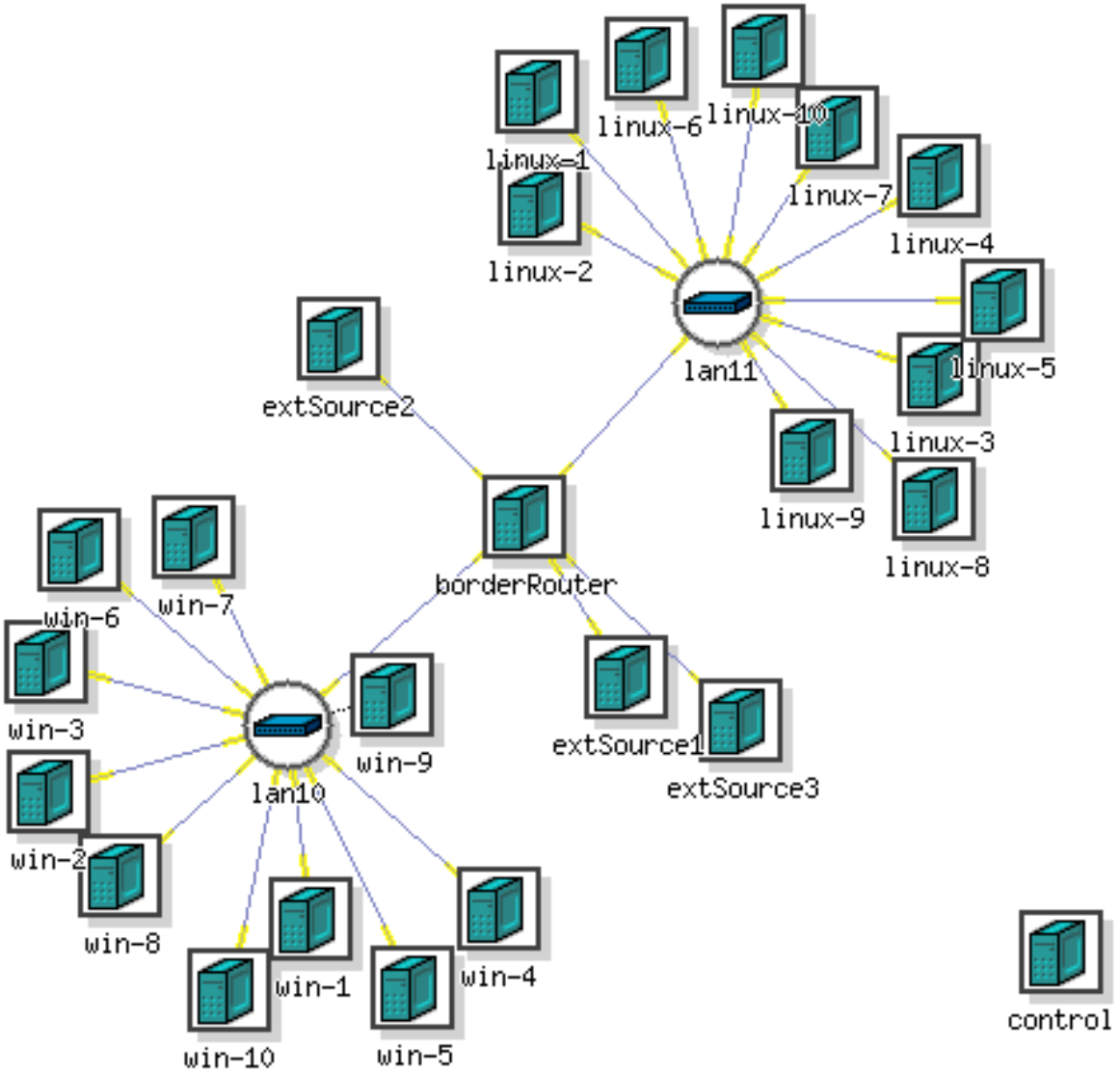
U.S. National Science Foundation
U.S. Department of Defense
U.S. Department of Energy
Idaho National Laboratory
HP Labs

