CEG7560

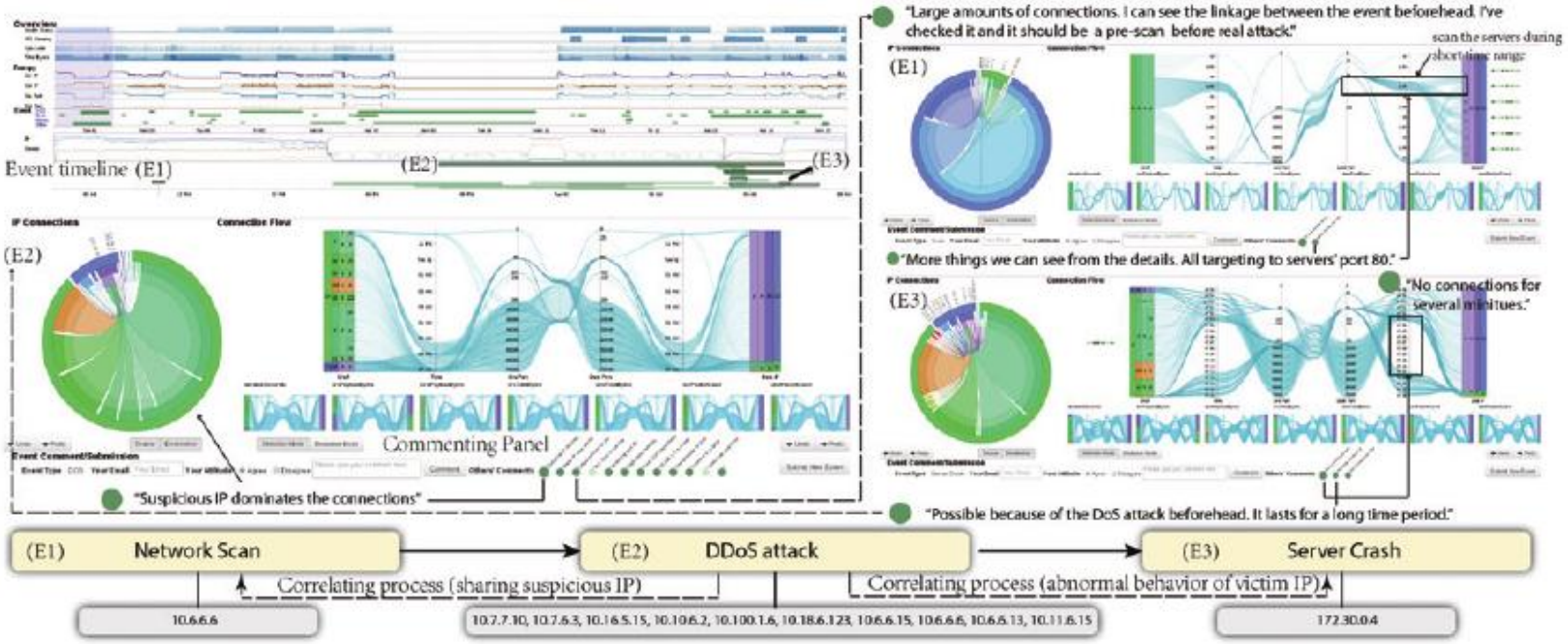
Visualization Examples for Cyber Security

Sample Visualization

OCEANS - Online Collaborative Explorative Analysis on Network Security:

Visualization and interactive analysis can help network administrators and security analysts analyze the network flow and log data. The complexity of such an analysis requires a combination of knowledge and experience from more domain experts to solve difficult problems faster and with higher reliability. The online visual analysis system called OCEANS was developed to address this topic by allowing close collaboration among security analysts to create deeper insights in detecting network events. Loading the heterogeneous data source (netflow, IPS log and host status log), OCEANS provides a multi-level visualization showing temporal overview, IP connections and detailed connections. Participants can submit their findings through the visual interface and refer to others' existing findings. Users can gain inspiration from each other and collaborate on finding subtle events and targeting multi-phase attacks. Our case study confirms that OCEANS is intuitive to use and can improve efficiency. The crowd collaboration helps the users comprehend the situation and reduce false alarms.

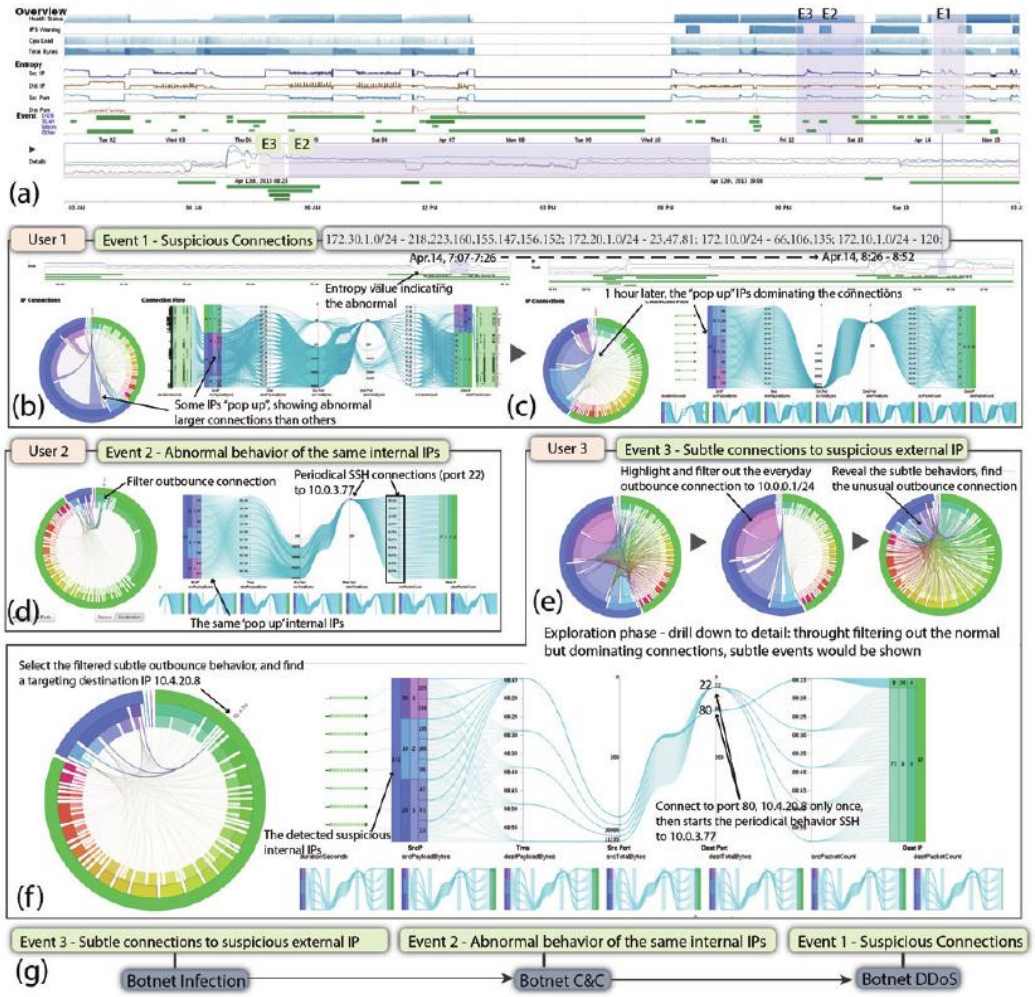
Sample Visualization



Event correlation and subtle events detection. Pre-scanning (subtle) before the DDoS attack. (E3) Server(E2) DDoS attack with many comments on it. (E1) crash (subtle) after the DDoS attack

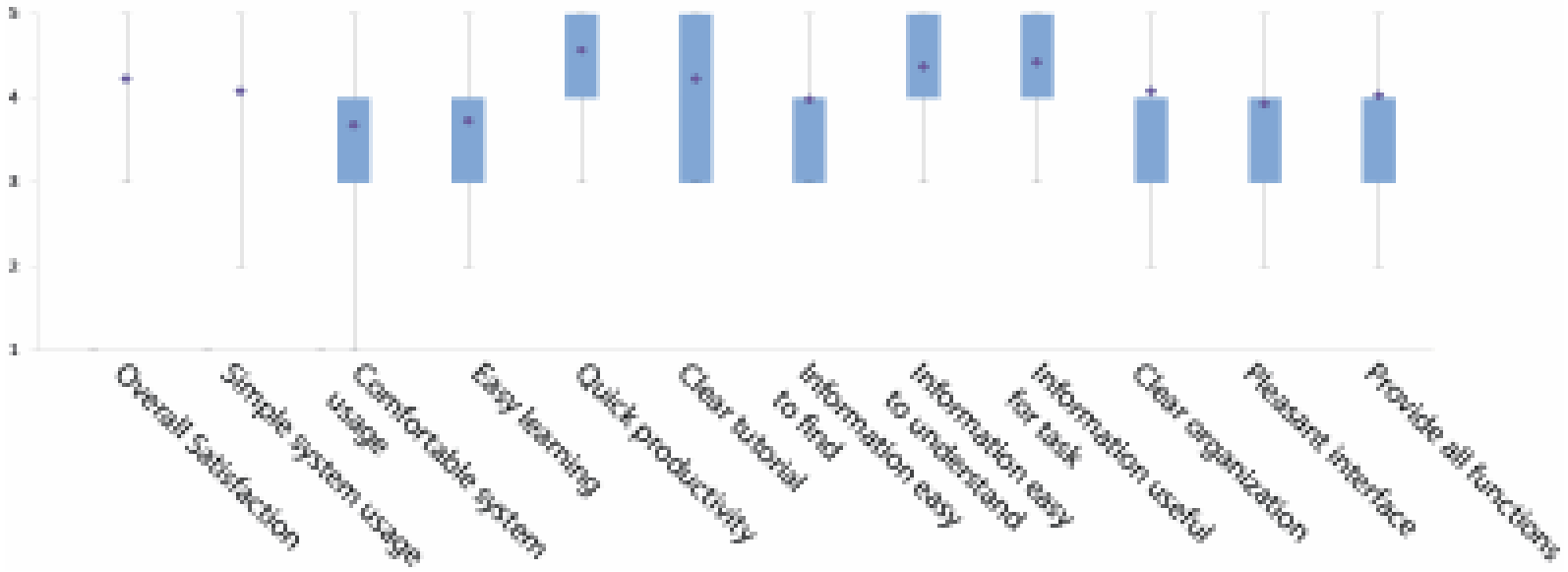
Sample Visualization

Botnet analysis. (a) Overview timeline. (b,c)-E1, firstly detected events, which turned out to be a botnet DDoS attack. (d)-E2, secondly detected events. By applying filters, user found the suspicious outbounce SSH connections. (e,f)-E3, botnet infection as subtle event. (g) Summarized attack pattern.



