EMIST (Evaluation Methods for Internet Security Technology) GUI MANUAL

Web: http://emist.ist.psu.edu
Newsgroup: pubnews.cse.psu.edu/psu.cse.research.emist

Table of contents

1. Overview

The EMIST GUI provides an integrated environment to interact with DETER or EMULAB test-beds and to conduct network security emulation/simulation experiments. The EMIST GUI is a modular, component-based topology editor, a TCL script generator, a worm experiment designer and a visualization tool for experimental results. First, the GUI offers a topology editor toolbar to draw network topologies including computer/end-host nodes, switch nodes, router nodes, sub-network/Internet interfaces and links. Each of these network components has configurable properties such as bandwidth and link latency, which can be stipulated and modified. The GUI can then generate a TCL script from a designed network topology in several formats: NS/2 format, DETER/EMULAB format without LAN, DETER/EMULAB format with LAN and virtualized nodes. Finally, the GUI can visualize the resulting experimental traffic (captured in TCPDUMP format) by animation or sliding charts and figures.

2. Getting started

System requirements

Currently, the EMIST GUI only runs on Windows XP and Windows 2000 platforms and requires at least 1000MByte of a combination of RAM and virtual memory.

Installation

Copy the executable PsuEmistGUI.exe to the chosen directory. During its first run, the GUI program will register itself with Windows and will associate itself with '.wor' file type.

3. Topology Design

3.1. Basic operation

The EMIST GUI can be used to design network topology which includes five different network components: computer/host, switch, router, link and Internet/sub-network.

Adding a network component: Click on the corresponding component icon on the toolbar, move the mouse pointer to the main window and click on the desired location to add a new component. To add a link, click on the source component, hold the mouse button down and move the mouse pointer to the target component, then release the mouse button.

Selecting a component: Click the **Select** icon on the toolbar (Arrow icon) to switch to "select mode", then click on the target component (the selected component will be highlighted). To select a group of components, hold the mouse button down to draw rectangular box over the components. To deselect a component or group of components, click on a blank space in the main window.

Moving a component: Select the component (single left-click on the component) and drag it to the target location.

Editing a property of a component: Each component has various properties which can be modified, select the component and right-click to open the property dialog window.

