Classification of UDP Traffic for DDoS Detection

Alexandru G. Bardas*, Loai Zomlot*, Sathya Chandran*,
Xinming Ou*, S. Raj Rajagopalan+, Marc R. Eisenbarth#

*Kansas State University, +HP Labs, #HP TippingPoint

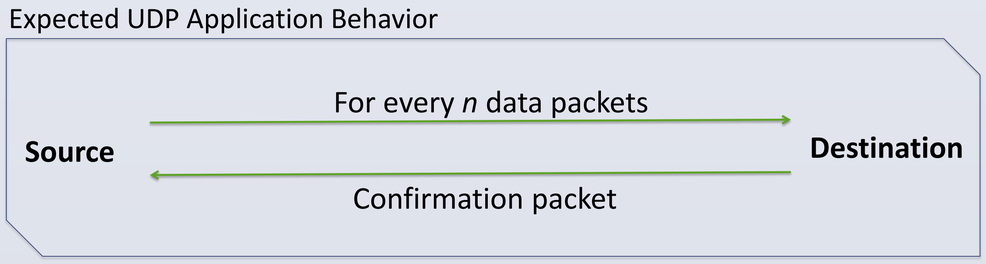
PROBLEM

PROPOSED SOLUTION

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

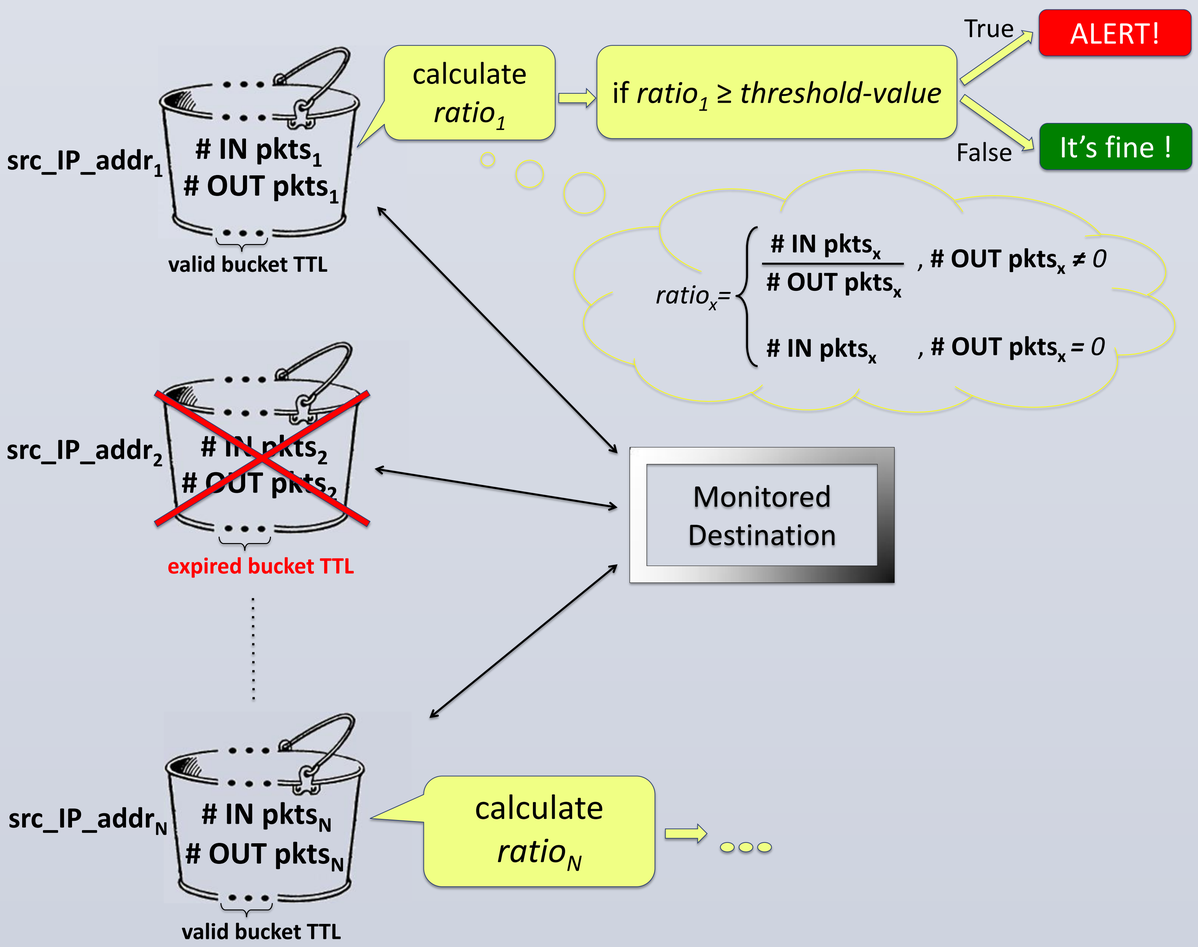
[T.M. Gil, M. Poletto, ***MULTOPS: a data-structure for bandwidth attack detection***, 2001]

Expected UDP Application Behavior



Hypotheses:

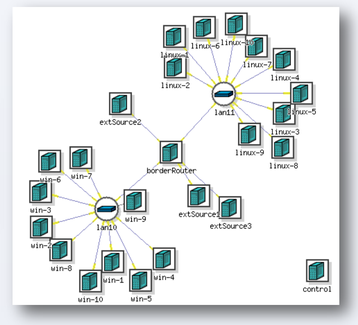
- Under normal operation the ratio will be less than a predefined maximum threshold value
- Ratio can be used to separate benign traffic from attack traffic



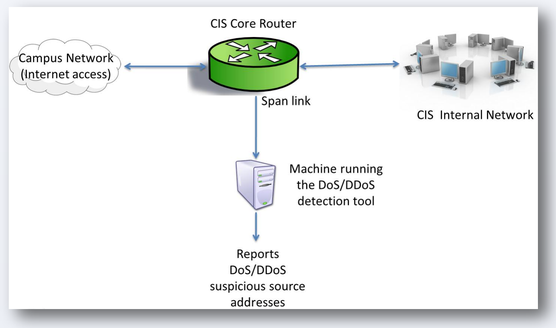
EXPERIMENTATION

Testing Environments:

Argus Testbed



DeterLab



CIS Departamental Network

Twelve Distinct Production Networks:

Universities, financial institutions, ISP's, large corporations *etc.*

Results:

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

* 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

Results Analysis:

Benign applications use UDP packets in different ways:

- ***Constant* communication** between sender and receiver. Examples: NFS, video streaming applications (*e.g.* 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

REFERENCES

- A. G. Bardas, L. Zomlot, *et al*. Classification of UDP traffic for DDoS detection. In *5th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2012.
- T. M. Gil and M. Poletto. MULTOPS: a data-structure for bandwidth attack detection. In *Proceedings of 10th Usenix Security Symposium*, 2001.

ACKNOWLEDGEMENT

This research was funded by the U.S. National Science Foundation under award no. 1038366 and 1018703, and HP Labs Innovation Research Program. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation, or Hewlett-Packard Development Company, L.P.