Sample Visualization

User evaluation: Feedback based on questionaire



Sample Visualization

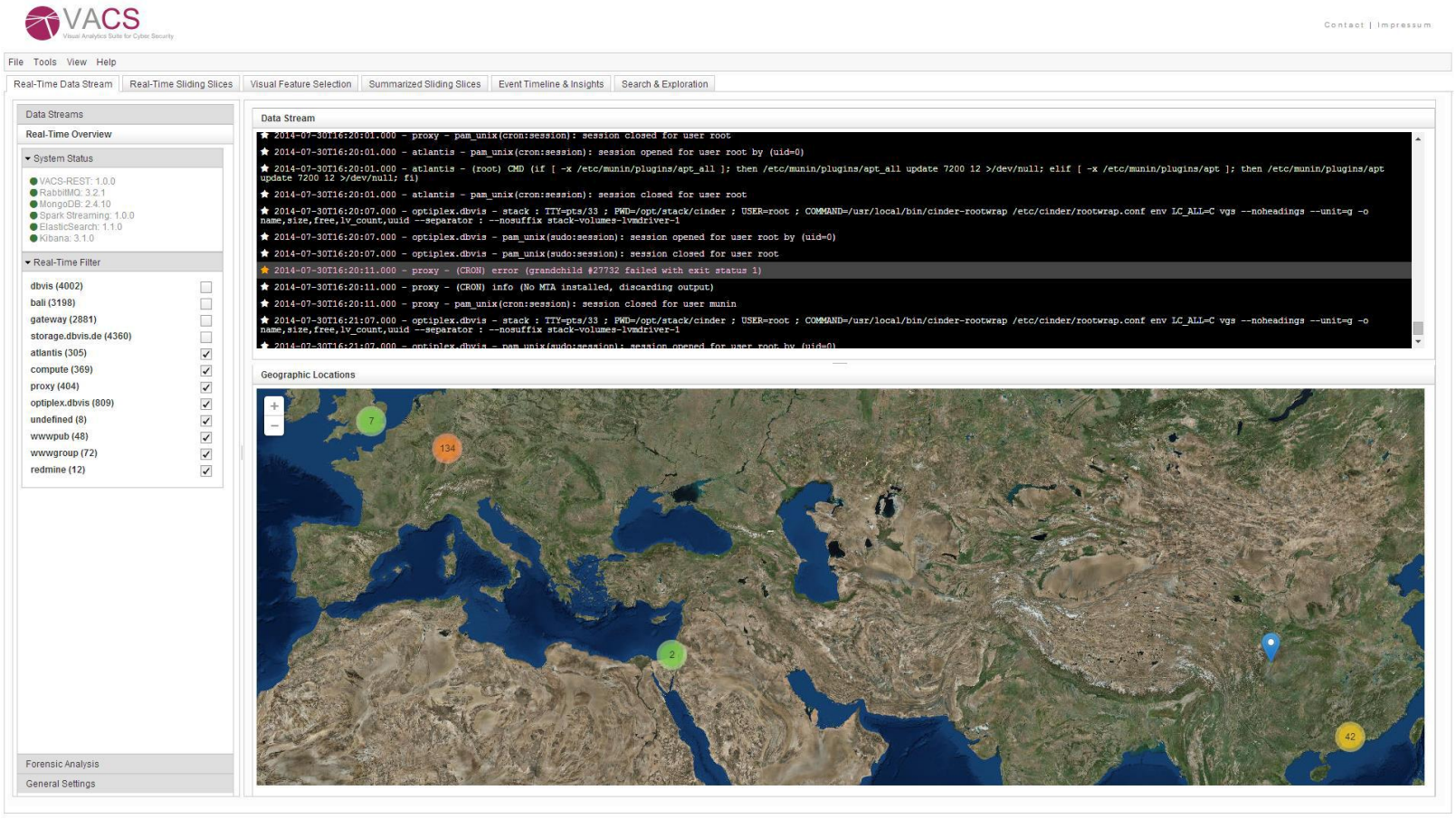
NStreamAware: Real-Time Visual Analytics for Data Streams to Enhance Situational Awareness

Integrated Perspectives

- Real-Time Data Stream Monitoring
- Real-Time Sliding Slices (NVisAware)
- Visual Feature Selection
- Summarized Sliding Slices
- Event Timeline & Insights
- Search & Exploration

Sample Visualization

Real-Time Data Stream Monitoring



Sample Visualization

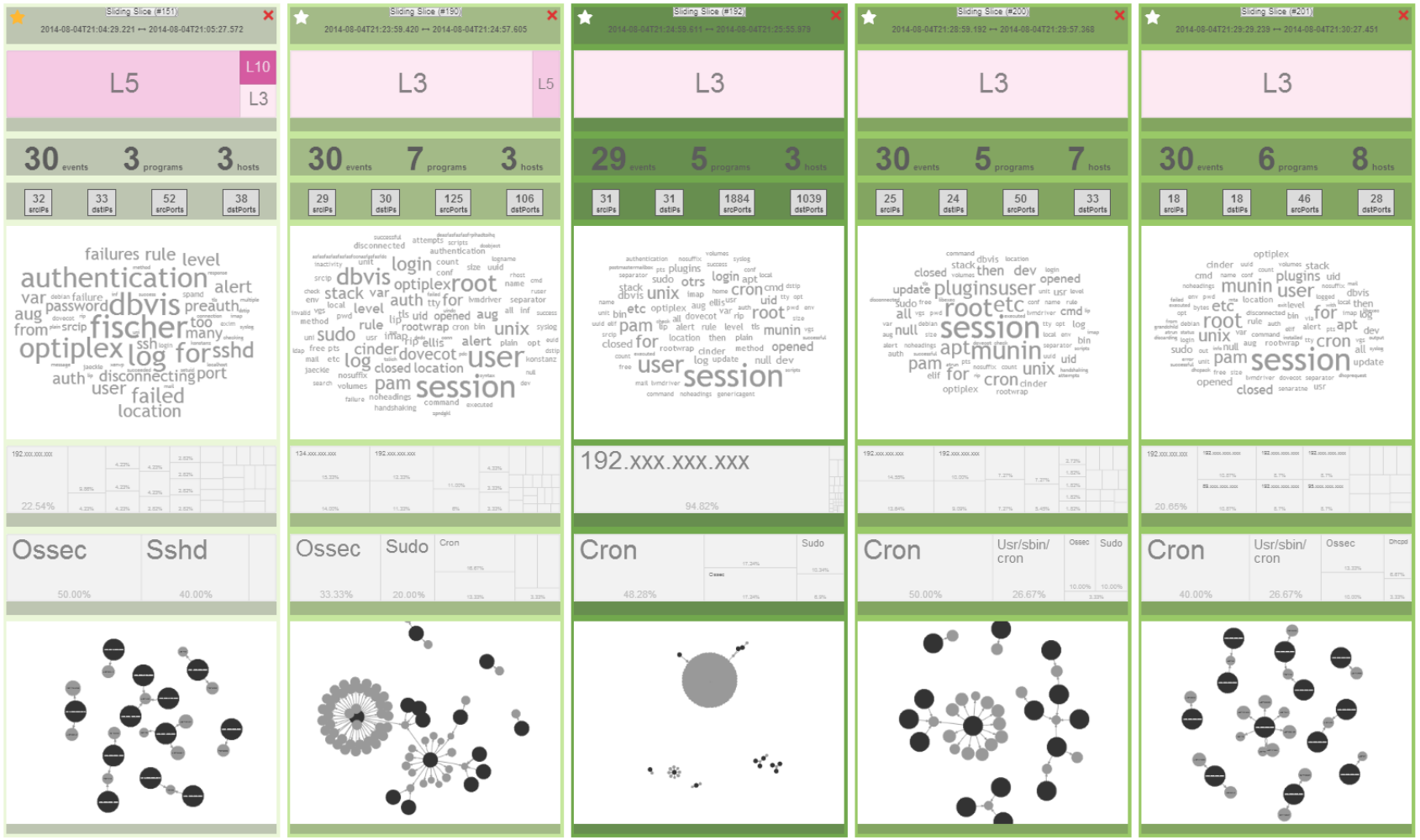
Real-Time SlidingSlice

- Interactive Widgets
  - Treemaps
  - Counters
  - Node-link diagrams
- Interactions
  - Star/Annotate slice
  - Remove slice
  - Retrieve data
- Color Encoding
  - Background for similarity
  - Importance of alerts