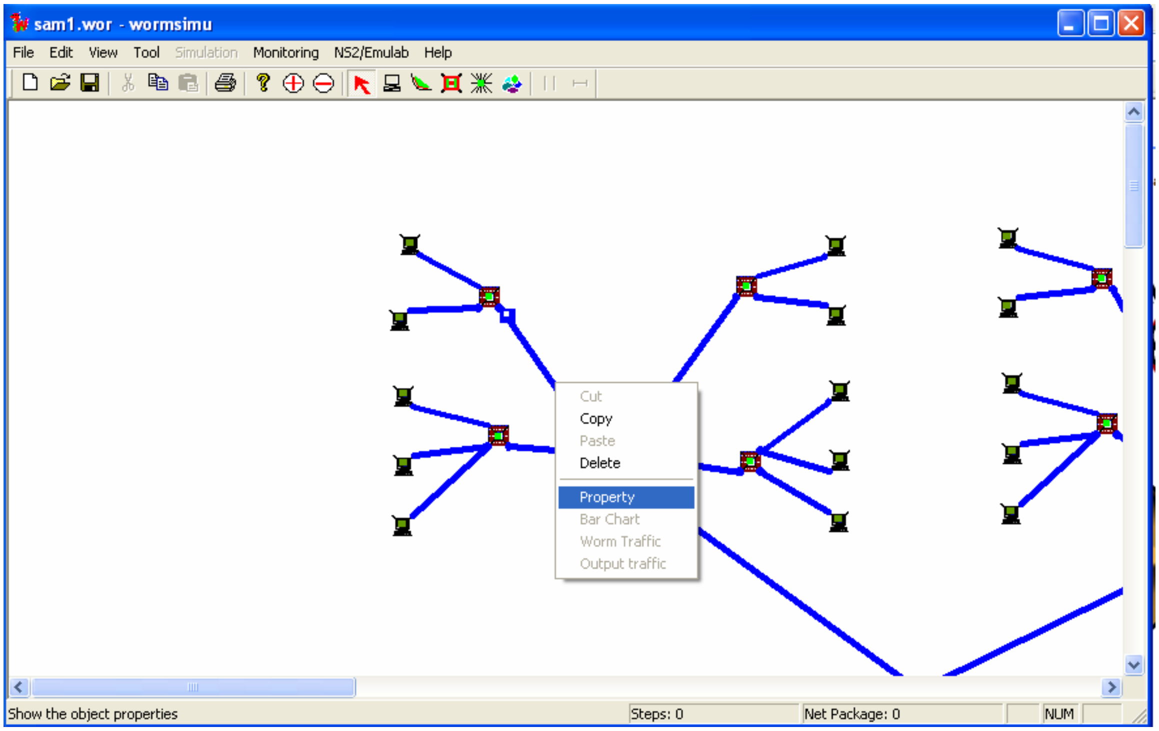


Figure 1: Topology design—property editing

Deleting a component: Select the component and choose menu **Edit->Delete** to delete it.

3.2. Miscellaneous features

There are some other helpful features in the GUI, which include:

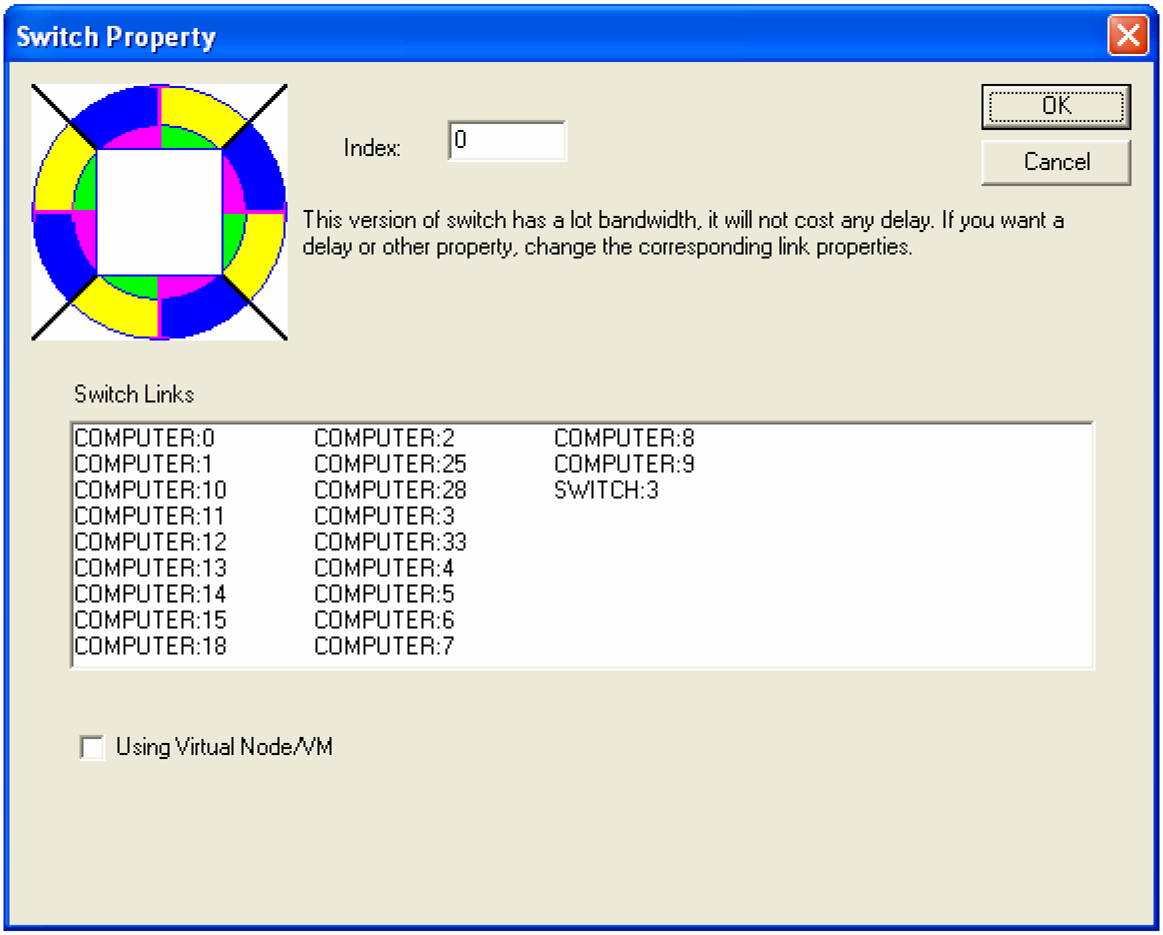
Topology zoom: Zoom in, zoom out, zoom by, and click-zoom. Click the **zoom in** or **zoom out** icon on the toolbar for larger or smaller zoom. Right-click on a blank space to open the zoom-by window. Hold down the '**CTRL**' key and right-click on the main window to zoom to level 8 centered at the click point.

