# Information Visualization for an Intrusion Detection System

(by Blustein, Fu, & Silver)

**Objective: A user interface supporting network information visualization for an Intrusion Detection System (IDS).**

1. Help the users to filter/recognize the most important messages from many messages generated by IDS
2. Flexible and adaptable to the users
3. Assists users in overcoming false detections from IDS

## Problems

**Current IDS have several problems that frustrate optimal security efforts:**

1. **Too many false detections**
   a. High traffic volume reduces effectiveness of even the best IDS
   b. Assuming 0.01% false alarm rate x 100,000 events per day = 10 false alarms every day (Both false negative & false positive)
   c. Current typical false alarms for a good IDS: about 5%

2. **IDS detections do not get immediate attention -** high volume of detections (including many false ones) make immediate response difficult.

+

## Spatial Hypermedia

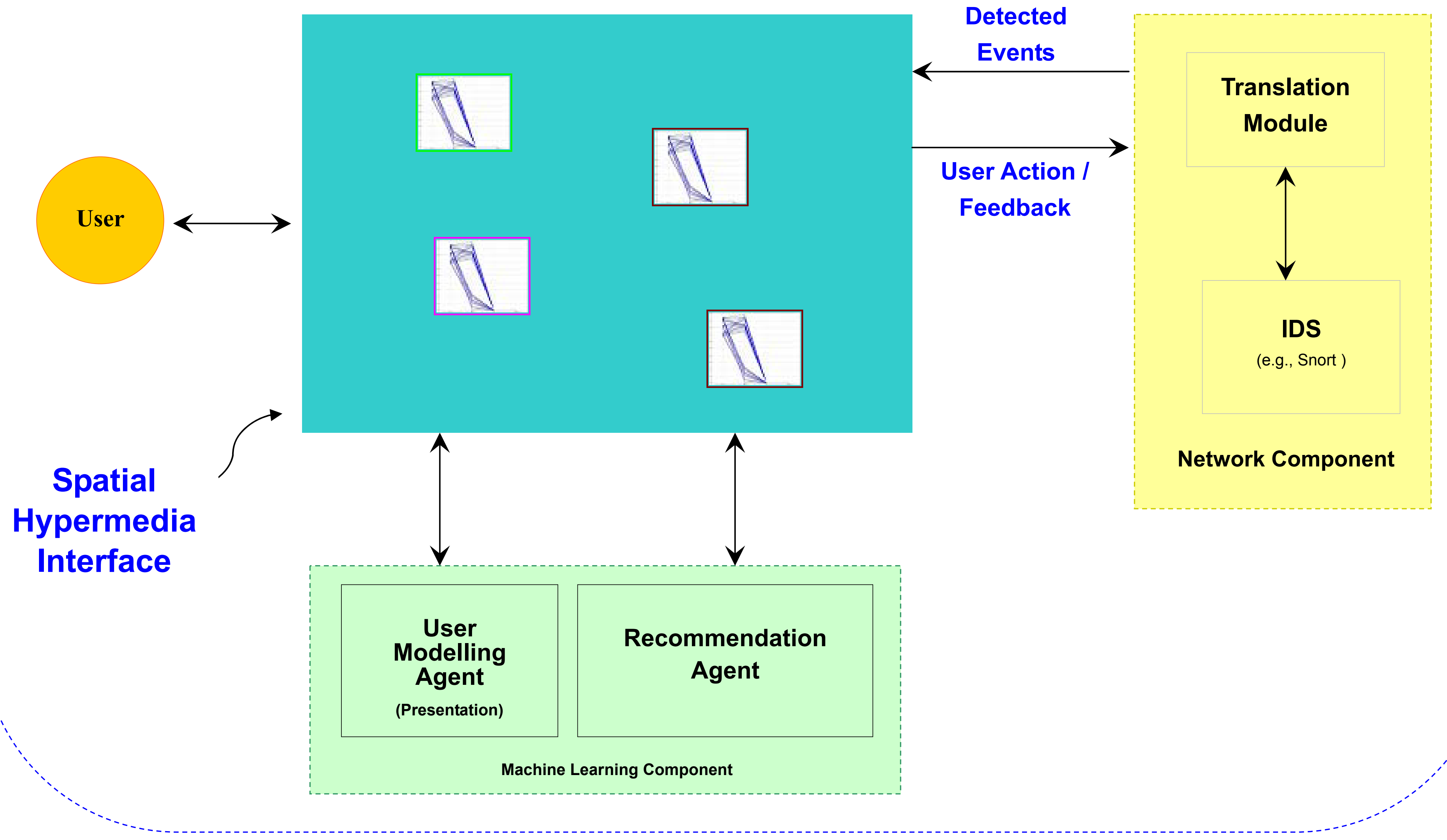
***Information Triage*** – sorting through numerous relevant materials and organize them to meet the needs of the tasks at hand.