Feature	Type	Stream
#events	count	Syslog
timestamps	set	Syslog
#programs	count	Syslog
#hosts	count	Syslog
#frequentWords	count	Syslog
programs	key-value list	Syslog
hosts	key-value list	Syslog
frequentWords	key-value list	Syslog
newHosts	new-set	Syslog
newPrograms	new-set	Syslog
srcAddr	key-value list	NetFlow
dstAddr	key-value list	NetFlow
srcPorts	key-value list	NetFlow
dstPorts	key-value list	NetFlow
topTalker	key-array list	NetFlow
#srcAddr	count	NetFlow
#dstAddr	count	NetFlow
#srcPorts	count	NetFlow
#dstPorts	count	NetFlow
ossecAlerts	key-value list	OSSEC

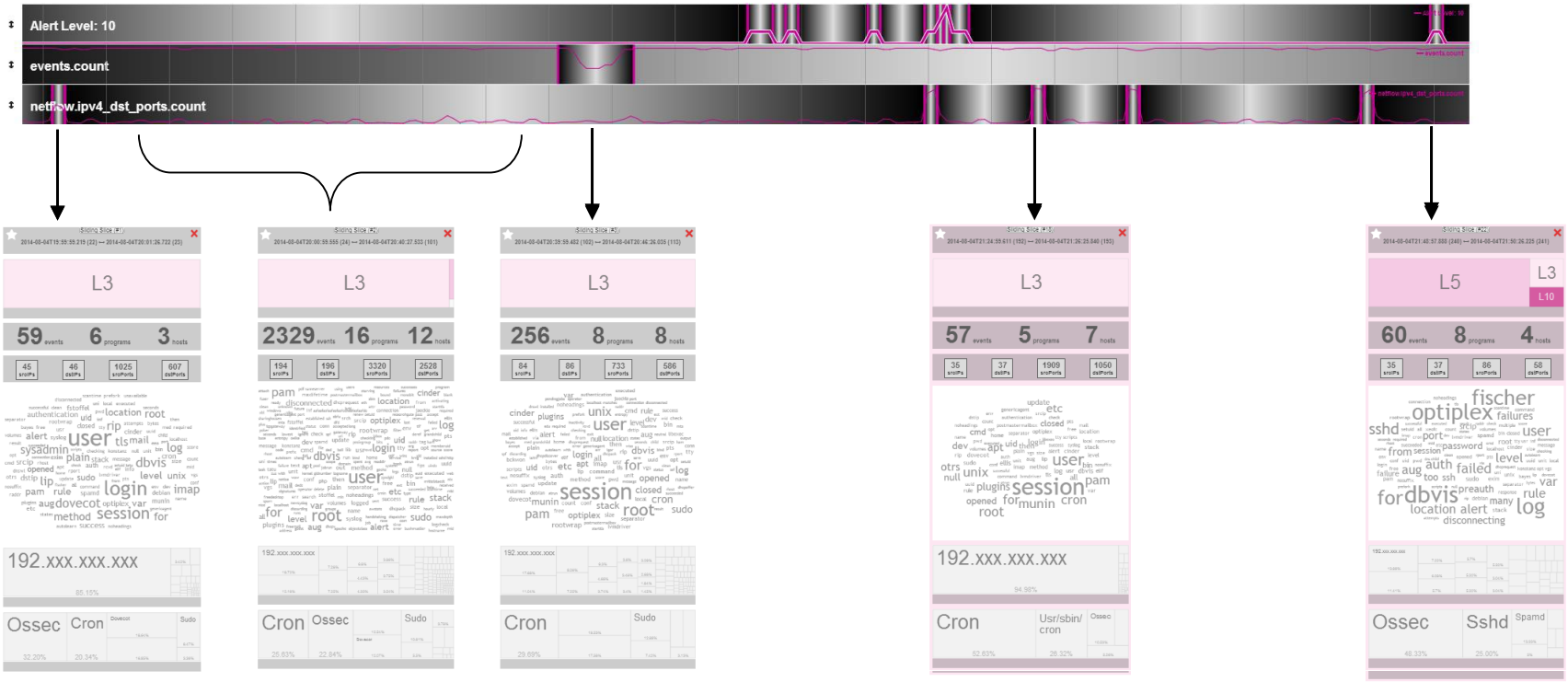
slicet

Sample Visualization



Sample Visualization

Example: UsingVisual Analytics for Interactive Summarization



Sample Visualization

Multiple Queries with Conditional Attributes (QCATs) for Anomaly Detection and Visualization

Sample Visualization

SEEM: A Scalable Visualization for Comparing Multiple Large Sets of Attributes for Malware Analysis

Sample Visualization

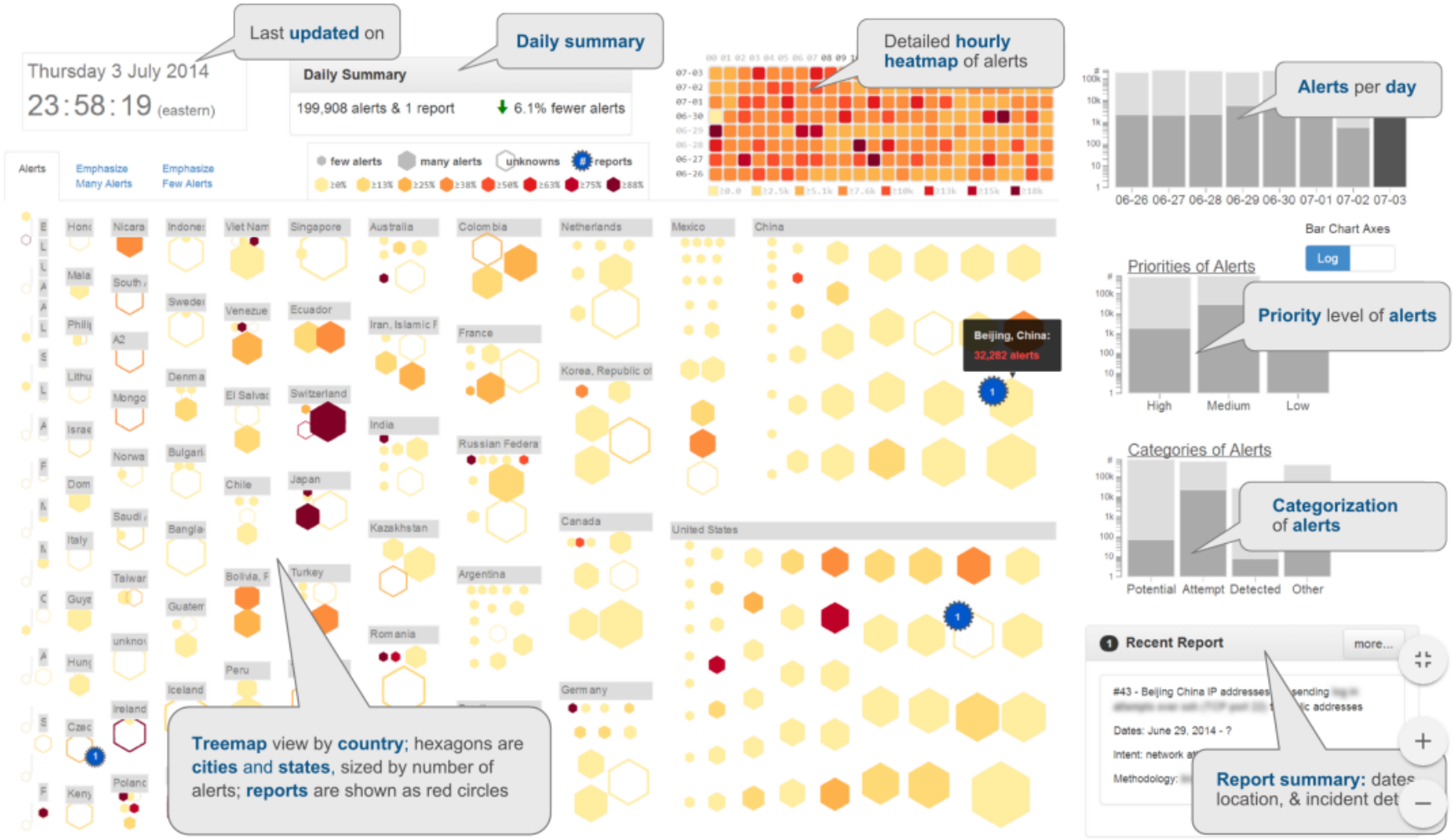
Designing STAR: A Cyber Dashboard Prototype

A central challenge for a strong cyber defense is the appropriate communication of cyber information. There are many key stakeholders that make decisions and convey information up to different levels of authority, and this information may not always be in sync. Additionally, cyber analysts know and often utilize technical jargon to pass along information, and these analysts can spend significant time and effort to building their own visualizations manually, such as network summaries, patterns, and recent attacks. To aid communication, a working prototype of a cyber dashboard was developed which visualizes a simplified view of a network, particularly the key external players which are extracted from both IDS alerts and reports from a traffic analyst. This prototype is one step towards enabling analysts to simplify and encode information into a visualization that can help tell the story of a cyber attack or a network's current defense status.

Sample Visualization

This paper presents a cyber visualization, or the STAR dashboard, an interactive web prototype with linked views that enable the use of simple stories by conveying both IDS alert data on top of analyst-created reports, connected through the use of external entities, both countries and cities, in the main treemap view.