Collaborators

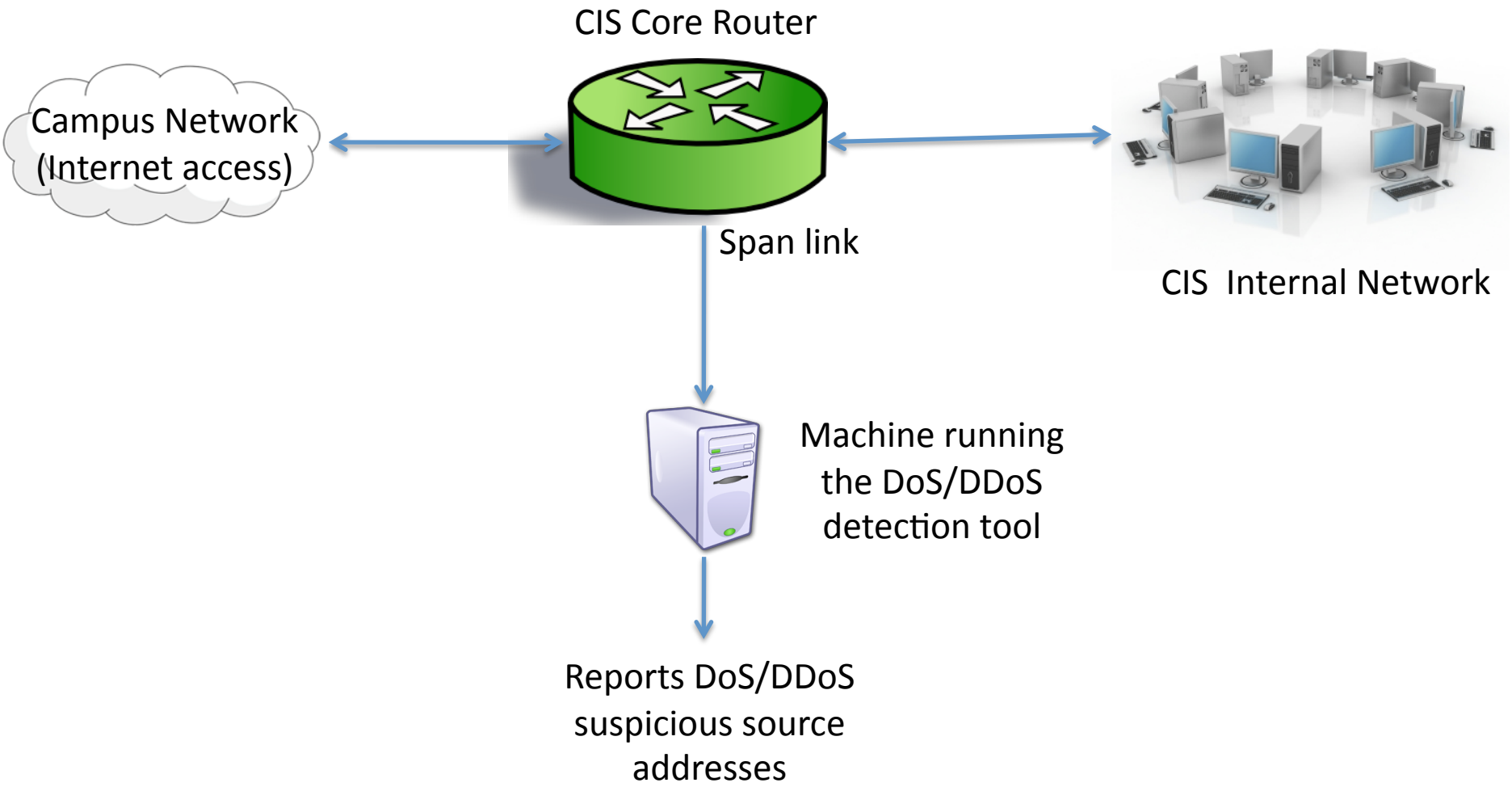
We have active collaborations with members of CISA on a number of innovative research projects. We also have close collaboration relationships with a number of industrial and government partners.

