EP2300 Project Report: SNMP-based Network Anomaly Detection

Denys Knertser
denys@kth.se

Fabrice Ndjamoy
fenn@kth.se

30 September 2012

1 Summary

The goal of the project is real-time anomaly detection in a testbed network [1]. Management software based on SNMP framework was developed to reach this goal. The management software is able to collect and display information about the topology of the network: the links between the routers and the routers configuration information. Based on this information, the software is able to monitor the overall network state (total consumed bandwidth of all links and the average packet size) continuously polling all the routers in the network for the links load information. The software stores a set of the recent network states and detects anomalies in the network using several statistical methods. The software performs the analysis in the real-time and raises an alarm whenever a suspicious network state is detected. Additionally, it allows to differentiate between two attack types and reports the probability to an attack.

2 Software design

The programming language for developing the software was chosen to be Python. The software depends on the following packages:

- Python 2.5 or higher
- PyCrypto
- NumPy [2]
- Multiprocessing [3] (included in Python core since version 2.7)
- PySNMP [4] (included in the software distribution)
- PyASN1 [5] (included in the software distribution)

The software consists of 4 executables and 6 additional modules. The package diagram of the software is shown on Figure 1.

my.snmpiface module defines SnmpIface class, instance of which handles single SNMP communication channel and provides simple interface which allows to request a single object using *get* message, a subtree or a set of objects using *getnext* message or a set of objects using *getbulk* message.

my.router module contains classes Router and RouterSnmp classes. Router class is essentially a data structure to store the necessary information about a single router.

RouterSnmp class inherits from Router class and links it to a corresponding SnmpIface object which handles communication with the router. In addition, RouterSnmp provides methods for collecting info about the router and polling the router for links state information.