Index display: GUI internal component index number starts from 0 for each class of components. To show the index number of each network component, choose menu **View->show computer index, View->show switch index** or **View->show router index.**

Computer node finder: Choose **View->Zoom to component** to open the dialog, and then input the computer node index. The found node will be located on the center of the main window.

Copy and Paste: Select a component or a group of components, then copy and paste using the right-click menu.

*Virtual node***:** A switch component has one special property "**Using Virtual Node/VM**". Modifying this property will change the way the GUI generates a DETER/EMULAB script. A virtualized switch is distinguished from a real switch by its color and symbol.



Index: 0

This version of switch has a lot bandwidth, it will not cost any delay. If you want a delay or other property, change the corresponding link properties.

Switch Links

```
COMPUTER:0        COMPUTER:2        COMPUTER:8
COMPUTER:1        COMPUTER:25       COMPUTER:9
COMPUTER:10       COMPUTER:28       SWITCH:3
COMPUTER:11       COMPUTER:3
COMPUTER:12       COMPUTER:33
COMPUTER:13       COMPUTER:4
COMPUTER:14       COMPUTER:5
COMPUTER:15       COMPUTER:6
COMPUTER:18       COMPUTER:7
```

□ Using Virtual Node/VM

Figure 2: virtualized LAN

4. Topology conversion and script generation

After finishing the topology design, you can save and restore your design using **File->Save** and **File->Load** menu items. Besides the customized binary representation, the GUI supports exporting the design in three different output formats: NS, one-to-one DETER format, and DETER format with virtual nodes. You can generate a script file in a specific format by choosing “output format” from menu **NS2/Emulab**.

1) **NS2/Emulab->Save as a TEXT NS file**: GUI will generate NS scripts when File->Save menu item is invoked.
2) **NS2/Emulab->Save to DETER script (one 2 one)**: GUI will generate DETER format without virtual nodes.
3) **NS2/Emulab->Generate DETER script (V node)**: GUI will generate DETER format with virtual nodes.

4.1. Node name and index conversion

GUI internal component index number starts from 0 for each class of components. In the TCL script all components except link are named by the following formula:

Computer:	n-(GUIindex)
Switch:	n-(ComputerCount+GUIindex)
Router:	n-(ComputerCount+SwitchCount+GUIindex)
Network:	n-(ComputerCount+SwitchCount+RouterCount+GUIindex)

Currently script generator doesn’t assign IP addresses for components. The mapping between node name and test-bed IP address is based on test-bed ***/etc/hosts*** file.

4.2. Additional start-up command scripts

In the DETER script, there are additional start-up commands after the topology script lines. You can modify or delete them for your particular experiment.

