DIAL
Digital access to libraries

"A Survey on Information Visualization for Network and Service Management"

Guimaraes, Vinicius Tavares ; Freitas, Carla Maria Dal Sasso ; Sadre, Ramin ; Rockenbach Tarouco, Liane Margarida ; Zambenedetti Granville, Lisandro

Abstract

Network and service management encompasses a set of activities, methods, procedures, and tools whose ultimate goal is to guarantee the proper functioning of a networked system. Computational tools are essential to help network administrators in their daily tasks, and information visualization techniques are of great value in such context. In essence, information visualization techniques associated to visual analytics aim at facilitating the tasks of network administrators in the process of monitoring and maintaining the network health. This paper surveys the use of information visualization techniques as a tool to support the network and service management process. Through a Systematic Literature Review (SLR), we provide a historical overview and discuss the current state of the art in the field. We present a classification of 285 articles and papers from 1985 to 2013, according to an information visualization taxonomy as well as a network and service management taxonomy. Finally, we...

Document type : *Article de périodique (Journal article)*

Référence bibliographique

Guimaraes, Vinicius Tavares ; Freitas, Carla Maria Dal Sasso ; Sadre, Ramin ; Rockenbach Tarouco, Liane Margarida ; Zambenedetti Granville, Lisandro. *A Survey on Information Visualization for Network and Service Management.* In: *IEEE Communications Surveys & Tutorials*, (24 Juli 2015)

DOI : 10.1109/COMST.2015.2450538

Available at:
http://hdl.handle.net/2078.1/171851

[Downloaded 2019/04/19 at 00:33:00]

A Survey on Information Visualization for Network and Service Management

Vinícius Tavares Guimarães [1], Carla Maria Dal Sasso Freitas [2], Ramin Sadre [3], Liane Margarida Rockenbach Tarouco [2], and Lisandro Zambenedetti Granville [2]

[1] Sul-Rio-Grandense Federal Institute of Education and Federal University of Rio Grande do Sul (UFRGS), Brazil
[2] Federal University of Rio Grande do Sul (UFRGS), Brazil
[3] Université catholique de Louvain, Belgium

This is a personal version of the paper. Please only cite the accepted version, published in:

A Survey on Information Visualization for Network and Service Management
Guimaraes, V.T.; Dal Sasso Freitas, C.M.; Sadre, R.; Tarouco, L.M., Granville, L.Z.
IEEE Communications Surveys & Tutorials, 2015
http://dx.doi.org/10.1109/COMST.2015.2450538

PREPRINT

***Abstract*—Network and service management encompasses a set of activities, methods, procedures, and tools whose ultimate goal is to guarantee the proper functioning of a networked system. Computational tools are essential to help network administrators in their daily tasks, and information visualization techniques are of great value in such context. In essence, information visualization techniques associated to visual analytics aim at facilitating the tasks of network administrators in the process of monitoring and maintaining the network health. This paper surveys the use of information visualization techniques as a tool to support the network and service management process. Through a Systematic Literature Review (SLR), we provide a historical overview and discuss the current state of the art in the field. We present a classification of 285 articles and papers from 1985 to 2013, according to an information visualization taxonomy as well as a network and service management taxonomy. Finally, we point out future research directions and opportunities regarding the use of information visualization in network and service management.**

***Index Terms*—Network Management, Service Management, Information Visualization.**

I. Introduction

NETWORK and service management is accomplished through the employment of a set of tools that help network administrators to perform the diverse tasks required in each stage of the management process. Such tools enable network administrators, for example, to retrieve management information from remote devices, to analyze the collected information, and to take decisions to fix or optimize the network by reconfiguring not well-tuned devices. Some of these tools are quite mature and widely deployed, such as the Simple Network Management Protocol (SNMP) [1], frequently referred to as the *de facto* management protocol for TCP/IP networks. Other tools, however, still require improvements to decrease the complexity of the management process effectively.

In the analysis of management data, the network administrator looks for unusual network conditions that require his/her reaction to lead the managed infrastructure back to a consistent state. Although network analysis can be almost fully automated, that is only possible after having the main network scenarios properly identified by human reasoning. Thus, human interpretation of the network conditions plays a key role, and tools to aid network administrators in this process also become essential. Information visualization is one of these tools that allows network administrators to understand the behavior of the managed network (*e.g.*, to identify usual or unusual patterns, to analyze performance measurements, and to react in case of identified anomalies).

