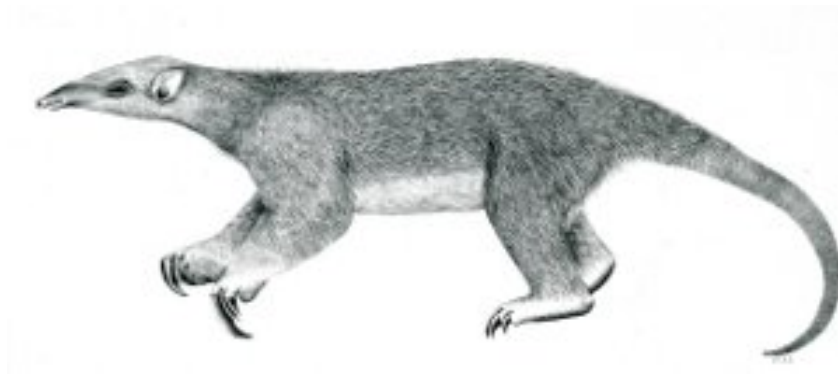

Tranalyzer2

pktSIATHisto



Packet Size and Inter-Arrival Time Histograms



Tranalyzer Development Team

Contents

1	pktSIATHisto	1
1.1	Description	1
1.2	Configuration Flags	1
1.3	Flow File Output	2
1.4	Post-Processing	2
1.5	Example Output	3

1 pktSIATHisto

1.1 Description

The pktSIATHisto plugin records the PL and IAT of a flow. While the PL reflects the bin, the IAT is divided by default into statistical bins to conserve memory / flow, see example below. Where the low precision is reserved for the most prominent IAT of all known codecs. Nevertheless, it can be configured by the user in any arbitrary way. If the memory is not sufficient then decrease HASHCHAINTABLE_BASE_SIZE in tranalyzer.h.

Bin	Range of IAT(default)
0 – 199	0 ms (incl.) – 200 ms (excl.), partitioned into bins of 1 ms
200 – 239	200 ms (incl.) – 400 ms (excl.), partitioned into bins of 5 ms
240 – 299	400 ms (incl.) – 1 sec. (excl.), partitioned into bins of 10 ms
300	for all IAT higher than 1 sec.

1.2 Configuration Flags

Classifying tasks may require other IAT binning. Then the bin limit IATBINBu and the binsize IATBINWu constants in *pktSIATHisto.h* need to be adapted as being indicated below using 6 different classes of bins:

```
#define IATSECMAX 6 // max # of section in statistics;
                    // last section comprises all elements > IATBINBu6

#define IATBINBu1 50// bin boundary of section one: [0, 50)ms
#define IATBINBu2 200
#define IATBINBu3 1000
#define IATBINBu4 10000
#define IATBINBu5 100000
#define IATBINBu6 1000000

#define IATBINWu1 10// bin width 1ms
#define IATBINWu2 5
#define IATBINWu3 10
#define IATBINWu4 20
#define IATBINWu5 50
#define IATBINWu6 100

#define IATBINNu1 IATBINBu1 / IATBINWu1// # of bins in section one
#define IATBINNu2 (IATBINBu2 - IATBINBu1) / IATBINWu2 + IATBINNu1
#define IATBINNu3 (IATBINBu3 - IATBINBu2) / IATBINWu3 + IATBINNu2
#define IATBINNu4 (IATBINBu4 - IATBINBu3) / IATBINWu4 + IATBINNu3
#define IATBINNu5 (IATBINBu5 - IATBINBu4) / IATBINWu5 + IATBINNu4
#define IATBINNu6 (IATBINBu6 - IATBINBu5) / IATBINWu6 + IATBINNu5
```

The number of bin sections is defined by IATSECMAX, default is 3. The static fields IATBinBu and IATBinWu need to be adapted when IATSECMAX is changed. The static definition in curly brackets of the constant fields IATBinBu[], IATBinBu[] and IATBinBu[] must adapted as well to the maximal bin size. The constant IATBINUMAX including his two dimensional packet length, IAT statistics is being used by the descriptive statistics plugin and can suit as a raw input for subsequent statistical classifiers, such as Bayesian networks or C5.0 trees.