4.3. Virtualized LAN segment information file

When generating a virtualized network segment, the GUI generates another separate file named ***map.001*** which includes information regarding that sub-network. Upload this file to the DETER test bed computer so that the experimental programs can access it. The following lines are part of an example map.001 file.

```
#node & virtual node map file
#n-### TYPE(B/I/W) S/N #####(GUI node index) #####(Last segment of IP)
n-902   W N 1     254
n-902   W N 3     253
n-902   W N 0     252
n-902   W N 2     251
n-902   W N 4     250
n-902   W N 6     249
n-902   W N 8     248
```

Each line of the map.001 file represents one virtualized/real host node. The fields of each line are: node name, node type, node susceptibility, node GUI index and last byte of node IP address.

Note: the GUI will override map.001 if there is map.001 file in the directory.
Note: Map.001 file format may be slightly different in example above than in other GUI versions.

4.4. Internet Worm Simulation File format

For Internet scale-down worm experiment, use **NS2/Emulab->[Topology Format Conversion]->Read Internet topology from file (SLAMMER)** to read the topology file. A sample of the scale-down topology file is shown below.

```
*********************************************************
network 0.0.0.0/17 3
worm 0.0.72.101
worm 0.0.85.214
worm 0.0.123.42
network 0.0.128.0/17 1
**********************************************************
```

5. Visualization

5.1. Log files preparation

To use the visualization feature of the GUI, all log files are required to be placed in the same directory. The log files are shown below:

1) *HOSTLIST file*: This is the /etc/hosts file of any experimental node and is renamed to ‘hostlist’. The GUI uses the hostlist file to obtain a mapping between the internal index

number (node, LAN, and link number in the script file) and the assigned IP address of a corresponding node.

2) *TCPDUMP log file:* The name of log file is tcplog_NN.NN.NN.NN. Note that the timestamp on each dump line has to be an unformatted number (using –tt option when running TCPDUMP program).
3) *Worm infection file*: The name of worm infection file can be either log_XXXX or log_NN.NN.NN.NN, where XXXX is a node index number and NN.NN.NN.NN is an IP address of node. The following is an example of a worm infection file:
3 by n-8-link6 10.1.5.3 at:1074366335.249722
Note: These files are only for WORM experiment.

5.2. Starting visualization

After collecting traffic and worm infection log files from an experiment, the GUI can visualize the result with the following steps:

1) Change the step time: Choose **NS2/Emulab->Change Step Time**. Specify an integer value between 1 and 60000 milliseconds.
2) Load the data: Choose **NS2/Emulab->DETER/EMULAB visualization (V node)**. When the dialog box named "Please locate the file directory" appears, go to the directory that contains all the necessary files (HOSTLIST file, Worm infection files, and TCPDUMP log files) and click the **Open** button (with or without clicking on any file in the directory).

After the GUI finishes calculating the starting time (the earliest TCP/UDP packet time minus two step times) and the traffic data of each link, it will visualize the data immediately and show the status of the network.   Note that the calculation time will vary according to the performance of your machine and size of the log file.