Throughout the years, several authors have addressed information visualization techniques as a tool to help in the network and service management activities. For instance, Becker *et al.* [2] presented the first relevant work in this context, still in the 90s. However, according to Pras *et al.* [3], the available information visualization techniques and interfaces for network administrators are not satisfying for the following reasons:

- Traditional topological views do not scale well with the increasing size and complexity of networks. This problem becomes even worse when attempting to visualize multiple or all of the involved layers.
- Visualization of measurement datasets and basic statistics is often static, with very limited support for interactive exploration (*e.g.*, by applying filters, zooming etc.).
- Traffic visualizations typically focus on the visualization of high-volume traffic components. However, certain tasks, especially in the context of security, require to extract and highlight unusual, sometimes small-volume traffic patterns.
- Many existing tools are designed for offline analysis and

visualization. However, there is a growing need for online or close to real-time visualizations to reduce detection and reaction times.

The focus of research on information visualization techniques and network and service management is an important point. Most of the current works focus on security management. Indeed, contributions in this field are more evident from 2004 when has occurred the first edition of the Visualization for Cyber Security (VizSec) forum [4]. Efforts by the security community have allowed a more comprehensive understanding of the use of information visualization techniques to deal with security issues. Shivari *et al.* [5], for example, presented a thorough study on visualization systems for network security, where the visualization systems are grouped by use-case classes and classified by the employed visualization techniques.

Although we have found many articles and papers adopting information visualization for security management, it is only one of the areas of network and service management. Thus, several other important topics are not covered or have few investigations carried out so far. For instance, there is still a clear lack of advanced visualizations that could cope with more modern networked systems (*e.g.*, Software-Defined Networking - SDN).

In this paper, we survey the literature on information visualization techniques as a tool to support network and service management tasks. To conduct our study, we carried out a Systematic Literature Review (SLR) [6]. Our contribution is three-fold: (*i)* we draw a historical overview of the research on information visualization for network and service management based on 285 articles and papers published from 1985 to 2013; (*ii)* we classify each article/paper according to both a network and service management taxonomy and an information visualization taxonomy, highlighting how each taxonomy is filled by the surveyed work; and (*iii)* we identify and discuss future research opportunities and challenges in the field.To the best of our knowledge, this is the first work to survey the literature on information visualization and network and service management in a large (*i.e.*, number of articles and papers) and comprehensive (*i.e.*, several topics on network and service management) way.

This survey targets a wide audience of experts in both fields of network and service management and information visualization. In Section II, we briefly review the background on network and service management and information visualization. We believe that Section II is helpful to readers that are unfamiliar with such areas. In Section III, we present the methodology adopted in this survey. In Section IV, we present a historical overview, the state of the art, and other initiatives in the field. In Section V, we introduce the taxonomies we adopted for each area (*i.e.*, information visualization and network and service management) as well as the results and discussions related to the classification of the surveyed articles and papers. In Section VI, we discuss the key future research directions, highlighting the investigation opportunities observed during our survey. Finally, in Section VII, we draw our final comments.

II. Background

In this section, we review some fundamentals of network and service management and information visualization. We start reviewing basics of network and service management and, afterward, address information visualization concepts. The purpose is to aid readers who are unfamiliar with such areas; experts can then skip this section.

A. Network and Service Management

To emphasize the importance of network and service management, we use the Formula 1 world championship as a metaphor. The basic assumption is that a great driver needs a competitive car to be a world champion. So, what should be done to get a competitive race car? Obviously, this question has some straightforward answers. For example, building up a competitive race car requires, minimally, a well-developed design, a qualified engineers team, and high-quality gears (such as mechanical and electrical equipment). Nevertheless, these requirements are not enough to ensure the car performance throughout the season. If this assumption were true, once a race car have been built and tested, no more improvements would be needed. Instead, Formula 1 teams normally have a huge budget to invest in computational capabilities such as monitoring performance by telemetry, and software tools for prediction and trend analysis. These are typical examples of resources that help teams to maintain the race car efficient and competitive.

