Classification of Internet Traffic

Alok Shriram

Need for Classification

- Classification required
  - To isolate traffic of interest
  - To treat special types of traffic in a different manner
- Some types of classification already seen in AI learning systems.
- Some types of classification seen in Data mining.

Three Techniques

- A Framework for Classifying Denial of Service Attacks (Single or Multiple Source Attacks)
- Identification of Repeated Attacks Using Network Traffic Forensics.
- Class of Service Mapping for QoS.

Identification of Repeated Attacks Using Network Traffic Forensics

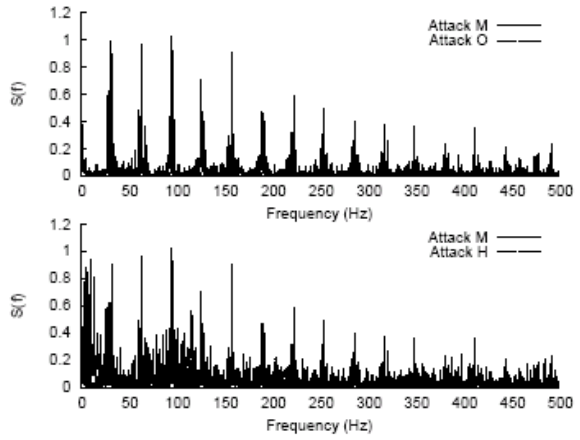
- To Identify repeated attacks
- Forensic evidence used to investigate and establish facts
- Depending on Intent attackers punishment is decided

Objective

- Build an attack fingerprinting system
- Make this system of creating fingerprints automatic
  - Fingerprint is any characteristic feature of an attack which can uniquely identify it.
- Automatic matching system
- Identify repeated attacks

Methodology in a Nutshell

- Given an attack scenario
  - Figure out if attack has occurred previously.
- For this we filter attack
- Create attack fingerprint
- Compare attack to previously fingerprinted attack



Creating Attack Fingerprint

- Convert packet trace into time series
- Consider interval of time p
  - Packet arrivals [t, t + p)
- For T second trace T/p samples
- Max frequency 1/2p Hz
- Use p=1 msec and attack segment length =2 s

Creating Attack Fingerprint(1)

- Thus we have time series x(t).
- Compute autocorrelation function(ACF) of time series
- Compute ACF for different values of L to get $r_k(L)$
- Compute FFT of $r_k(L)$
  - Periodicity shows up as dominant frequency.

Creating Attack Fingerprint(2)

- Ideally exact match identifies complete spectrum
- However
  - Adds complexity
  - Needs more samples
- Thus we take the twenty most common samples

Creating the fingerprint(3)

- F_a consists of all segment fingerprints X_k
- Use F_a to compute digest

  M_a=mean of X_k

  C_a= covariance of X_k
- $N_a/\#X_k >=10$
  - Thus N_a=20

Creating the fingerprints (Finally)

- F_a is 20 by 200 matrix
- M_a vector of size 20
- C_a vector of size 20 by 20

Comparing Fingerprints(1)

- Use a comparator to match similarity
- Bayes ML classifier
  - Assumptions
    - Spectral profiles normal w.r.t dominant frequency
    - Each scenario equally likely
    - Attacks are independent

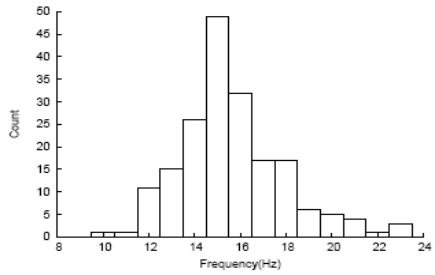


Figure 2: The distribution of the first dominant frequency in F_A for 200 attack segments is approximately normal.

Comparing Fingerprints(2)

- With each attack we just need some information to compare each segment against signature
- Quantify separation between current attack and signatures

Analyzing the results

- Low_{CA} 5 % quartile indicate the at least 5 % match very accurately
- 95%-5% small range of this indicates precision.