Sample Visualization



Sample Visualization

CORGI: Combination, Organization and Reconstruction through Graphical Interactions

Sample Visualization

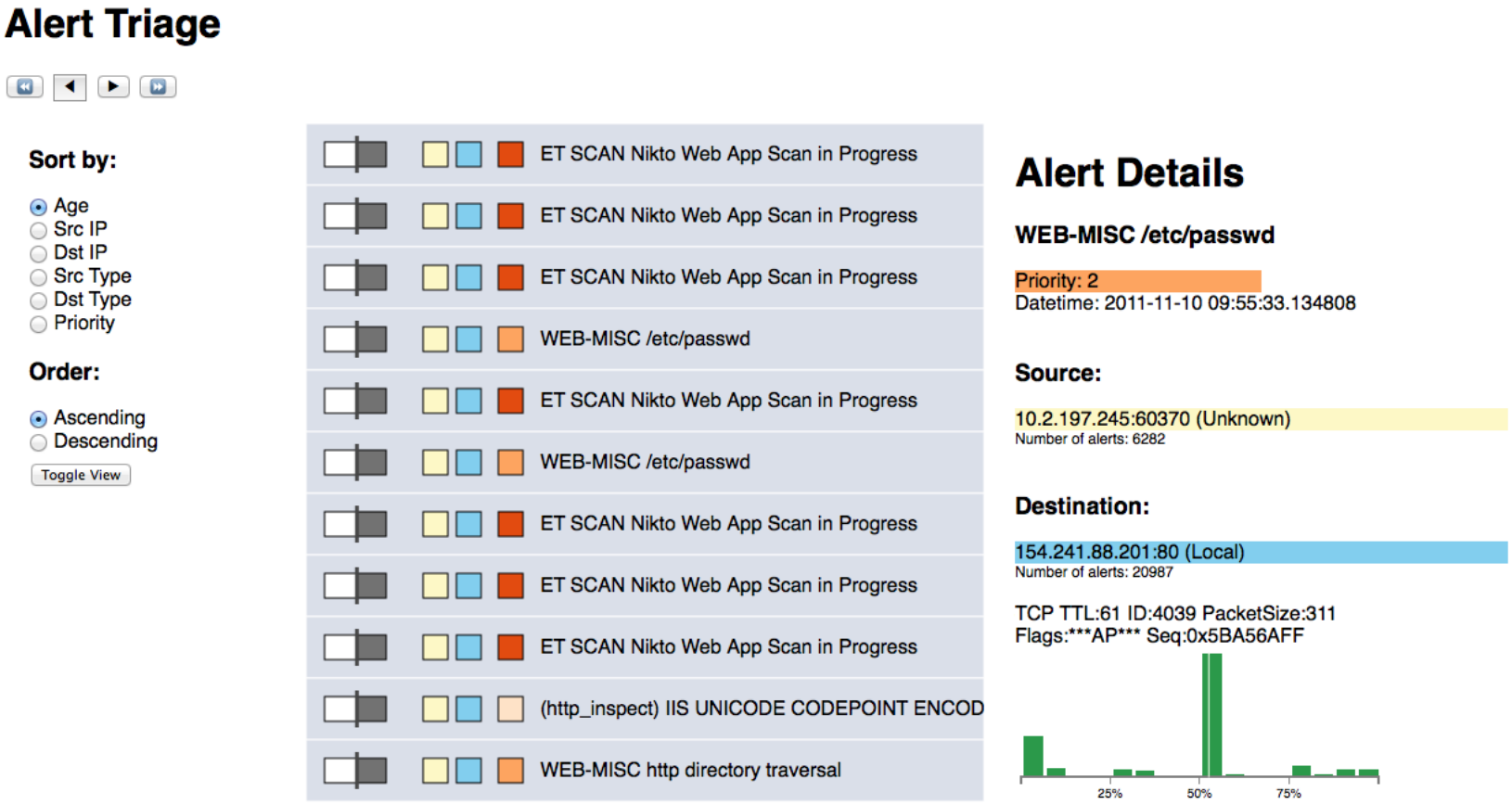
Visual Filter: Graphical Exploration of Network Security Log Files

Sample Visualization

A Tool for Rapid Visual Interrogation & Triage of Alerts

This paper presents a tool to assist in the rapid browsing and interrogation of network alert data from monitoring systems like Snort. The tool are designed for time-sensitive applications where further analysis is offloaded after initial identification; thus, rapid exploration and at-a-glance summaries are paramount. Towards these ends, our primary tool uses simple visualization and interaction for identifying what alerts need processing.

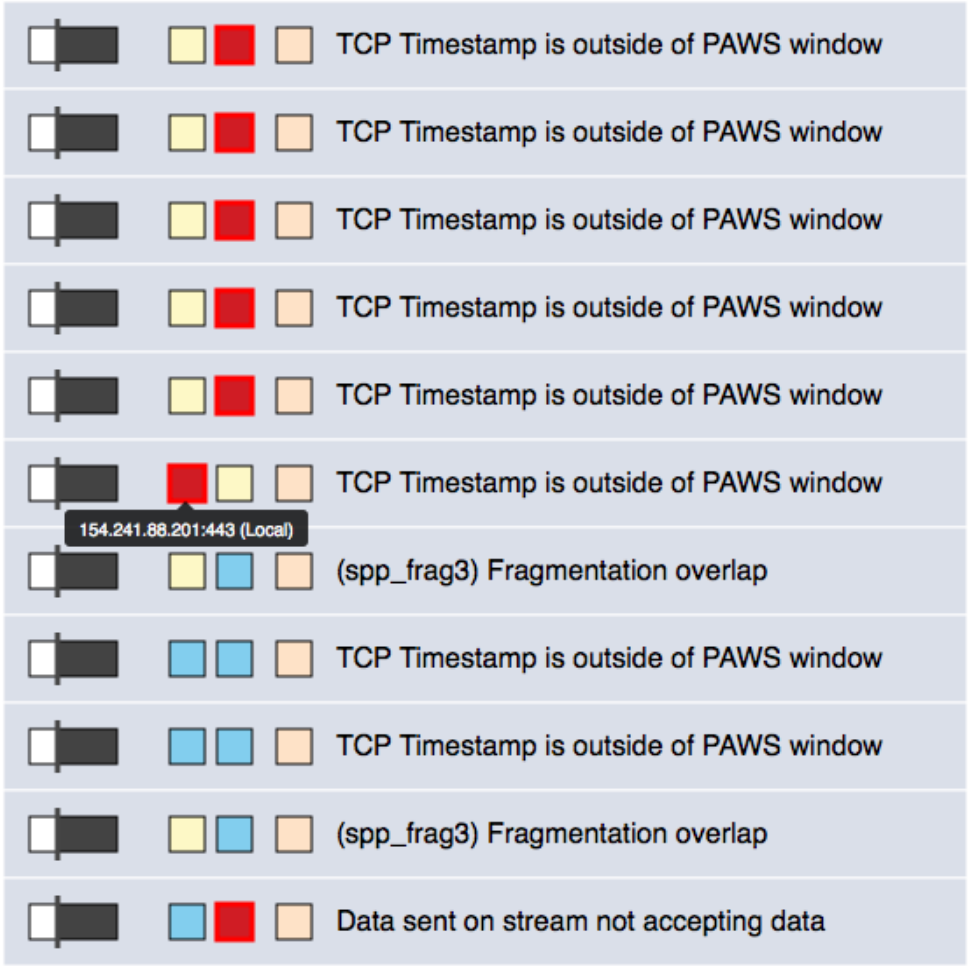
Sample Visualization



The Alert Triage System. Events information is summarized in the center, with specific alert data and the event histogram to the right, navigation to the left.

Sample Visualization

Marking: Compromised and malicious IPs can be marked in red for triage and later processing.

