The Netflow Observatory: An Interactive 3-D Event Visualization

Larry Bunch
Florida Institute for Human and Machine Cognition
40 S. Alcaniz St.
Pensacola, FL
+1 850-202-4475
lbunch@ihmc.us

Jeffrey M. Bradshaw
Florida Institute for Human and Machine Cognition
40 S. Alcaniz St.
Pensacola, FL
+1 850-202-4422
jbradsahw@ihmc.us

Michael Vignati
Florida Institute for Human and Machine Cognition
40 S. Alcaniz St.
Pensacola, FL
+1 850-202-4422
mvignati@ihmc.us

ABSTRACT
This poster describes a novel interactive three-dimensional visualization capable of displaying large numbers of temporal events and their attributes. A prototype implementation using Netflow network traffic metadata displays interactions between an enterprise computer network and the public Internet to reveal communication patterns and help identify suspicious cyber behavior.

Categories and Subject Descriptors
H.5.2 [**Information Interfaces and Presentation**]: User Interfaces—*Graphical user interfaces (GUI);* D.4.6 [**Security and Protection**]: Information flow controls; C.2.0 [**Computer-Communication Networks**]: General – *Security and protection*; C.2.3 [**Computer-Communication Networks**]: Network Operations – *Network monitoring*

General Terms
Design, Security, Human Factors.

Keywords
Event Visualization, Network Monitoring, Netflow.

1. INTRODUCTION
This poster describes the Netflow Observatory prototype visualization software. This visualization uses a metaphor of particles flowing through 3-D space with the passing of time to represent computer network communication events. Several aspects of this approach have been designed specifically to engage the human ambient vision channel for the task of monitoring network traffic and directing the users focus toward anomolies.

2. BACKGROUND
The metaphor underlying the Observatory visualization is representing temporal events as particles in water flowing through a segment of a transparent tube. Time is the common frame of reference for the events and dictates each event particle's relative location on the timeline along the tube length. Particles have different characteristics like size and color, but all particles flow through the tube at the same speed. One can then imagine placing patterned surfaces at either end of the tube so that these surfaces determine where the particles enter and leave the tube according to some attributes of the events the particles represent.

This concept is similar to the parallel coordinates visualization [1] extended to three dimensions with each coordinate projected onto a plane rather than a line. These planar coordinates enable using an image, such as a world map, to represent the range of possible values for a given coordinate.

3. VISUAL PRINCIPLES
Many aspects of this visualization are designed to take advantage of the human ambient vision system by applying lessons learned from the OZ flight display [2, 3]. People use ambient vision naturally to maintain spatial awareness and direct their focal vision. For example, when driving a car one uses focal vision to read a road sign while simultaneously using ambient vision to stay in the lane, notice if traffic slows ahead, and find the next road sign. Engaging ambient vision is a key characteristic we are leveraging specifically to create more effective real-time monitoring visualizations. Visual aspects that work well in this regard include: the use of a simple atomic graphic primitives like line segments and rectangles, the high contrast created by the black background, and the use of motion to convey change over time.

4. NETFLOW PROTOTYPE
Figure 1 is a screenshot from the Netflow Observatory prototype that has been annotated to point out specific features. Each particle or 'dart' represents one or more network connections as collected from an enterprise router using the Cisco Netflow metadata format [4]. The top map represents the geo-location of the source IP address for the network connection and the bottom map represents the geo-location of the destination IP address. As time advances, these darts appear on the top map and move on a trajectory toward the bottom map. The darts are color-coded by source and destination country. Some of the darts have been annotated with larger red dots indicating in this case a match of an IP address with a blacklist of known bot IP addresses [5].

The visualization is played much like a video where as time advances the timeline along the left margin scrolls down and the event darts all flow from top to bottom based on the timestamp for each Netflow event record. Note that the one can control the rate and direction of the flow of time. In the center of Figure 1 are objects labeled with specific ports such as 'http:80'. These 'port rings' attract only event darts that have the given property such that these darts must flow through the ring en route to their target location on the destination map.