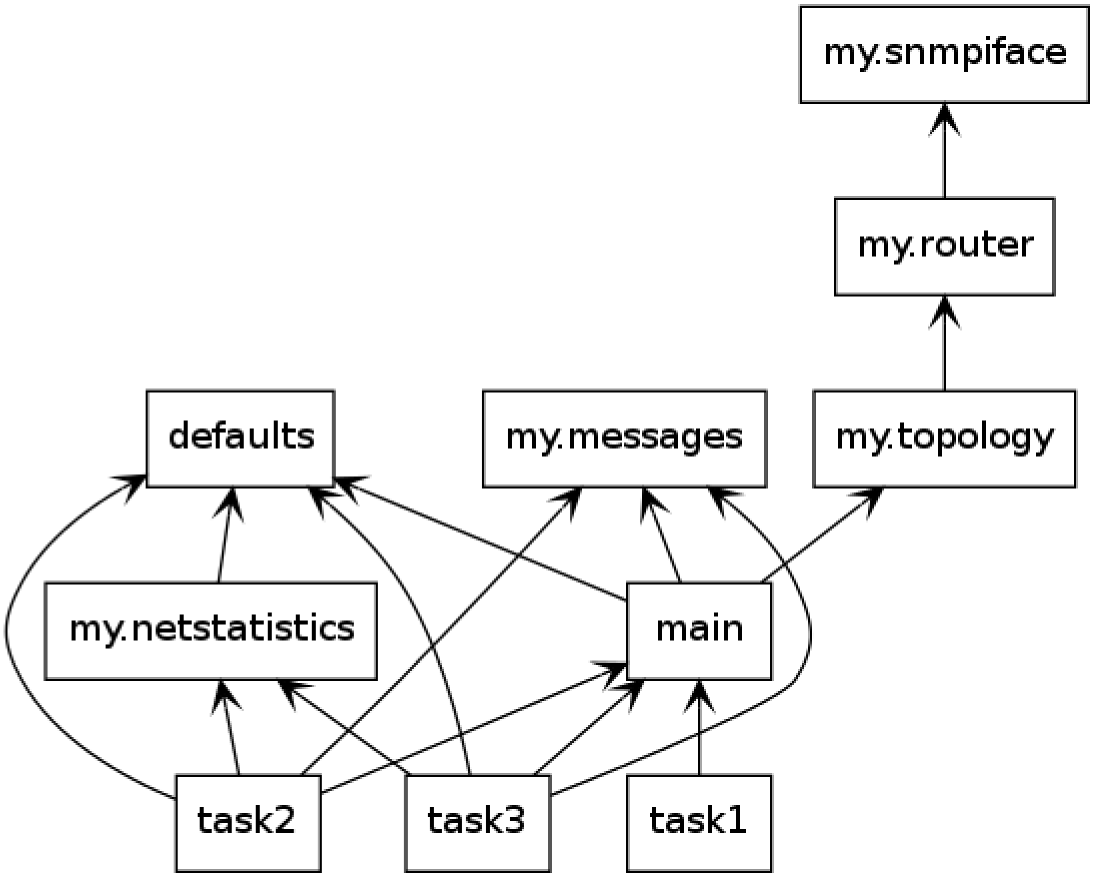

Figure 1 - UML package diagram

my.topology module defines Topology class which collects the information about the topology and keeps the array of RouterSnmp objects for further use.

my.netstatistics module contains the description of the NetStatistics module which calculates the global network state and stores a set of the recent network states. It defines outlier detection methods and summarizes the output information from these methods. It is also able to detect an attack type if the outlier is detected.

main.py executable collects the information about the topology and saves it to a file. As a module, it also provides interface to load the topology from the file. It has to be run before any other executable. If otherwise happens, the notification to run ‘main.py’ is raised.

task1.py loads the topology information from the file and displays it.

task2.py loads the topology information from the file and starts continuously polling the routers for the link states. The routers are polled in parallel using multiprocessing. The information from all the routers is passed to the NetStatistics object which calculates alarm threshold and raises alarm if this threshold is exceeded.

task3.py acts essentially the same as ‘task2.py’, but polls routers not only for the links load, but also for the number of packets to calculate the average size of packet which is used to determine the attack type. It also enables NetStatistics object to use 3 outlier detection methods instead of 1.

defaults module contains default configuration of the parameters, such as the inputs to all the tasks and the name of the file which is used to store the topology information.

my.messages modules defines several modes of data output.

The list of SNMP OID’s which the software uses:

- ipRouteNextHop (1.3.6.1.2.1.4.21.1.7)
- sysName (1.3.6.1.2.1.1.5.0)
- ifNumber (1.3.6.1.2.1.2.1.0)
- ifDescr (1.3.6.1.2.1.2.2.1.2)
- ipAdEntAddr (1.3.6.1.2.1.4.20.1.1)
- ifInOctets (1.3.6.1.2.1.2.2.1.10)
- ifInUcastPackets, ifInNUcastPackets, ifInDiscards, ifInErrors (1.3.6.1.2.1.2.2.1.[11-14]) are implicitly used by querying ifInOctets OID with getbulk for the number of objects which is 5 times number of interfaces.

3 Outlier detection schemes

The schemes for detecting outliers used in the software are the following:

- Standard Deviation method [6]
- Median rule [6]
- MADe method [6]

The optional schemes were chosen to be Median rule and MADe method because their performance is satisfactory regardless of the traffic distribution type. First, it is important, because it is impossible to study the traffic in the testbed in advance and there is no information about the origination of this traffic (it is generated randomly). Second, the attacks experienced during the learning period (where no outliers are detected because there are too few samples available to take any statistical decision) can shift the original distribution, so it would be impossible for a non-universal method to operate normally.

The pseudocode for SD method:

```
OBTAIN Current network state
OBTAIN Network_States: statistical set of previous network states
COMPUTE Mean of Network_States
COMPUTE Standard deviation of Network_States
SET Threshold := value of Mean + 3 * value of Standard deviation
IF Current network state > Threshold THEN
     DISPLAY “ALARM”
END
```

The pseudocode for MR method:

```
OBTAIN Current network state
OBTAIN Network_States: statistical set of previous network states
SORT Network_States
ASSIGN Network_States_left := left half of Network_States array
ASSIGN Network_States_right := right half of Network_States array
COMPUTE Median of Network_States_left
COMPUTE Median of Network_States_right
ASSIGN IQR := Median of Network_States_right - Median of Network_States_left
COMPUTE Median of Network_States
ASSIGN Threshold := Median of Network_States + 2.3*IQR
IF Current network state > Threshold THEN
     DISPLAY “ALARM”
END
```