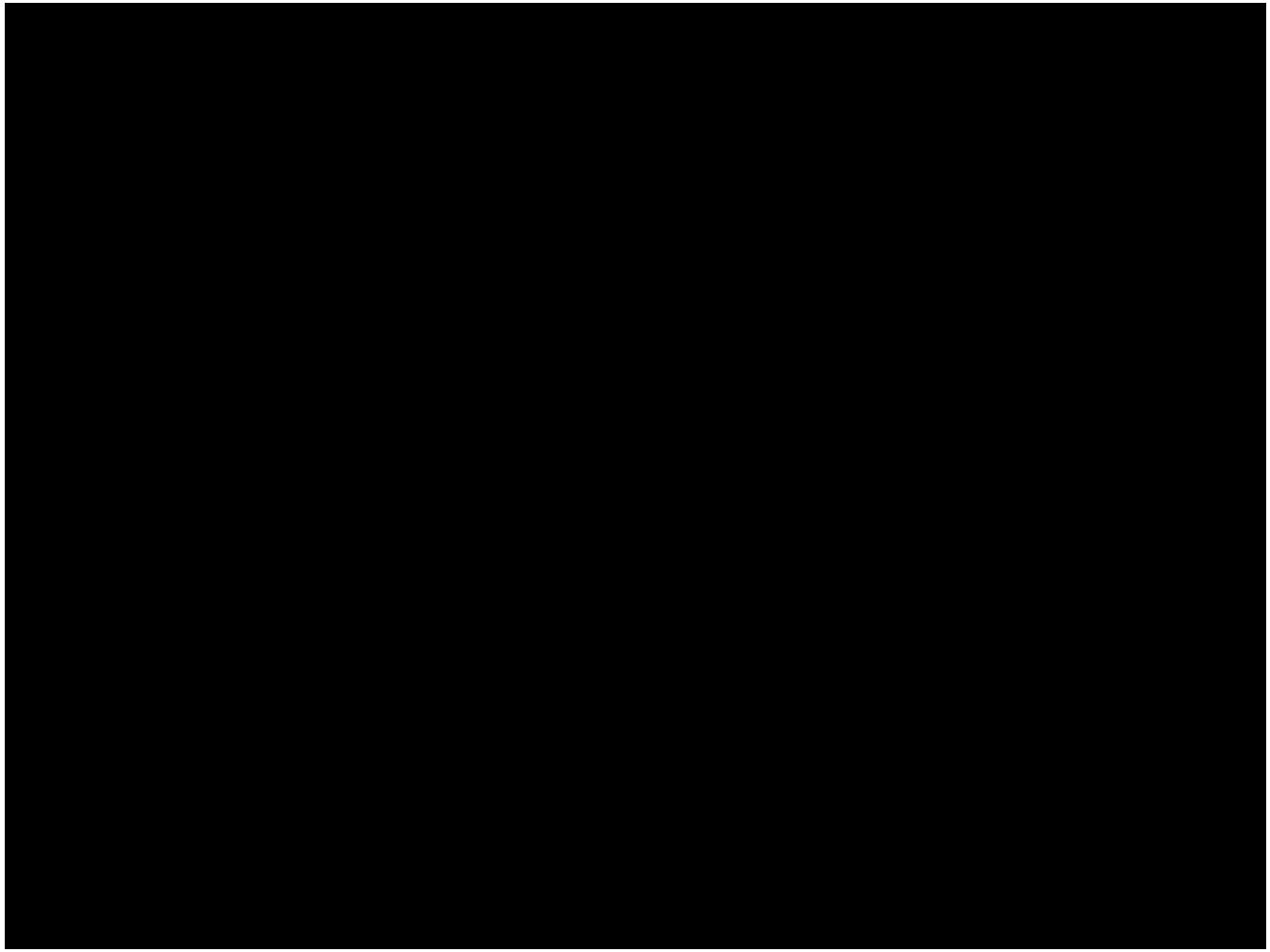


Sample Visualization

SNAPS: Semantic Network traffic Analysis through Projection and Selection

Most network traffic analysis applications are designed to discover malicious activity by only relying on high-level flowbased message properties. However, to detect security breaches that are specifically designed to target one network (e.g., Advanced Persistent Threats), deep packet inspection and anomaly detection are indispensible. This paper focuses on how to support experts in discovering whether anomalies at message level imply a security risk at network level. SNAPS (Semantic Network traffic Analysis through Projection and Selection), provides a bottom-up pixel-oriented approach for network traffic analysis where the expert starts with low-level anomalies and iteratively gains insight in higher level events through the creation of multiple selections of interest in parallel. The tight integration between visualization and machine learning enables the expert to iteratively refine anomaly scores, making the approach suitable for both post-traffic analysis and online monitoring tasks. To illustrate the effectiveness of this approach, example explorations on two real-world data sets for the detection and understanding of potential Advanced Persistent Threats in progress are presented.

Sample Visualization



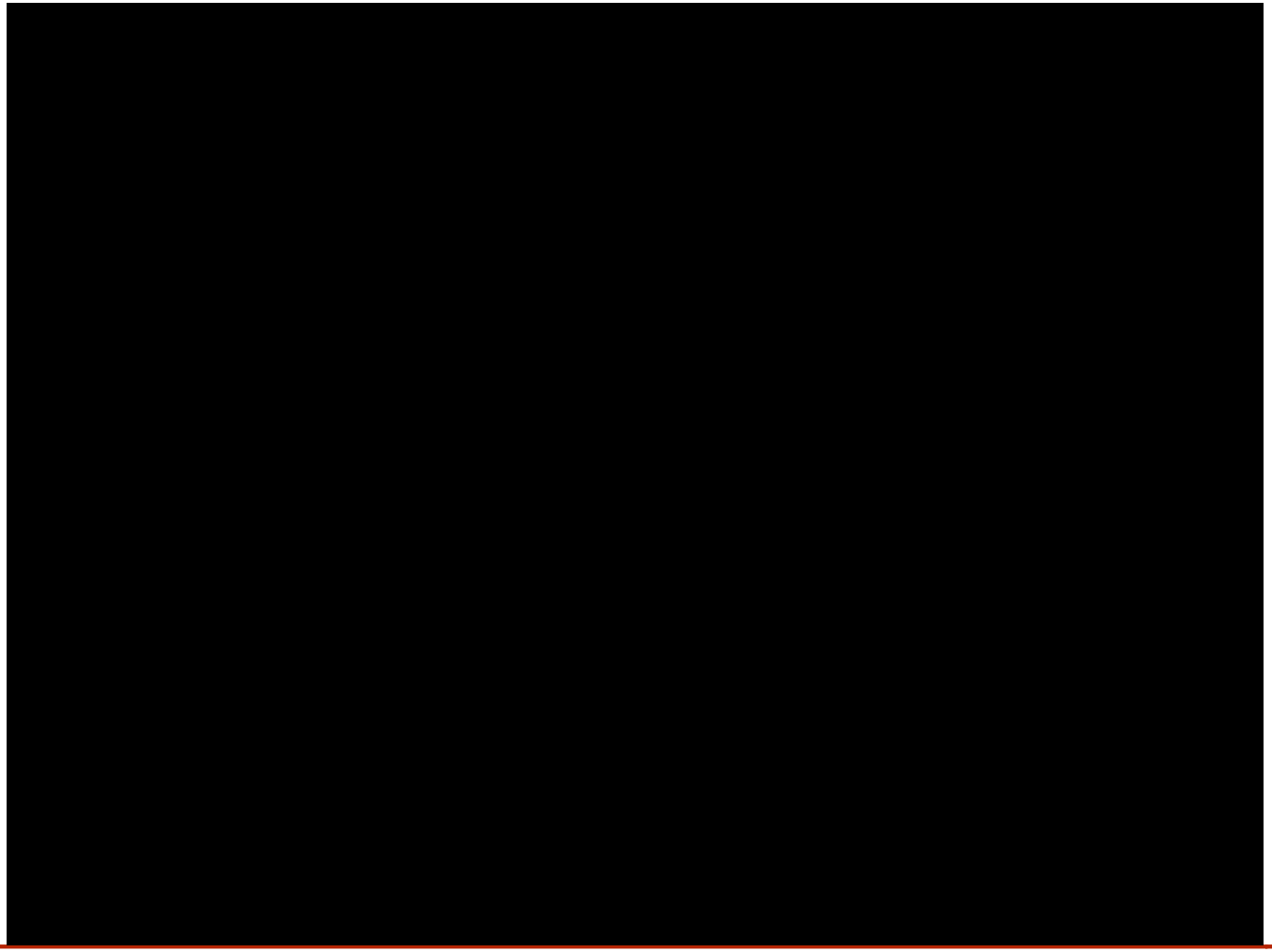
Sample Visualization

PERCIVAL: Proactive and rEactive attack and Response

assessment for Cyber Incidents using Visual AnaLytics

Abstract—Situational awareness is a key concept in cyber-defence. Its goal is to make the user aware of different and complex aspects of the network he or she is monitoring. This paper proposes PERCIVAL, a novel visual analytics environment that contributes to situational awareness by allowing the user to understand the network security status and to monitor security events that are happening on the system. The proposed visualization allows for comparing the proactive security analysis with the actual attack progress, providing insights on the effectiveness of the mitigation actions the system has triggered against the attack and giving an overview of the possible attack's evolution. Moreover, the same visualization can be fruitfully used in the proactive analysis since it allows for getting details on computed attack paths and evaluating the mitigation actions that have been proactively computed by the system. A preliminary user study provided a positive feedback on the prototype implementation of the system.

Sample Visualization



Sample Visualization

The Netflow Observatory:

An Interactive 3-D Event Visualization

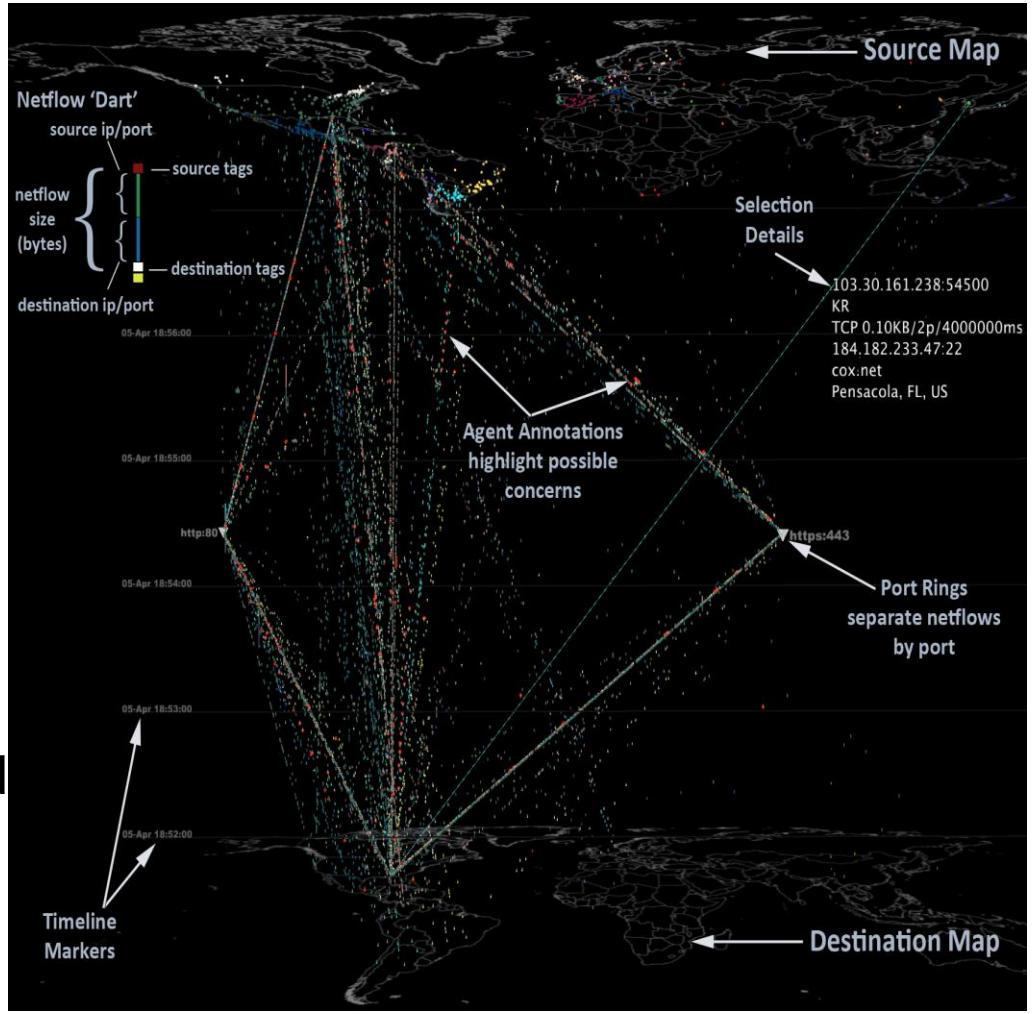
This work describes a novel interactive three-dimensional visualization capable of displaying large numbers of temporal events and their attributes. A prototype implementation using Netflow network traffic metadata displays interactions between an enterprise computer network and the public Internet to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

Sample Visualization

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.