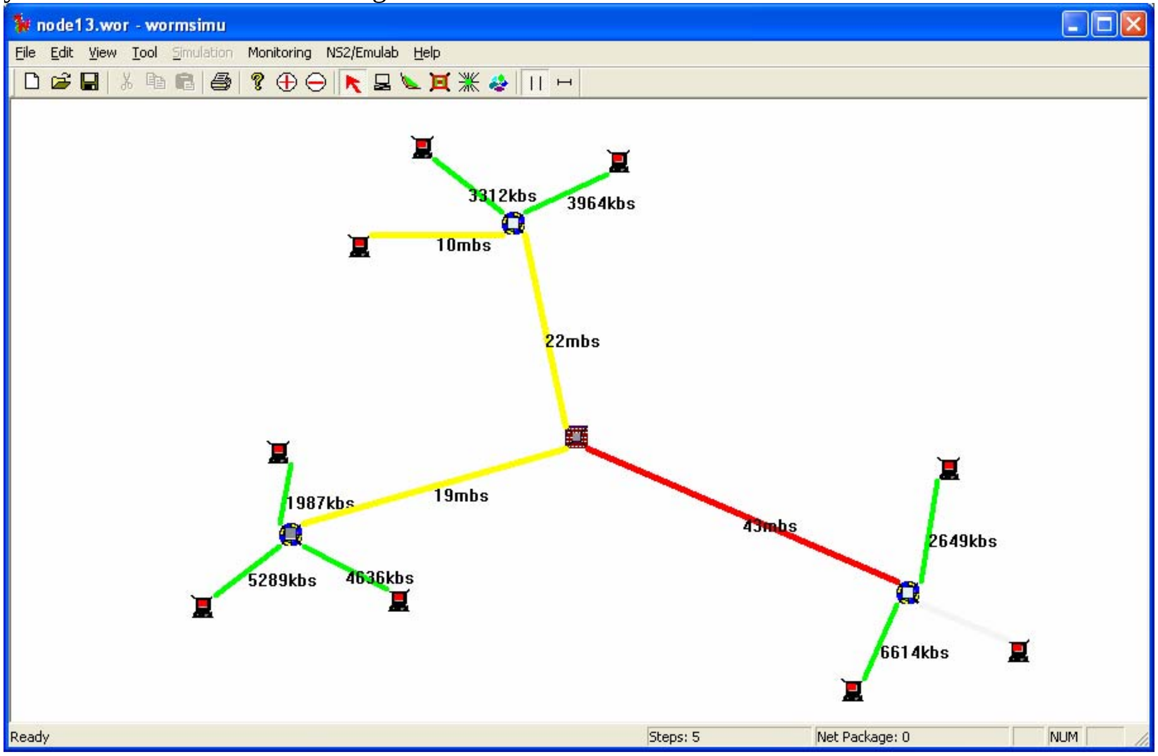


Figure 3: Worm propagation animation

5.3. Interpreting the animation

The color of a link represents the traffic volume on that link (in KBps and in Mbps). The color of a host indicates the host status.

Link color

1) Light Gray: less than 1 percent of bandwidth
2) Green: more than 1 percent of bandwidth
3) Yellow: between green and red
4) Red: more than 30 percent of bandwidth

Host color (Varied by experiment. The following example is for worm experiment.)

1) Red: Infected node.
2) Green: Vulnerable node but not infected
3) Gray: Non-vulnerable node

5.4. Controlling animation

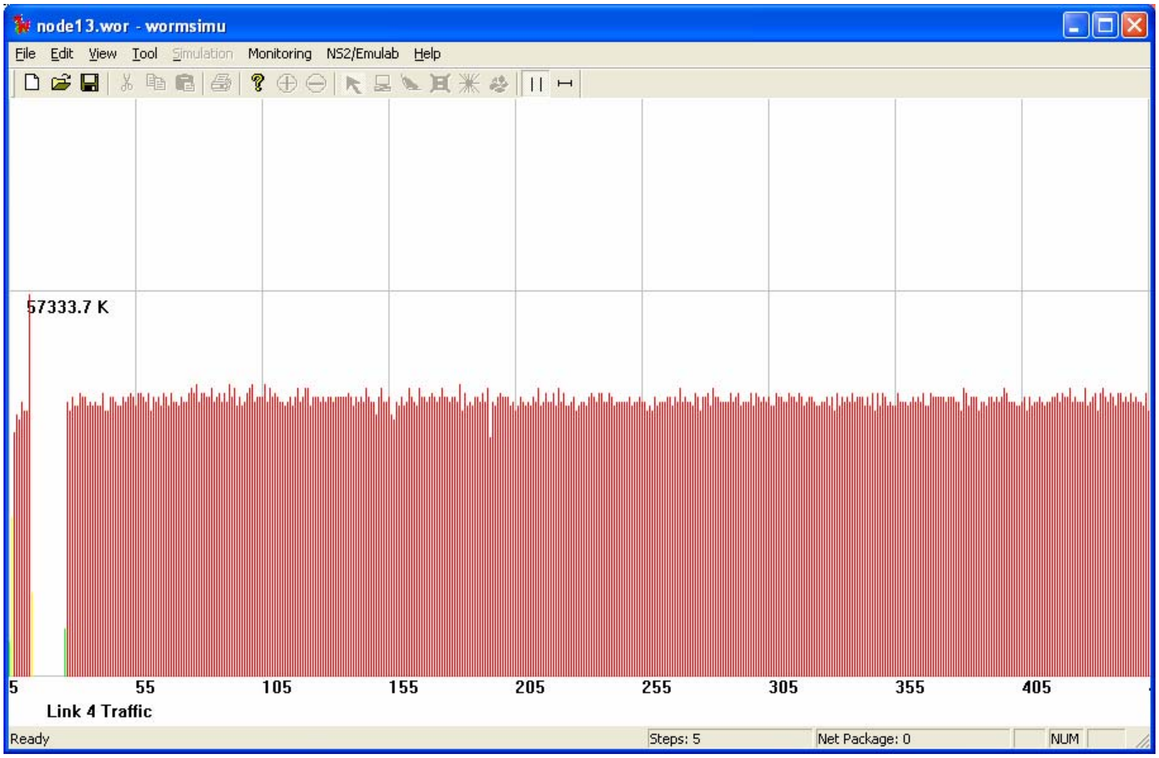
The GUI provides the following two buttons on the right-most side of the toolbar to allow users to control the animation.