The pseudocode for MADe method:

```
OBTAIN Current network state
OBTAIN Network_States: statistical set of previous network states
COMPUTE Median of Network_States
INIT MAD_Array := empty array
FOR N in Network_States
     next item of MAD_Array := | N - Median of Network_States |
END
ASSIGN MADe := 1.483 * Median of MAD_Array
ASSIGN Threshold := Median of Network_States + 3 * MADe
IF Current network state > Threshold THEN
     DISPLAY “ALARM”
END
```

4 Results and analysis

Figure 2 and Figure 3 illustrate the network load and detected outliers in Task 2 and Task 3 correspondingly.

It can be seen on the Figure 2 that the average usual traffic load is around 50 KB/s. However, there are two types of bursts: around 2 MB/s, without losing connection and around 5 MB/s, which is preceded by 20-30 seconds routers inaccessibility. The plot shows the dynamics of the threshold decreasing: every time a high-load network state learned in the training period is replaced by the usual data point, the threshold drops significantly. It can be stated that SD method performs quite well over time, but in the beginning some of the outliers might be missed.

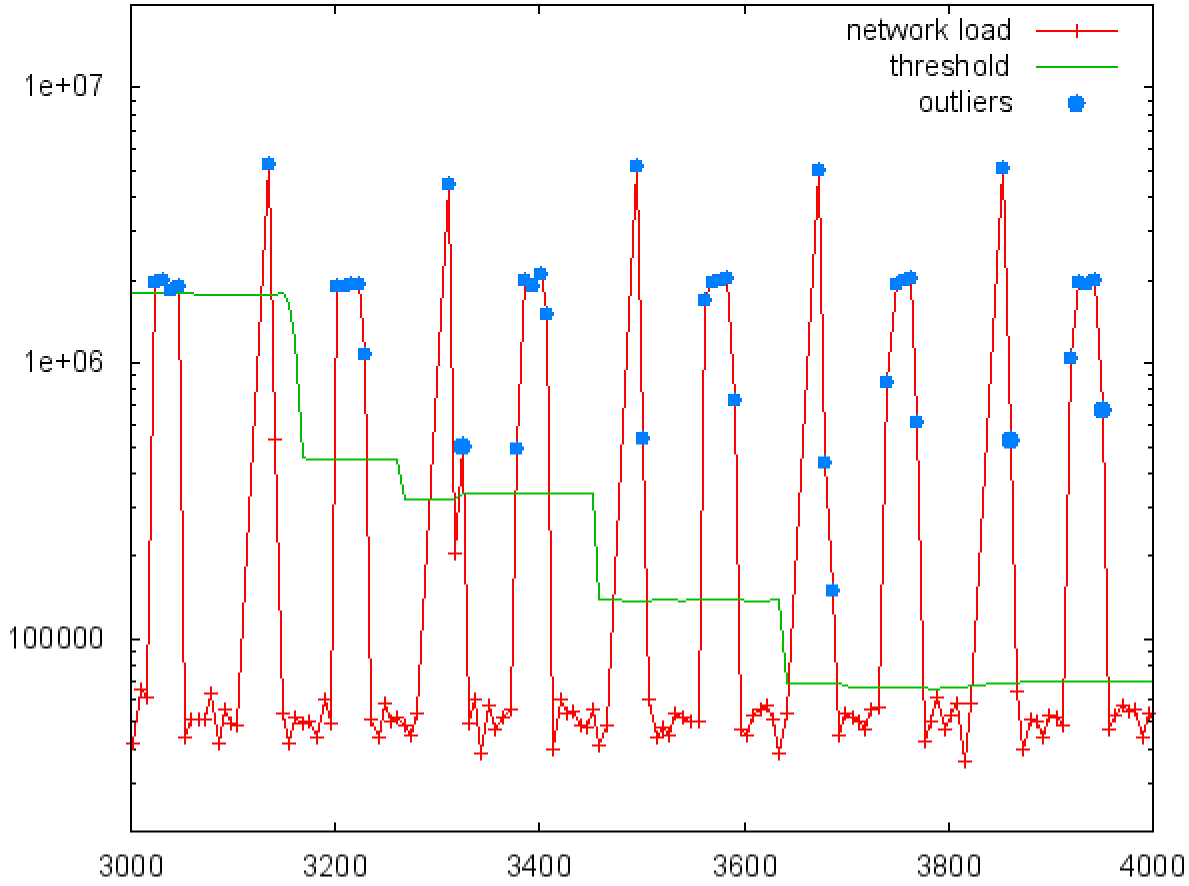

Figure 2 - Network load and outliers detected in Task 2

Figure 3 shows not only the network load and outliers, but also the probability of an attack and type of an attack (Flash crowd or DoS attack). The traffic characteristics are similar to those in Task 2. It appears that the thresholds of the three methods are very close to each other, however the additional reason for this is that different methods help to filter out the outliers (which are not considered in threshold calculation), so SD method converges (stabilizes its threshold) much quicker than in Task 2. Most of the attacks are detected with 100% probability.

The console outputs for Task 1, Task 2 and Task 3 are in appendices A, B and C correspondingly.

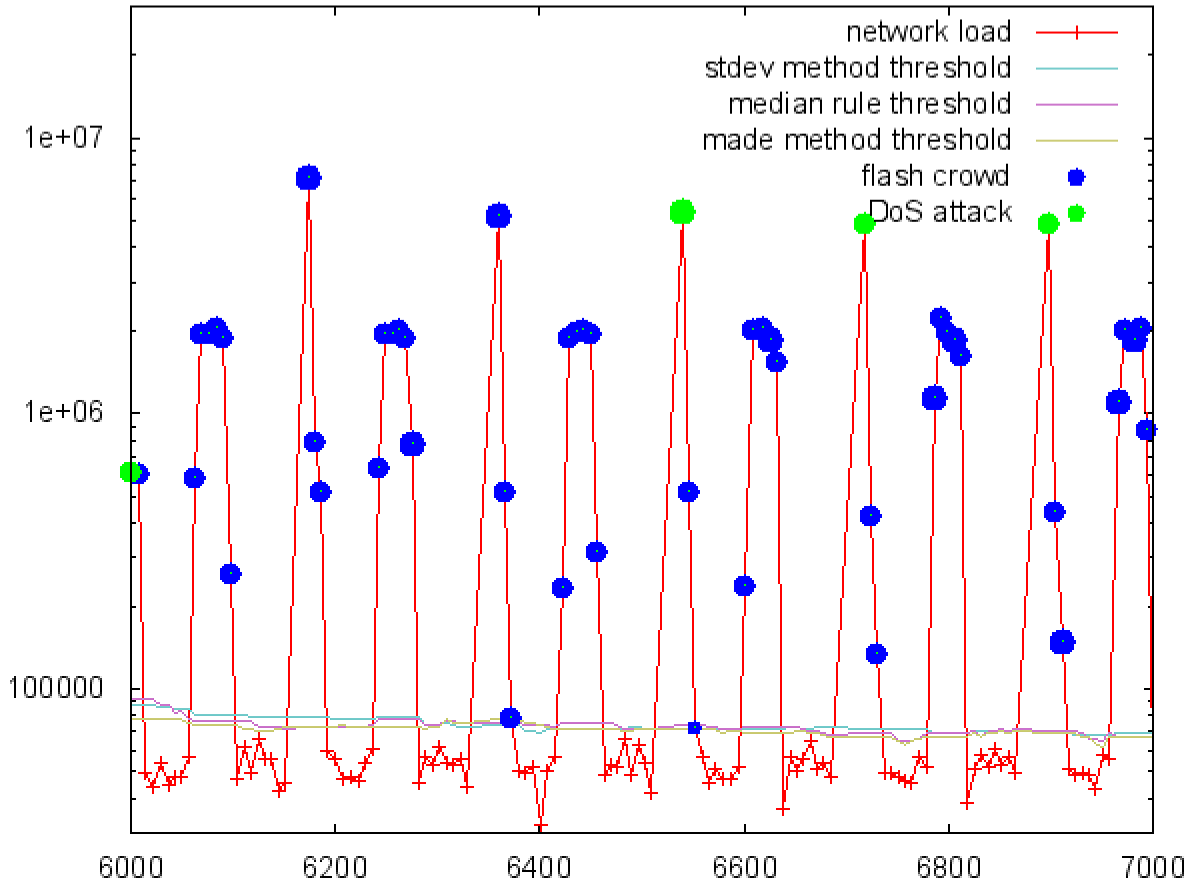

Figure 3 - Network load, outliers and type of attack detected in Task 3 (the probability of an attack is determined by circle size)