Sample Visualization

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.



Sample Visualization

CyberSAVe – Situational Awareness Visualization for Cyber Security of Smart Grid Systems

Problem:

- Lack of visualization techniques for Cyber Trust

Application:

- Power Grid SCADA system

Solution:

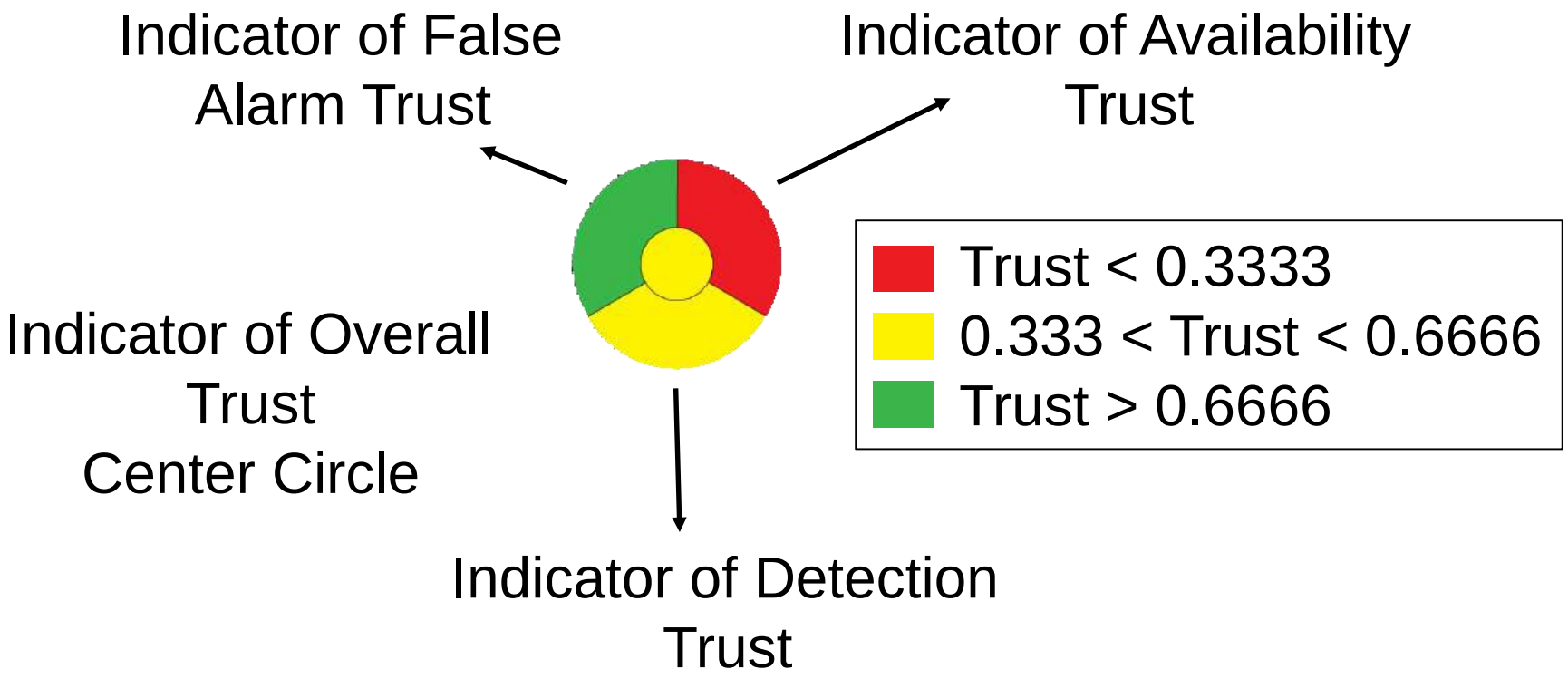
- Mathematical model for Cyber Trust
- Geo-Spatial Visualization of trust for each power plant and sub-station
- Calculation / Visualization of Trust Metrics (Time history, Histogram)
- Visualization of data aggregations (Geographic & bar graphs)

Sample Visualization

Multi-Dimensional Trust

- Different behaviors lead to different types of trust
- Power grid cyber attacks
  - False alarm → False alarm trust
  - Missed detection → Detection trust
  - Damaged/affected sensor → Availability trust
- Overall trust
  - Computed from all three types of trust
  - Weighted average, minimum, predictability

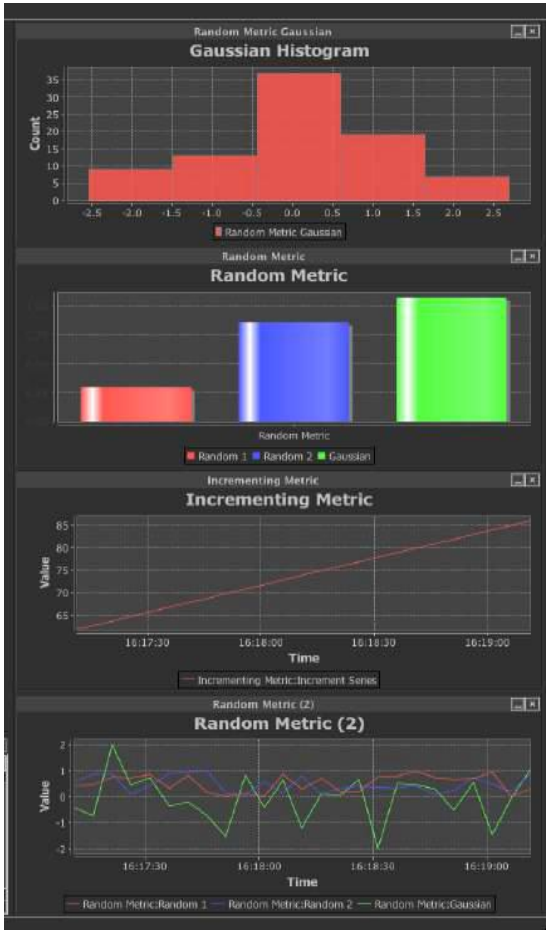
Sample Visualization



Sample Visualization

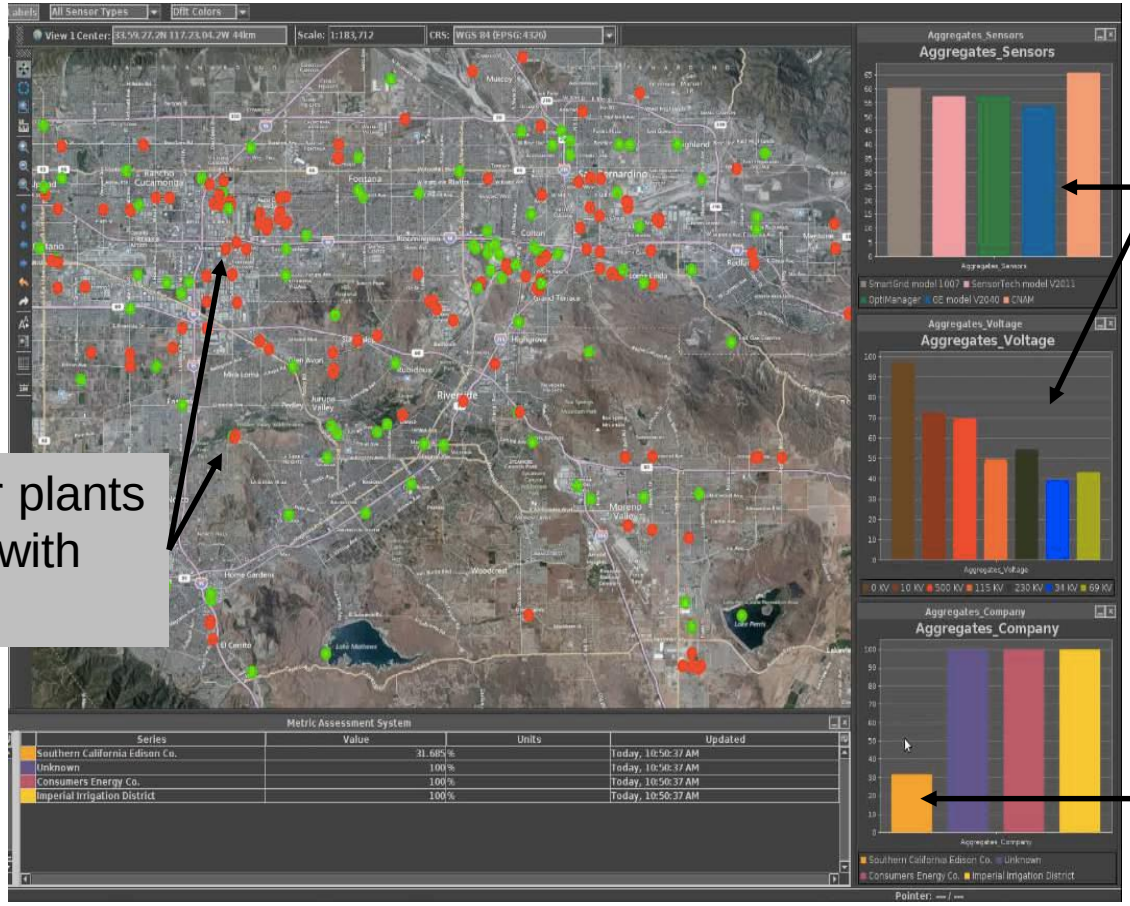
Metric Assessment System (MAS)