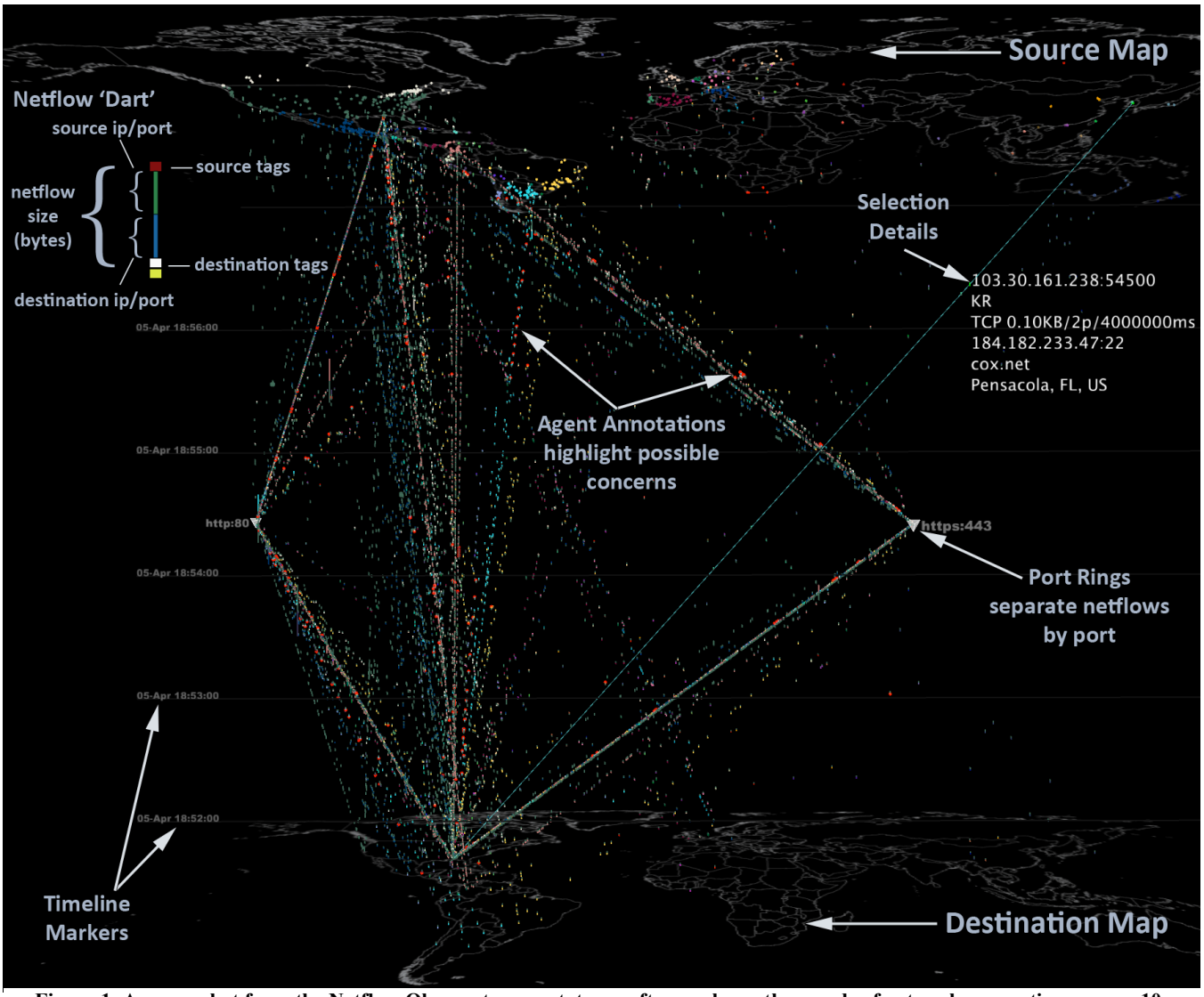

Figure 1. A screenshot from the Netflow Observatory prototype software shows thousands of network connections over a 10-minute timeframe. The screenshot has been annotated to describe particular features including the IP address geo-location maps, individual event darts, and port rings.

5. ACKNOWLEDGMENTS

Our thanks to Tamara Yu and Maureen Hunter at MIT Lincoln Lab for their valuable contributions and support.

6. REFERENCES

[1] Inselberg, A., & Dimsdale, B. (1991). Parallel coordinates. In *Human-Machine Interactive Systems* (pp. 199-233). Springer US.

[2] Still, D. L., & Temme, L. A. 2001. OZ: A human-centered computing cockpit display. In *The Interservice/Industry Training, Simulation & Education Conference* (Vol. 2001, No. 1). I/ITSEC 2001. National Training Systems Association.

[3] Still, D. L., Eskridge, T. C., & Temme, L. A. (2004). Interface for non-pilot UAV control. In *Human factors of UAVs workshop, Mesa, AZ.*

[4] NetFlow Version 9 Flow-Record Format. 2011. http://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9_ps6601_Products_White_Paper.html

[5] The Carrot and The Stick Project. http://tcats.stop-spam.org/nmsbl/.