References

[1] Misbah Uddin, “EP2300 Project. SNMP-based Network Anomaly Detection”

[2] Scientific Computing Tools for Python [Online]. Available: http://numpy.scipy.org/ [Accessed: 30-Sep-2012]

[3] multiprocessing 2.6.2.1 [Online]. Available: http://pypi.python.org/pypi/multiprocessing/ [Accessed: 30-Sep-2012]

[4] SNMP library for Python [Online]. Available: http://pysnmp.sourceforge.net/ [Accessed: 30-Sep-2012]

[5] ASN.1 library for Python [Online]. Available: http://pyasn1.sourceforge.net/ [Accessed: 30-Sep-2012]

[6] Songwon Seo. A review and comparison of methods for detecting outliers in univariate data sets. Master's thesis, University of Pittsburgh, 2006.

Appendix A. Task 1 sample output

```
Router R0:
        IP addresses:
                192.168.14.1
                192.168.8.1
        Interfaces:
                FastEthernet0/0
                FastEthernet0/1
                Null0
        Link-layer neighbours:
                192.168.8.2
                192.168.14.14

Router R1:
        IP addresses:
                192.168.8.2
                192.168.0.2
        Interfaces:
                FastEthernet0/0
                FastEthernet0/1
                Null0
        Link-layer neighbours:
                192.168.0.11
                192.168.8.1

Router R2:
        IP addresses:
                192.168.13.3
                192.168.12.3
        Interfaces:
                FastEthernet0/0
                FastEthernet0/1
                Null0
        Link-layer neighbours:
                192.168.13.15
                192.168.12.4
```

```
Router R3:
        IP addresses:
                192.168.12.4
                192.168.9.4
        Interfaces:
                FastEthernet0/0
                FastEthernet0/1
                Null0
        Link-layer neighbours:
                192.168.9.9
                192.168.12.3

Router R4:
        IP addresses:
                192.168.5.5
                192.168.3.5
        Interfaces:
                FastEthernet0/0
                FastEthernet0/1
                Null0
        Link-layer neighbours:
                192.168.5.6
                192.168.3.8

Router R5:
        IP addresses:
                192.168.5.6
                192.168.15.6
                192.168.100.100
        Interfaces:
                Loopback0
                FastEthernet0/0
                FastEthernet0/1
                Null0
        Link-layer neighbours:
                192.168.15.7
                192.168.5.5
```

```
Router R6:
        IP addresses:
                192.168.15.7
                192.168.6.7
        Interfaces:
                FastEthernet0/0
                FastEthernet0/1
                Null0
        Link-layer neighbours:
                192.168.6.16
                192.168.15.6

Router R7:
        IP addresses:
                192.168.3.8
                192.168.7.8
        Interfaces:
                FastEthernet0/0
                FastEthernet0/1
                Null0
        Link-layer neighbours:
                192.168.3.5
                192.168.7.11

Router R8:
        IP addresses:
                192.168.9.9
                192.168.10.9
        Interfaces:
                FastEthernet0/0
                FastEthernet0/1
                Null0
        Link-layer neighbours:
                192.168.9.4
                192.168.10.12

Router R9:
        IP addresses:
                192.168.4.10
                192.168.1.10
        Interfaces:
                FastEthernet0/0
                FastEthernet0/1
                Null0
        Link-layer neighbours:
                192.168.4.14
                192.168.1.15

Router R10:
        IP addresses:
                192.168.0.11
                192.168.7.11
        Interfaces:
                FastEthernet0/0
                FastEthernet0/1
                Null0
        Link-layer neighbours:
                192.168.0.2
                192.168.7.8

Router R11:
        IP addresses:
                192.168.11.12
                192.168.10.12
        Interfaces:
                FastEthernet0/0
                FastEthernet0/1
                Null0
        Link-layer neighbours:
                192.168.10.9
                192.168.11.13
```

```
Router R12:
        IP addresses:
                192.168.2.13
                192.168.11.13
        Interfaces:
                FastEthernet0/0
                FastEthernet0/1
                Null0
        Link-layer neighbours:
                192.168.2.16
                192.168.11.12

Router R13:
        IP addresses:
                192.168.4.14
                192.168.14.14
        Interfaces:
                FastEthernet0/0
                FastEthernet0/1
                Null0
        Link-layer neighbours:
                192.168.14.1
                192.168.4.10

Router R14:
        IP addresses:
                192.168.13.15
                192.168.1.15
        Interfaces:
                FastEthernet0/0
                FastEthernet0/1
                Null0
        Link-layer neighbours:
                192.168.13.3
                192.168.1.10

Router R15:
        IP addresses:
                192.168.6.16
                192.168.2.16
        Interfaces:
                FastEthernet0/0
                FastEthernet0/1
                Null0
        Link-layer neighbours:
                192.168.2.13
                192.168.6.7
```