1. Suitable for information intensive tasks
2. New patterns can be recognized from the objects on the workspace as the user is working to find a solution.
3. Visually oriented workspace allows the user to recognize familiar patterns and respond immediately.
4. Patterns that are difficult to put into words can be presented to the user with simple spatial cues (color, proximity, alignment, orientation, etc.), and the presentation may be recognized immediately.
5. Containment - able to present the big picture, yet the user can reveal the details very quickly.

=

## Proposed Solution

1. Allow users to visualize network in many dimensions
   a Time, flow, event types, etc.
2. Users can recognize developing patterns
   a Gain a sense of normal network activities
   b Recognize intrusion *as it happens*, not after
3. ***Translation Module*** makes it possible to adopt the user interface to many different IDS programs
4. ***Recommendation Agent*** gives suggestions unobtrusively to assist the user to sort the objects on workspace – so that the user can recognize anomalies more easily.
5. ***User Modelling Agent*** – develops a user model that allows the system interface presentation to be adapted to the user.



User

Spatial Hypermedia Interface

Detected Events

User Action / Feedback

Translation Module

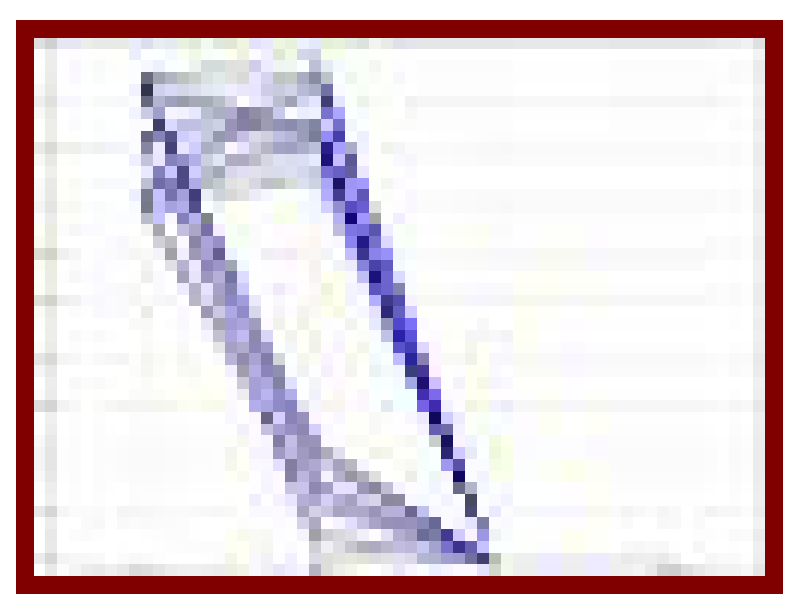
IDS
(e.g., Snort )

Network Component

User Modelling Agent
(Presentation)

Recommendation Agent

Machine Learning Component



***The plot graph icon:*** each icon represents a different host or a sub-network. The different border colors represent the different types of hosts/networks. Features selected by the IDS are used to draw the plot graph.