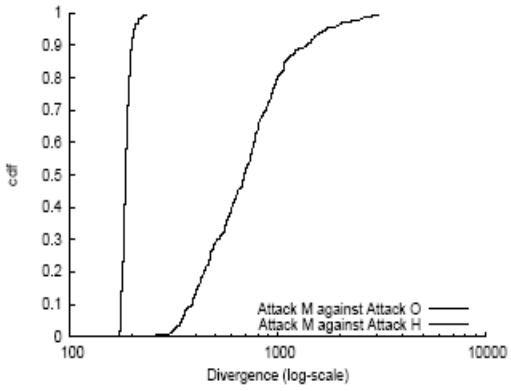


Figure 3: The maximum-likelihood values when comparing the attack M with attacks O and H.

Experimental Results (1)

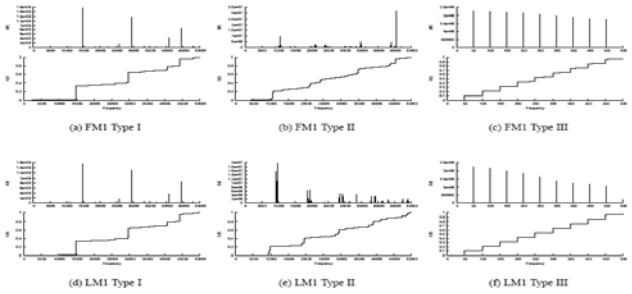


Figure 7: Effect of the operating system on the attack fingerprint

Experiments and Results (2)

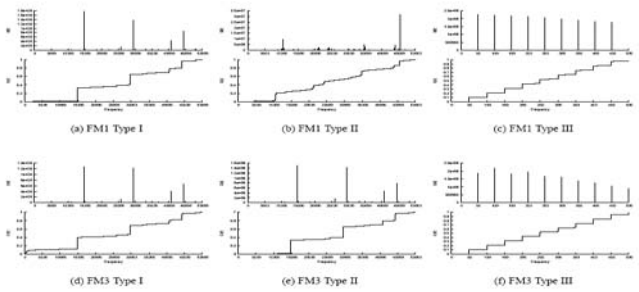


Figure 8: Effect of CPU on the attack fingerprint

A Framework for Classifying Denial of Service Attacks

- Denial Of Service Attacks are of two types
  - Single Source
  - Multiple Source
- Identifying the number of sources helps in mitigation strategies

Objective

- Develop framework to classify attacks as single or multiple source
  - Use Ramp up behavior
  - Port numbers
  - Spectral Characteristics of attack traffic
- Spectral content cannot be spoofed
- Could be used in DOS detection and response systems

Two Types of Attacks

- Software Attacks
- Flooding Attacks
  - Single Source
  - Multiple Source
  - Reflector Attacks

Classifying Attacks

- Three Methods that are used for classification
  - Header Content
  - Ramp-up Behavior
  - Spectral Characteristics

Header Content

- Use fragment ID field and TTL field
  - Single hosts monotonically increasing
  - Multiple Hosts
    - Many ID sequences
    - Two sequence considered unique if they have an IDgap >16
    - ID gap is there to tolerate moderate packet reordering.

Version (4 bits)	Header Length (4 bits)	Type of Service (8 bits)
Packet Length (16 bits)		
Packet Identifier (16 bits)		
Fragmentation Data (16 bits)		
Time to Live (8 bits)	Protocol (8 bits)	
Header Checksum (16 bits)		
Source Address (32 bits)		
Destination Address (32 bits)		

Ramp-up Behavior

- Single sources don't exhibit a ramp-up behaviour
- Multiple source with large number of processes
  - Exhibit ramp up behavior
  - Clock and RTT skews cause gradual buildup
  - By observing this we can guess the number of sources.

Spectral Analysis

- Stuff about spectra analysis here from previous slides..