Appendix B. Task 2 sample output

```
   0.00    ::   start polling
-----------------------------
time       network load          | threshold
   7.35    ::     66836          |
  15.03    ::     56893          |
  22.18    ::     74109          |
  29.29    ::     66224          |
  37.90    ::     58332          |
  45.04    ::     64864          |
  58.74    ::   Router(s) didn't respond
  68.91    ::   Router(s) didn't respond
  75.55    ::   5196803          |
  82.65    ::    494433          |
  89.80    ::     59198          |
  96.88    ::     57717          |
 104.08    ::     73541          |
 111.05    ::     68470          |
 117.95    ::     67538          |
 124.88    ::     43940          |
 133.02    ::     65872          |
 142.04    ::   1006530          |
 150.14    ::   2044694          |
 158.90    ::   1966187          |
 166.96    ::   1940212          |
 173.96    ::    252494          |
 181.03    ::     48555          |
 187.97    ::     68765          |
 195.59    ::     51832          |
 202.67    ::     59632          |
 209.59    ::     68482          |
 217.70    ::     55806          |
 224.70    ::     73913          |
 238.20    ::   Router(s) didn't respond
 248.84    ::   Router(s) didn't respond
 255.97    ::   5184859          |
 262.88    ::    513002          |
 269.98    ::     59798          |
 276.89    ::     61352          |
 283.85    ::     58356          |  4622213  |
 290.78    ::     83140          |  4622299  |
 297.85    ::     52257          |  4622045  |
 304.76    ::     60216          |  4622267  |
 311.92    ::     53306          |  4622328  |
 319.71    ::    725451          |  4622382  |
 326.77    ::   2051682          |  4631176  |
 334.67    ::   2076781          |  3762569  |
 343.56    ::   1934021          |  3912117  |
 350.99    ::    874245          |  4030153  |
 358.03    ::     63813          |  4040748  |
 365.06    ::     55118          |  4040970  |
 371.97    ::     55801          |  4041281  |
 378.99    ::     56036          |  4041554  |
 386.02    ::     59961          |  4041260  |
 393.04    ::     66935          |  4041397  |
 400.26    ::     64519          |  4023202  |
 412.67    ::   Router(s) didn't respond
 426.36    ::   Router(s) didn't respond
 432.73    ::   5025999          |  3887167  |  ALARM
 439.34    ::    268019          |  3887167  |
 447.11    ::    297047          |  3750496  |
 454.25    ::     62600          |  3607713  |
 461.18    ::     72010          |  3607574  |
 468.40    ::     61880          |  3607385  |
 475.31    ::     66957          |  3607437  |
 482.40    ::     47865          |  3607314  |
 489.30    ::     67273          |  3607416  |
 496.90    ::    162798          |  3607425  |
 505.91    ::   1918644          |  3607030  |
 513.04    ::   2011342          |  3746441  |
 521.04    ::   1971051          |  2569984  |
 528.06    ::   1612863          |  2764844  |
 535.91    ::     56514          |  2875979  |
 544.03    ::     62820          |  2876120  |
 552.24    ::     57924          |  2875990  |
 559.80    ::     51738          |  2876687  |
 566.93    ::     63797          |  2876703  |
 573.82    ::     67174          |  2876600  |
 580.91    ::     54682          |  2876199  |
 594.27    ::   Router(s) didn't respond
 608.39    ::   Router(s) didn't respond
 614.58    ::   4810001          |  2867054  |  ALARM
 621.16    ::    509596          |  2867054  |
 627.49    ::     60932          |  2663541  |
 634.05    ::      53427          |  2424897  |
 640.44    ::      61408          |  2191160  |
 646.94    ::      54344          |  2148489  |
 653.49    ::      57237          |  2148588  |
 659.88    ::      43797          |  2148565  |
 666.54    ::      60451          |  2148707  |
 672.98    ::      33992          |  2148661  |
 680.68    ::     912215          |  2148979  |
 687.79    ::    2066831          |  2196337  |
 694.70    ::    1957784          |  2464253  |
 701.84    ::    1959837          |  2673056  |
 708.13    ::    1494872          |  2860672  |
 715.24    ::      45663          |  2947443  |
 721.56    ::      51707          |  2948244  |
 728.07    ::      48533          |  2948555  |
 734.41    ::      42589          |  2949114  |
 741.59    ::      48812          |  2949282  |
 749.25    ::      50089          |  2949839  |
 755.96    ::      53030          |  2952536  |
```