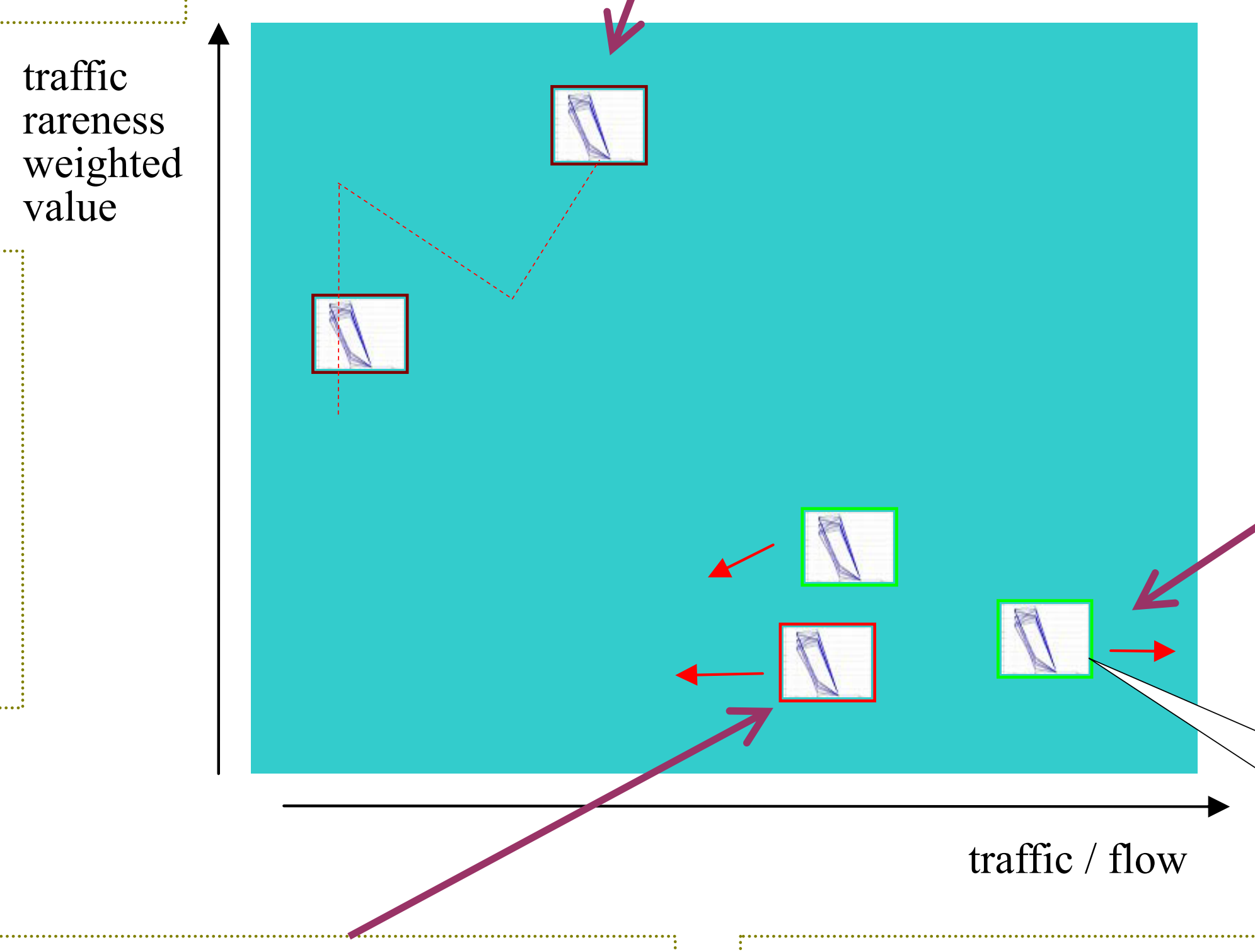
The features could be time of the day, traffic amount, etc.

The graphic pattern could reveal whether there are anomalies from some hosts/ networks.