HP Labs
Defence Research & Development Canada
National Institute of Standards and Technology
Idaho National Laboratory

DeterLab Setup



CIS Departmental Network Setup



Twelve Distinct Networks

- Data from a large number of production networks including:
  - Large corporations (edge and core)
  - ISPs
  - Universities
  - Financial institutions
- For privacy reason DNS traffic was removed and names cannot be revealed
- Data was captured between 2002 and 2012

Benign UDP-Traffic Ratios Variations

BTTL in sec	Argus Testbed	DeterLab	Data from Production Networks							
			CIS	D+	G	ISP	O+	S	T	C0
1	51	281	200	1090	9	85	330	80	41	85
2	41	411	300	1305	18	85	560	95	28	135
3	54	560	450	1305	21	85	580	115	28	141
4	43	728	600	1305	21	85	790	121	30	141
5	42	778	700	1305	21	85	915	129	41	141
. . .										
100	42	1230	2500	1305	30	85	11600	1680	122	820
600	12	1230	2500	1305	30	285	20300	2600	512	1070

Legend:

Symbol	Meaning
+	contains one-way protocols

Attack Traffic Ratios

Time into the Attack (sec)	Ratio – ArgusTestBed (w/ LOIC traffic)		Ratio – DeterLab (w/ LOIC traffic)	
	Highest Speed	Lowest Speed	Highest Speed	Lowest Speed
1	≈ 44,000	≈ 250	≈ 75,000	≈ 97
2	≈ 88,000	≈ 500	≈ 150,000	≈ 200
3	≈ 132,000	≈ 750	≈ 225,000	≈ 300
4	≈ 220,000	≈ 250	≈ 75,000	≈ 100
5	≈ 430,000	≈ 500	≈ 150,000	≈ 200
6	≈ 660,000	≈ 750	≈ 225,000	≈ 300
…				
34	≈ 220,000	≈ 250	≈ 75,000	≈ 100
35	≈ 430,000	≈ 500	≈ 150,000	≈ 200
36	≈ 660,000	≈ 750	≈ 225,000	≈ 300

Attack Traffic is present and BTTL = 3 sec

Results Analysis (1/2)

- Benign applications use UDP packets in different ways:
  - ***Constant* communication** between sender and receiver
    - Examples: NFS, video streaming applications (Sopcast)
  - **Initial communication** and then a **one-way burst** of UDP packets
    - Examples**:** SIP (Session Initiation Protocol), T.38 protocol (fax)
  - **One-way burst of packets** (by protocol design no response message is necessary)
    - Examples: Syslog over UDP, Netflow (older versions)
- Hypotheses hold if the cutoff pair values (threshold value - BTTL) are appropriately chosen

Results Analysis (2/2)

- DDoS attempt discovered in the *ISP* dataset
  - Benign Ratio was approx. 85
  - Discovered using a sequence of classifiers (with different cutoff pair values) to monitor the same target

Duration (sec)	1	2	3	4	5	6	…	34	35	36	…	124
Ratio	≈21	≈ 39	≈ 45	≈ 64	≈ 84	≈ 99	…	≈ 100	≈ 218	≈ 349	…	≈ 373

Limitations & Future Work

- **Spoofed** (especially **randomized**) **IP addresses** and **N**etwork **A**ddress **T**ranslation setups can cause problems for the classifier
- Inline version of the classifier is under development
  - Interacts with the source by blocking the incoming packets for a very short time (*NACK* feature)

Conclusion

- Designed a UDP traffic classification algorithm based on the proportional-packet rate assumption
- Proportionality assumption examined through experimentation on a large number of data sets from production networks and various testbeds
- Experimentation results provide key observations for DoS/DDoS detection