Appendix C. Task 3 sample output

```
   0.00      ::     Router(s) didn't respond
   9.77      ::     Router(s) didn't respond
  16.58      ::     start polling
-----------------------------
time         network load, packetsize   |      thresholds
  23.42      ::      509888              988          |
  30.33      ::       65812              235          |
  37.11      ::       57180              250          |
  44.08      ::       56740              246          |
  50.93      ::       74449              249          |
  58.14      ::       58979              252          |
  65.06      ::       59327              233          |
  72.11      ::       55127              239          |
  79.17      ::      781125             1146          |
  87.50      ::     1955519             1308          |
  95.31      ::     2008815             1344          |
 102.28      ::     1965929             1312          |
 109.28      ::     1275721             1230          |
 116.90      ::       55884              246          |
 125.19      ::       61917              229          |
 132.15      ::       54786              258          |
 139.20      ::       55645              250          |
 146.20      ::       55551              236          |
 153.33      ::       66943              248          |
 160.30      ::       69689              243          |
 172.03      ::     Router(s) didn't respond
 184.86      ::     Router(s) didn't respond
 191.54      ::     4507004              164          |
 198.70      ::      241292              654          |
 205.79      ::      426468              882          |
 212.85      ::       63398              242          |
 219.84      ::       68689              251          |
 226.43      ::       60310              264          |
 233.12      ::       63612              250          |
 239.70      ::       42294              260          |
 246.41      ::       53747              262          |
 253.01      ::       45633              246          |
 259.72      ::     1054487             1278          |
 266.56      ::     1987512             1358          | 3352739  1107821   101361 |
ALARM   66   Flash crowd (packet size threshold 0)
 273.44      ::     1963585             1354          | 3352739  1107821   101361 |
ALARM   66   Flash crowd (packet size threshold 0)
 280.30      ::     2119007             1372          | 3352739  1107821   101361 |
ALARM   66   Flash crowd (packet size threshold 0)
 287.15      ::     1617907             1309          | 3352739  1107821   101361 |
ALARM   66   Flash crowd (packet size threshold 0)
 293.83      ::       68325              301          | 3352739  1107821   101361 |
 301.19      ::       43579              245          | 3348372   915955    99475 |
 309.35      ::       48288              250          | 3348665   916290   100195 |
 316.02      ::       50332              246          | 3348784   916507   101712 |
 322.80      ::       46076              285          | 3348869   917482   106335 |
 329.39      ::       51358              250          | 3349223   916785    98265 |
 336.15      ::       55336              263          | 3349321   919175   108893 |
 342.60      ::       50164              261          | 3349372   919175   108893 |
 355.72      ::     Router(s) didn't respond
 368.43      ::     Router(s) didn't respond
 375.13      ::     5053382              205          | 3349437   924669   113458 |
ALARM  100   Flash crowd (packet size threshold 0)
 381.83      ::      493262             1059          | 3349437   924669   113458 |
 388.89      ::       54251              245          | 3335941   924669   113458 |
 395.56      ::       51751              261          | 3166598   497158   102037 |
 402.27      ::       58591              237          | 2968593    98045    90265 |
 408.69      ::       53160              270          | 2758559    95745    89678 |
 415.43      ::       51668              273          | 2663401    94669    88376 |
 422.00      ::       50881              245          | 2663372    94575    87864 |