The user is able to customize the output by changing several define statements in the header file *pktSIATHisto.h*. Every change requires a recompilation of the plugin using the *autogen.sh* script.

HISTO_PRINT_BIN == 0, the default case, selects the number of the IAT bin, while 1 supplies the lower bound of the IAT

bin's range.

As being outlined in the Descriptive Statistics plugin the output of the plugin can be suppressed by defining `PRINT_HISTO` to zero.

For specific applications in the AI regime, the distribution can be directed into a separate file if the value `PRINT_HISTO_IN_SEPARATE_FILE` is different from zero. The suffix for the distribution file is defined by the `HISTO_FILE_SUFFIX` define. All switches are listed below:

Name	Default	Description	Flags
<code>HISTO_NODEPOOL_FACTOR</code>	17	multiplication factor redblack tree nodepool	
<code>PRINT_HISTO</code>	1	print histo to flow file	
<code>HISTO_PRINT_BIN</code>	0	Bin number; 0: Minimum of assigned inter arrival time. Example: Bin = 10 -> iat = [50:55) -> min(iat) = 50ms	
<code>HISTO_EARLY_CLEANUP</code>	0	after onFlowTerminate tree information is destroyed. MUST be 0 if dependent plugins are loaded	
<code>PSI_XCLD</code>	0	1: include (BS_XMIN,UINT16_MAX]	
<code>PSI_XMIN</code>	1	minimal packet length starts at PSI_XMIN	<code>PSI_XCLD==1</code>
<code>PSI_MOD</code>	0	> 1 : Modulo factor of packet length	
<code>IATSECMAX</code>	3	max # of sections in statistics, last section comprises all elements > IATBINBuN	<code>PSI_XCLD==1</code>

1.3 Flow File Output

The pktSIATHisto plugin outputs the following columns:

Column	Type	Description	Flags
<code>tCnt</code>	U32	Packet size inter-arrival time number of tree entries	
<code>Ps_IatBin_Cnt_</code> <code>PsCnt_IatCnt</code>	R(U16_4xU32)	Packet size inter-arrival time bin histogram	<code>HISTO_PRINT_BIN=0</code>
<code>Ps_Iat_Cnt_</code> <code>PsCnt_IatCnt</code>	R(U16_4xU32)	Packet size min inter-arrival time of bin histo	<code>HISTO_PRINT_BIN=1</code>

All PL-IAT bins greater than zero are appended for each flow in the `PREFIX_flows.txt` file using the following format:

```
[ps]_[IAT]_[# packets]_[# of packets PL]_[# of packets IAT]
```

the PL-IAT bins are separated by semicolons. The IAT value is the lower bound of the IAT range of a bin.

1.4 Post-Processing

By invoking the script `statGplt` under *trunk/scripts* files are generated for the 2/3 dim statistics in a Gnuplot/Excel/SPSS column oriented format. The format is:

- For the 3D case: **PL <tab> IAT <tab> count**
- For the 2D case: **PL <tab> count**

1.5 Example Output

Consider a single flow with the following PL and IAT values:

Packet number	PL (bytes)	IAT (ms)	IAT bin
1	50	0	0
2	70	88.2	17
3	70	84.3	16
4	70	92.9	18
5	70	87.1	17
6	60	91.6	18

Packet number two and five have the same PL-IAT combination. Packets number two to five have the same PL and number two and five as well as the number four and six fall within the same IAT bin. Therefore the following sequence is generated:

50_0_1_1_1 ; 60_90_1_1_2 ; 70_80_1_4_1 ; 70_85_2_4_2 ; 70_90_1_4_2

Note that for better readability spaces are inserted around the semicolons which will not exist in the text based flow file!