| |: Toggle between pause and resume animation

|——|: Move to a specific point in entire simulation time

5.5. Charts and other views

1) Bar chart: Shows the change in traffic on a particular link. **Right-click** on a particular link to show a pop-up menu and choose **Bar Chart** to switch to this view.



2) Worm traffic chart: Shows the traffic composition on a link. **Right-click** on a particular component to show a pop-up menu and choose **Worm Traffic** to switch to this view. The blue part of a bar represents the non-worm background traffic volume. The red part of a bar stands for worm traffic. Currently, this worm traffic chart feature can identify only SLAMMER worm traffic.

To return to the main animation view (main window) from a bar chart view or a worm traffic chart view, choose menu **View->Normal view**.

5.6. Output traffic data to text file

You can save the traffic data of a link into a text-file format for, e.g., further statistical analysis using another software package. Click on the link and choose ->**Output traffic**. The following is a sample of a traffic data file in which each line shows traffic data on a link during one time-step interval.

```
Traffic(kps)    Packets   WormTraffic(kps) WormPackets
       0.000          0        0.000          0
       0.000          0        0.000          0
    2649.600          4        0.000          0
    2649.600          4        0.000          0
    3974.400          6        0.000          0
    5289.600          8        0.000          0
   23846.400         36        0.000          0
   36432.000         55        0.000          0
   39081.600         59        0.000          0
   38419.200         58        0.000          0
   41068.800         62        0.000          0
   39744.000         60        0.000          0
   39744.000         60        0.000          0
```

5.7. Internet scale-down worm experiment visualization

For Internet scale-down worm experiment, use **NS2/Emulab->Internet Simulation Visualization** to see the worm infection animation. Choose **View->Statistics/Traffic** to check the worm infection curve. The followings are samples of an infection log file, which must be named *gui_result*.

```
InfectedIP:    0.0.72.101 Time: 0.00 TotalScans:       4315 Scan/Worm:    4315
InfectedIP:  0.48.170.103 Time: 3.52 TotalScans:       8630 Scan/Worm:    4315
```

6. Features in the next version

- Support of popular network topology formats: The GUI will support the output from popular scale-free topology generators (e.g., those of GA Tech and Umich) and will convert it to EMIST GUI format.
- User-defined visualization: The GUI will allow users to filter packet flows by various FDAs (Flow Defining Attributes) and will have more options pertaining to the type of visualization, e.g., cumulative or sliding time-window.
- Experiment and data management: The GUI will be an interface to the DHS data repository and will incorporate traffic traces of different formats into EMIST GUI.
- Traffic source generation tool from TCPDUMP and NETFLOW traces.