 428.70      ::       46668              254          | 2663292    95457    86692 |
 435.32      ::       42203              252          | 2663238    96719    91203 |
 441.85      ::     1841051             1340          | 2663152    96021    90621 |
ALARM   66   Flash crowd (packet size threshold 0)
 448.49      ::     1972182             1345          | 2663152    96021    90621 |
ALARM   66   Flash crowd (packet size threshold 0)
 456.84      ::     1990279             1367          | 2663152    96021    90621 |
ALARM   66   Flash crowd (packet size threshold 0)
 464.08      ::     1990017             1364          | 2663152    96021    90621 |
ALARM   66   Flash crowd (packet size threshold 0)
 470.54      ::      705041             1103          | 2663152    96021    90621 |
ALARM   66   Flash crowd (packet size threshold 0)
 477.28      ::       51963              247          | 2663152    96021    90621 |
 484.33      ::       48254              242          | 2663127    95517    87875 |
 492.48      ::       42368              254          | 2662986    99245    84676 |
 499.49      ::       51546              274          | 2662782    87286    80125 |
 506.08      ::       53415              247          |  718503    86582    76999 |
 513.09      ::       50686              269          |  709416    79479    74365 |
 519.84      ::       56174              249          |  672418    75443    67986 |
 531.61      ::     Router(s) didn't respond
 544.23      ::     Router(s) didn't respond
 550.42      ::     5303765              205          |  672328    69884    67986 |
ALARM  100   Flash crowd (packet size threshold 0)
 557.03      ::      107988              503          |  672328    69884    67986 |
ALARM   66   Flash crowd (packet size threshold 0)
 563.60      ::      514233             1006          |  672328    69884    67986 |
ALARM   66   Flash crowd (packet size threshold 0)
 570.38      ::       47602              273          |  672328    69884    67986 |
 576.99      ::       58366              245          |  672076    69334    68407 |
 583.68      ::       46272              269          |  672051    69334    68407 |
 590.04      ::       56980              282          |  671866    68798    68068 |
 596.63      ::       62868              250          |  671984    69334    68407 |
 603.42      ::       41844              260          |  672095    71261    69092 |
 610.05      ::       56164              264          |  672077    71261    69092 |
 616.82      ::      381438              943          |  300594    71238    69092 |
ALARM  100   Flash crowd (packet size threshold 0)
 623.39      ::     1939477             1348          |  300594    71238    69092 |
ALARM  100   Flash crowd (packet size threshold 0)
```

```
 632.90       ::    1973240             1359          |  300594    71238    69092 |
ALARM  100    Flash crowd (packet size threshold 0)
 640.43       ::    1968527             1369          |  300594    71238    69092 |
ALARM  100    Flash crowd (packet size threshold 0)
 647.06       ::    1668850             1350          |  300594    71238    69092 |
ALARM  100    Flash crowd (packet size threshold 0)
 653.69       ::      58250              268          |  300594    71238    69092 |
 660.27       ::      40102              263          |  300299    71238    69092 |
 667.01       ::      51188              255          |  300288    71238    69092 |
 674.09       ::      52472              262          |  300325    71238    69092 |
 682.23       ::      46282              248          |  300357    71360    69757 |
 689.21       ::      51875              247          |  300359    71360    69757 |
 695.85       ::      60659              264          |  300366    71443    70209 |
 702.67       ::      50066              248          |  300488    71466    71384 |
 714.88       ::    Router(s) didn't respond
 728.38       ::    Router(s) didn't respond
 735.16       ::    5023073              205          |  300486    71466    71384 |
ALARM  100    Flash crowd (packet size threshold 0)
```