- MAS Allows for real time assessment of data
- Support plotting of data in various formats and axis in context with geographic visualization
  - Single node Historical trust of time
  - Multi-node historical trust
  - % of nodes at low trust / high trust
- Bar graph by aggregated value
  - Plant owner
  - Fuel type (nuclear, solar, gas)
  - City (zip code)
  - Equipment (sensor type, generators, controllers)
- Histogram of all sensor nodes



Sample Visualization

Results



Trust evenly distributed among other parameters

Multiple power plants & substations with low trust

Low Trust in Southern California Edison

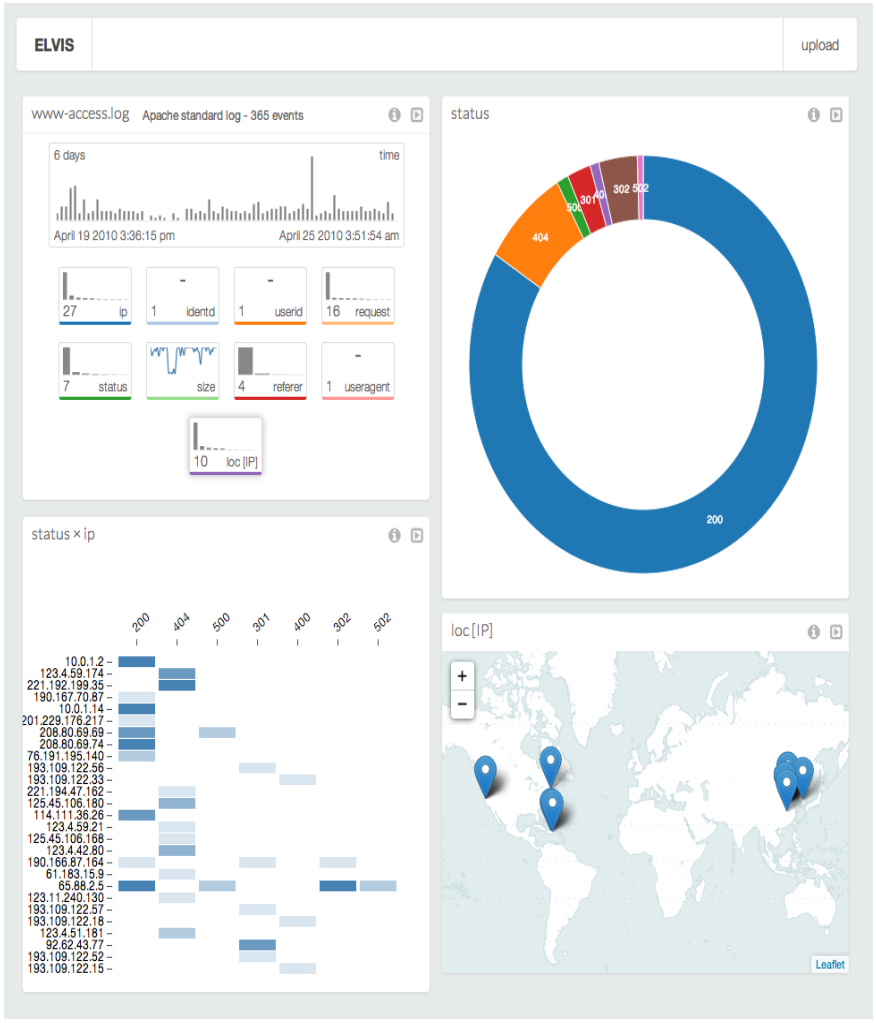
Sample Visualization

ELVIS: Extensible Log VISualization

ELVIS is a security-oriented log visualization tool that allows security experts to visually explore numerous types of log les through relevant representations. When a log file is loaded into ELVIS, a summary view is displayed. This view is the starting point for exploring the log. The analyst can then choose to explore certain fields or sets of fields from the dataset. To that end, ELVIS selects relevant representations according to the fields chosen by the analyst for display

Sample Visualization

Multiple representations automatically selected by ELVIS based on the fields chose by the user.



Sample Visualization

BGPfuse: Using visual feature fusion for the detection and attribution of BGP anomalies

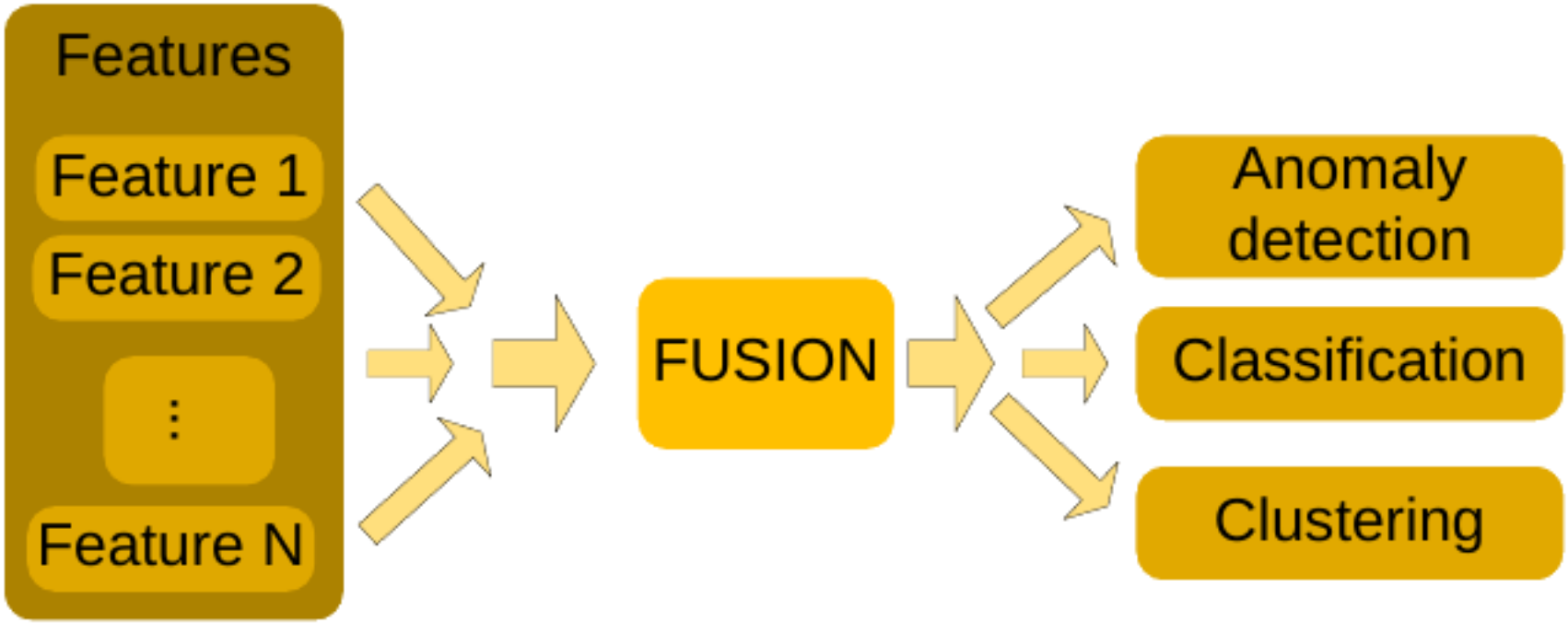


Fig. Feature Fusion procedure

Sample Visualization

Feature fusion background

- Appropriate combination of a set of features for classification, clustering or anomaly detection
- Examples of algorithmic fusion frequently used:
  - Weighted sum
  - Geometric/harmonic/generalized means
  - Support Vector machine (SVM)
  - Neural Networks (NN)
  - Combinations of Multiple classifiers

Sample Visualization

Visual vs. Automated analysis

Visual analysis

+ uses power of human visual system
+ user-guided analysis possible
+ detect interesting features and parameter selections
+ understand results in context
- limited dimensionality
- often only qualitative results

Automated analysis

+ hardly any interaction required (after setup)
+ scales better in many dimensions
+ precise results
- needs precise definition of goals
- result without explanation
- computationally expensive

Sample Visualization

Basic background in BGP

- BGP stands for Border Gateway Protocol
- De facto protocol used today for the exchange of routing information between Autonomous Systems (AS)
- AS is a is a collection of routers under the control of one network operator
- Each AS is assigned a unique number
- Each Internet AS has a hosting country, i.e. majority of its network infrastructure are located.