***Traffic rareness weighted value:***
We give uncommon traffic a higher weight value. The weight indicates level of suspicion. For example, the use of uncommon ports and high traffic volume are suspicious.

***Temporal play back:*** Sometimes, no matter how you look at the current patterns, the vital information cannot be presented in the 'snapshot view.' The pattern is only visible over time. A way to reveal an attack pattern is to show the historical traffic pattern.

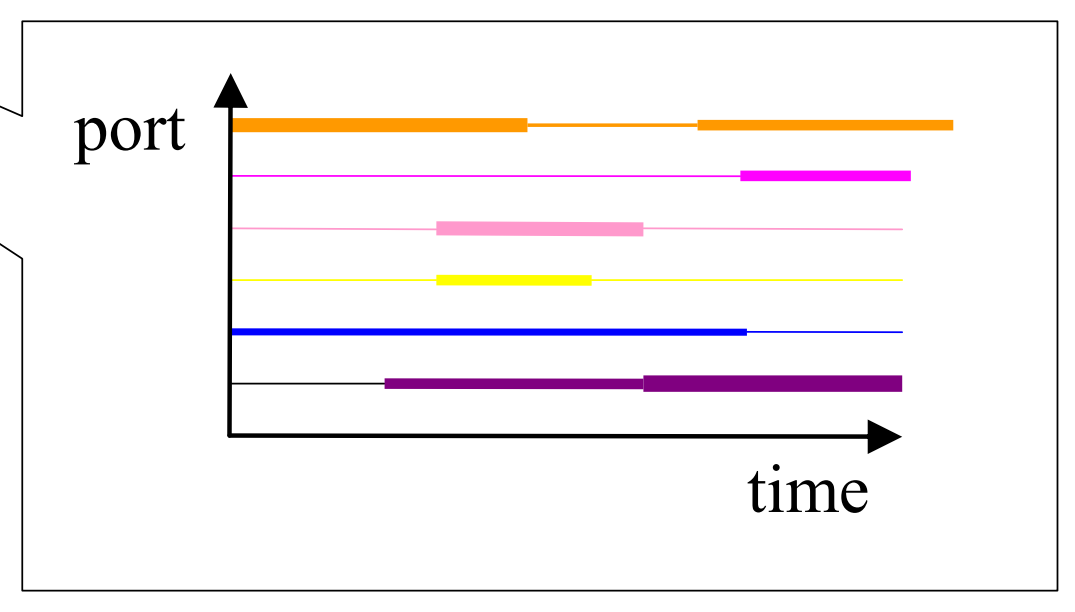
The user can select one or more networks/hosts to playback. A slider control is provided to let the user manipulate the time index. The user can see how the patterns were changed and the positions of the objects in the work space.



The moving directions of the objects can also reveal important information.
For example, if an object is moving apart (toward right) from the others, the host might be experiencing a denial of service attack.

This represents a sub-network. We can also choose to drill down to see the hosts / sub-networks in the lower level. It will look similar in style to what has been shown here.

The user can manipulate objects on the workspace. This means that the scale of the range of the graph is distorted. Sometimes, it is a means of showing some details that are not easy to see in the normal scale.



1. Drill down of the object reveals the traffic flow of the host/network
2. Each bar is given a unique color for easy identification
3. Each bar is a different traffic identified by TCP port number
4. The width of each bar represents the flow of the traffic (bandwidth)

## Issues

1. Too many hosts/networks in the workspace
   Possible solutions:
   a Multiple screens for different part of the network
   b Fisheye/distorted view – display entire, yet part of the details is revealed
2. Pattern presentation using a 'plot graph icon'
   A challenge to find suitable plane in the multi-dimension space to show the significance of anomaly patterns
3. Feature selection for plot graph icon
   The number of important features in from the input is huge. A proper selection of features is directly related to the effectiveness of the interface.
4. Definition of the traffic rareness weighted value it
5. Other issues?
   Your input will be greatly appreciated!