Experiments: Packet Header Analysis

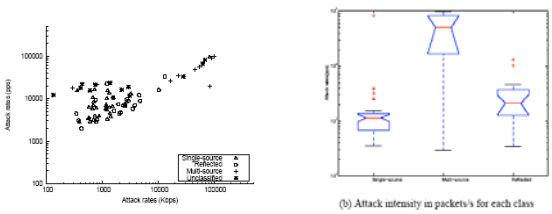
Attack Class	# Attacks	Range (packets/s)	Range (kbits/s)
Single-source	37	350–82500	2700–93000
Multi-source	10	300–98000	17000–100000
Reflected	20	340–13000	3000–33000
Unclassified	13	400–68500	12000-66000

Table 1: Number of attacks in each class based on header analysis

Protocol	Packet Type	Attack Class S	M	R	U
TCP	SYN	2	3 (2)	-	7 (5)
	ACK	5	2 (2)	-	3 (2)
	SYN-ACK	9	-	4	-
	no flags	15	1 (1)	-	-
	unusual	5	1	-	-
	state exploit	2	-	-	-
ICMP	echo request	5	-	-	-
	echo reply	1	-	16 (3)	-
	invalid	-	-	-	1 (1)
UDP	all	6 (1)	-	-	5 (4)
Other	ip-proto 0	5	-	-	-
	ip-proto 255	-	3	-	-
	fragmented	1	-	-	3 (3)

Table 2: Detailed analysis of packet headers. *S* indicates single-source, *M* indicates multi-source, *R* indicates distributed reflectors, and *U* indicates unclassified attacks. The number in parenthesis indicates attacks terminating within our ISP while the first number indicates total attacks.

Experiments: Arrival Rate Analysis

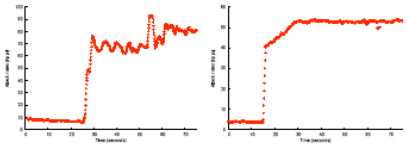


(a) Attack intensity in packets/s and Kbits/s

(b) Attack intensity in packets/s for each class

Figure 4: Correlation of attack rates and attack class

Experiments: Ramp Up Behavior Analysis

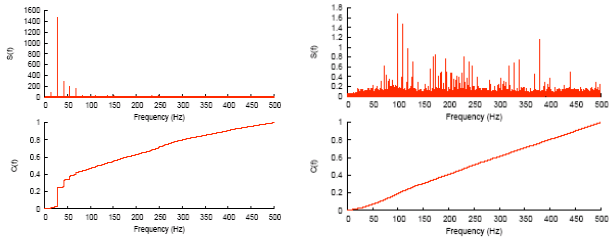


(a) Multiple source addresses observed in attack

(b) Subnet spoofed source addresses

Figure 5: Due to lack of synchronization among the zombies, multi-source attacks exhibit initial ramp-up behavior

Experiments: Spectral Content Analysis



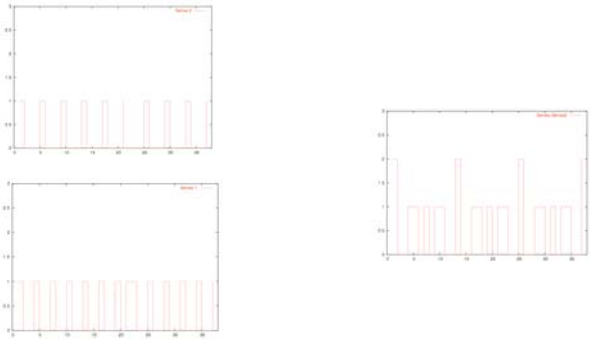
(b) Multi-source

(a) Single-source

Experiment: Explanation

- Single Source Dominant high frequencies
- Multi Source attacks Dominant low Frequencies

How do two sources combine to form lower frequency??



Class of Service Mapping for QoS

- Support different applications
- With different quality demands
- Concept has been around for some time
  - What ails QoS?
    - The ability to identify types of traffic

Objective

- Develop a signature based classification framework
- Class of Service to Traffic mapping problem
- How to choose statistics that accurately represent traffic behavior.

Traffic Classification (In the dark ages)

- Based on Port Numbers
- These techniques had several limitations
  - More than one application using the same port
  - P2P does not use any standardized ports.
  - Some applications tunnel through other application ports
  - Different ports used to circumvent control.

Implementing CoS Mapping

- Three Stage process
  - Statistics Collection
  - Classification
  - Rule Creation

Statistics Collection

- Place monitors and collect network stats
- Need to collect aggregate stats
- Form a vector of statistics
- Ideally statistics should be updatable recursively or in an online manner.