Sample Visualization

BGP analysis - Definition of Features

- The sequence of the traversed ASes is highly dependent on their geographic presence.
- Analyzing the geographic coherence of the AS-paths could lead to anomaly detection
- Transform the AS-paths of the BGP announcements to Country-Paths:

AS path

Country-path

Sample Visualization

BGP analysis - Definition of Features

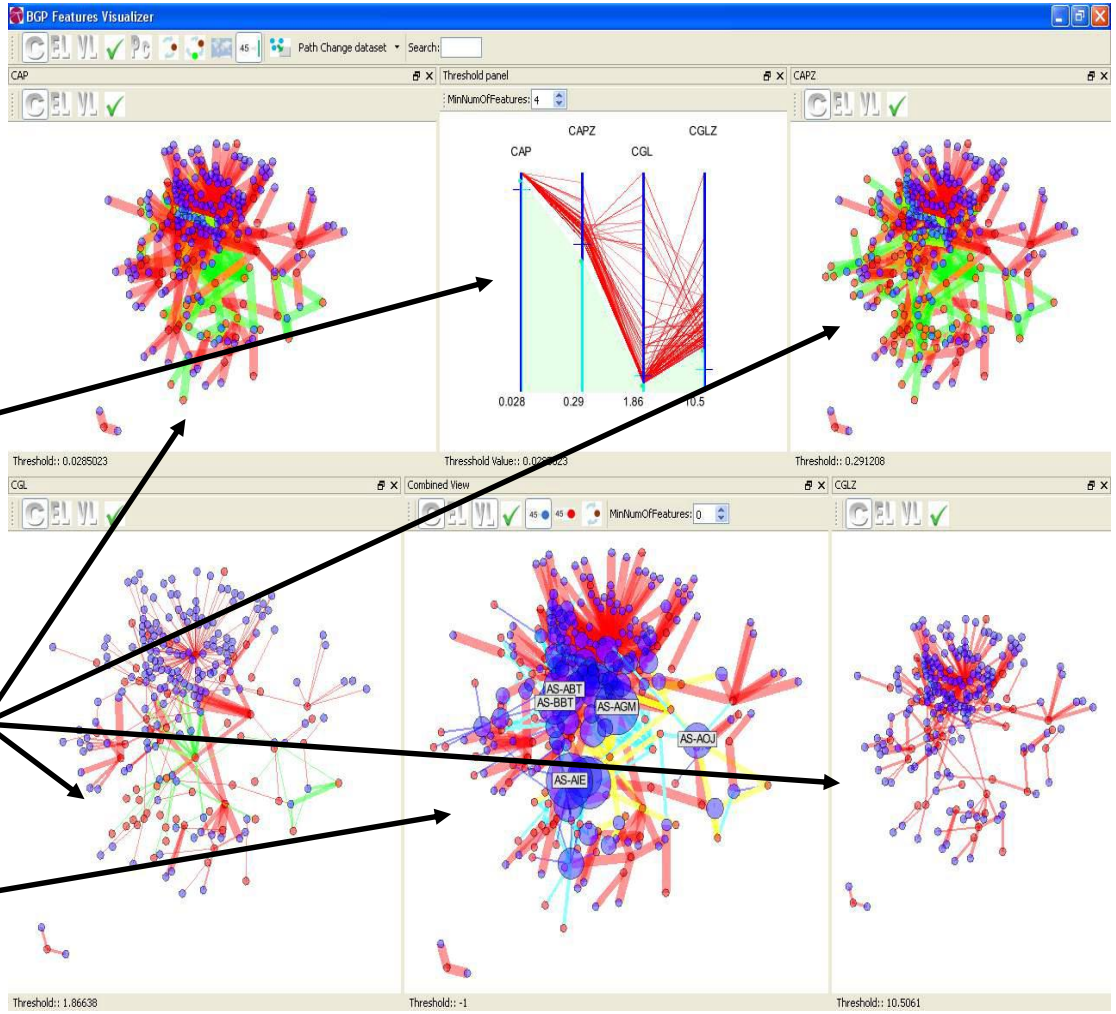
- The values of the overall BGP path-change event are equal to the corresponding values of the **less probable** and **more deviating** Intermediate-Country.
- The most suspicious ASes in the path are the ones that are hosted in this **outlying** Intermediate-Country.
- Thus, the aforementioned features can be eventually **defined on per Intermediate-AS basis, for each Origin-Country** appearing in the BGP announcements (Destination-Country is static)

Sample Visualization

BGPfuse: Visual feature fusion

Three main components:

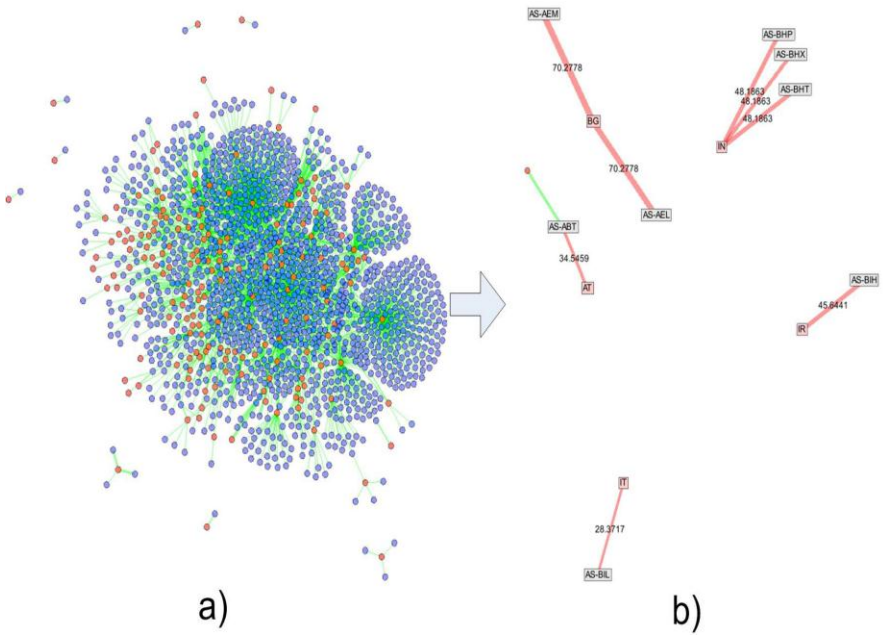
1. Parallel Coordinates User Interface
2. Feature Graph view
3. Combined Graph view



Sample Visualization

Feature Graph view

- Graph based visualization of each feature
- Edge = Path change event
- Red vertices = Origin Countries
- Blue vertices = Intermediate ASes
- Visualization of:
  - Intermediate ASes and source Countries involved in suspicious events
  - relationships that may exist between actors



Sample Visualization

Implementation in real life scenario

Hijacking:

- On August 20, 2011, a Russian telecommunication company (**Victim-AS**), reported to the North American Network Operators Group (NANOG) that five of its **prefixes had been hijacked**.
- **False routes** were injected for the purpose of diverting Internet traffic through the **Hijacking-AS** located in US.

Countermeasure:

- The Victim-AS responded on August 24, by **announcing longer subprefixes** with the correct paths.

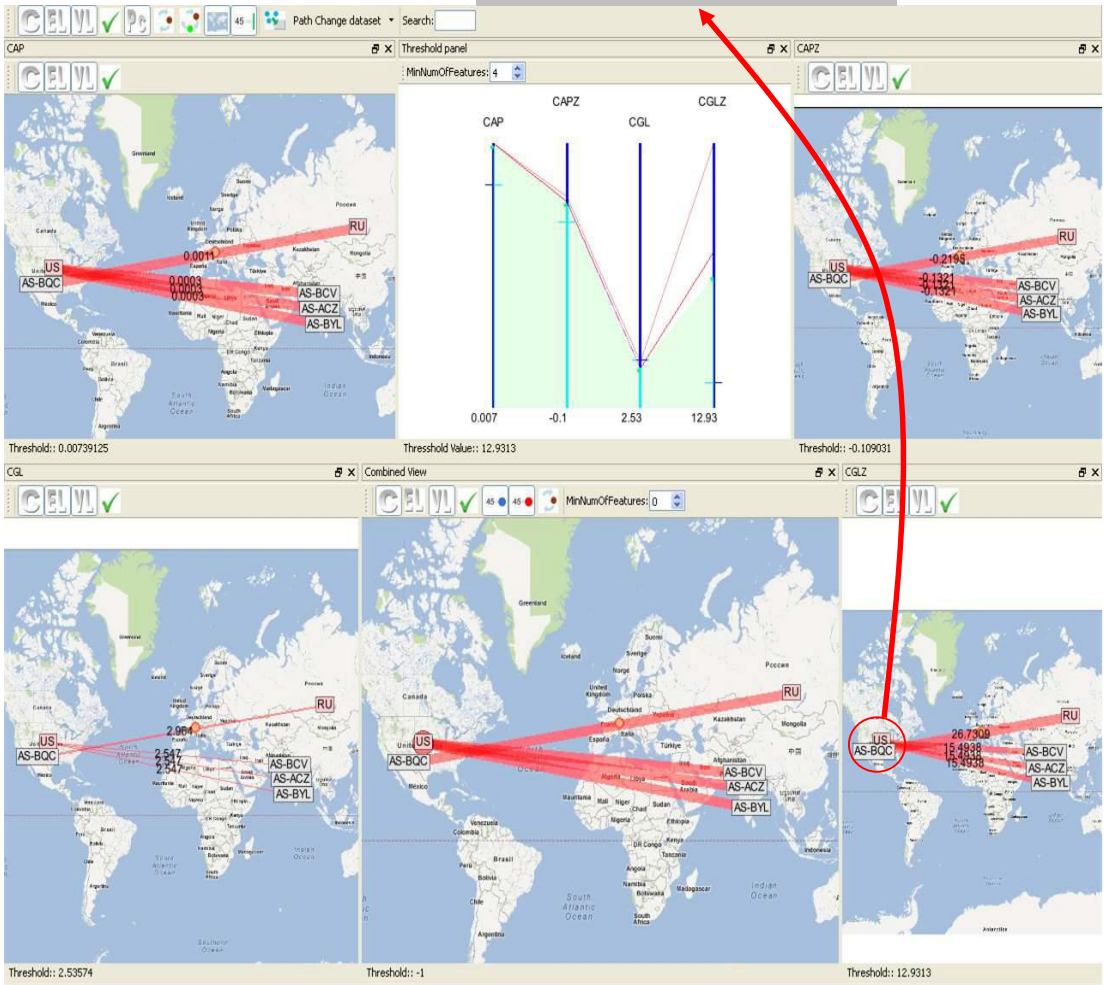
Note: the actual **AS-numbers** on the figures of BGPfuse **are not presented** due to privacy concerns.

Sample Visualization

Visualize the successful BGP path change events (*Wpc*)

- AS-BQC is the Hijacking AS of the aforementioned event
- Hijacking an AS located in Russia

AS-BQC has very high CGLZ score



Sample Visualization

Security Visualization: Key Challenges