Instance of recursive Classification

1. **average:**

$$\bar{X}_{j+1} = \frac{1}{j+1} X_{j+1} + \frac{j}{j+1} \bar{X}_j,$$

2. **variance:**

$$\mathrm{var}\,(\mathbf{X}_{j+1}) = \frac{1}{j} X_{j+1} + \frac{j-1}{j} \mathrm{var}\,(\mathbf{X}_j) + \frac{j}{j-1} \bar{X}_j^2 - \frac{j+1}{j} \bar{X}_{j+1}^2.$$

Classification

- Now we have a collection of statistics indexed by aggregate
- Use classification algorithm to classify traffic
- This classification can have a direct quality mapping

What type of traffic can there be?

- Interactive -> Real time interaction.
- Streaming -> Multimedia with RT constraints.
- Bulk Data Transfers-> Large volumes of data over the internet.
- Transactional-> Small volumes of traffic.

What statistics can we collect

- Packet Level features
  - Mean Packet Size
  - RMS size
- Flow Summaries
  - Mean flow duration
  - Mean data volume

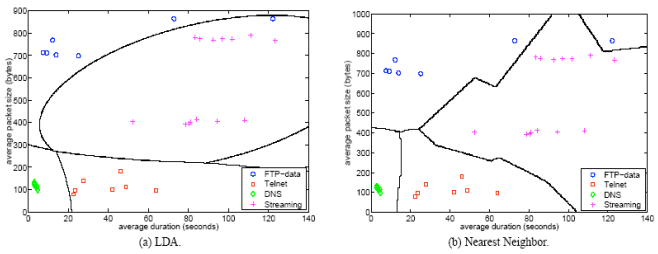
What statistics can we collect

- Connection Level
  - Track Connection level Characteristics
  - Symmetry of connection
  - Advertised window size
- Intra-flow
  - IAT between packets
- Multi Flow
  - Features across different flows.

Classification methods

- Two methods of classification
  - Linear Discriminant Analysis (LDA)
  - Nearest Neighbor (NN)
- Given *k* classes *m* features and *n* training data points
  - Can we classify traffic into characteristics types?

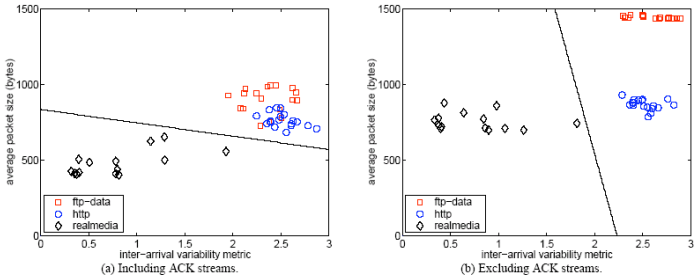
Simple Classification Results



(a) LDA. (b) Nearest Neighbor.

Figure 1: Four class breakup for the Waikato data.

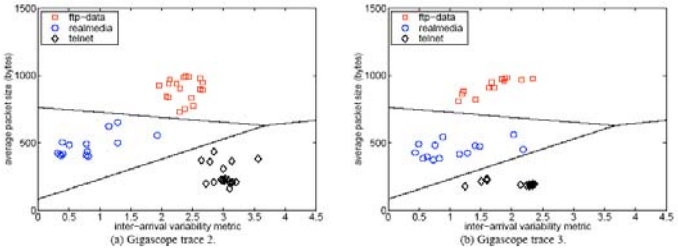
Streaming vs. Data



(a) Including ACK streams. (b) Excluding ACK streams.

Figure 6: The inter-arrival variability metric for three applications: HTTP, FTP-data, and RealMedia.

Temporal Difference



(a) Gigascope trace 2. (b) Gigascope trace 3.

Figure 7: Scatter plots of the inter-arrival variability metric, and average packet size, along with classifi cation boundaries derived from Gigascope trace 2 using LDA.

What does this have to do with NIDS?

- If we can classify traffic as the DOS type traffic
- Provide QoS of zero to it.
  - Basically means deny service to that traffic

The END