Based on that metaphor, it is possible to outline a similar context for networked systems. Certainly, a significant portion of the performance of a networked system is obtained by proper design, an expert team of engineers and network administrators, infrastructure, and suitable hardware and software. However, this is only an important phase in the process, as well as the race car designing and building. Network operators and engineers teams should be enabled, for example, to monitor, measure, and analyze the networked ecosystem to keep it healthy as long as possible. Thus, the fundamentals and practices defined by the network and service management discipline are mandatory.

Efforts on network management standardization were started by the Open Systems Interconnection (OSI), within the International Organization for Standardization (ISO) in conjunction with the Telecommunication Standardization Sector of the International Telecommunications Union (ITU-T). In this context, we highlight the widely known OSI Management Framework [7] and OSI Systems Management Overview (SMO) [8], which divided management functions into five functional areas. These areas are commonly denoted by the term “FCAPS”, an acronym for **F**ault, **C**onfiguration, **A**ccounting, **P**erformance, and **S**ecurity management.

In general, the standardization of the OSI reference model is the basis for other network management definitions. Here, we introduce two definitions of network and service management. Network management is the act of initializing, monitoring, and modifying the operation of the primary network functions, where primary network functions are those functions that directly support user requirements [9]. Secondly, network

PREPRINT

management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems [10].

Nowadays, services and applications that comprise business processes are supported by networked systems. Typical examples are Electronic Data Interchange (EDI) systems. Enterprises may incur extreme losses (*e.g.*, billing, productivity, image degradation) because of interruption or degradation of their EDI system. From this example, it is possible to understand how sensitive business processes are in the event of disruption or instability in the network and service infrastructure. Thus, the network and service management is no longer a relevant issue only for network operators and engineers teams. The concerns about an efficient network and service management became part of the business goals since it is one of the pillars to ensure competitive advantages in the market.

Based on such context, computational tools are essential to perform network and service management tasks. In essence, they are means to support the management workflow as a whole. In a general way, the management workflow is based on three main axes: (*i*) monitoring, (*ii*) analyzing, (*iii*) and acting. The monitoring process is characterized by obtaining raw data from the managed environment (*e.g.*, configuration and performance data). In turn, the analysis process is based on the interpretation and reasoning over the collected data. Finally, in the acting phase, actions (*e.g.*, reaction to a failure event, reconfiguration, optimization) are performed. Fig. 1 depicts a generic network and service management workflow based on these three main axes.

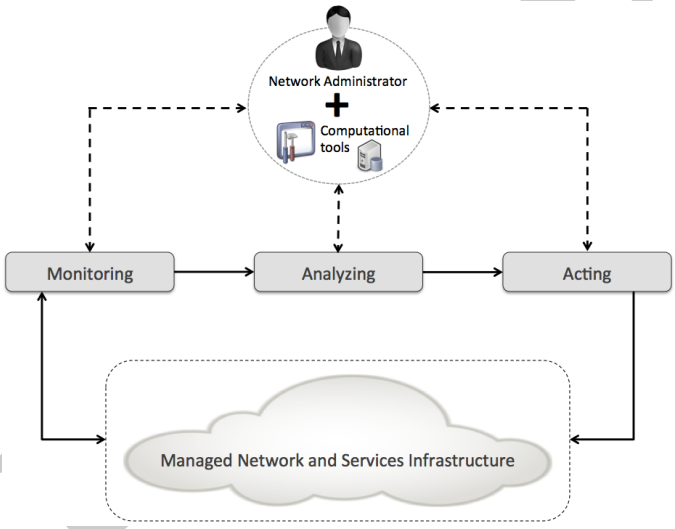


Figure 1. A generic network and service management workflow based on three main axes: monitoring, analyzing, and acting. Two roles are depicted at the top: the network administrator and the computational tools.

Over the years, several computational tools have been developed to support the management activities. In fact, most of them are quite mature and widely employed in production environments. On the other hand, several gaps and opportunities remain. The use of information visualization techniques over management datasets as a tool to help human operators in their analysis and reasoning is an example.

B. Information Visualization

We start with quoting Shneiderman's statement [11]: *"a picture is often cited to be worth a thousand words and, for some (but not all) tasks, it is clear that a visual presentation - such as a map or photograph - is dramatically easier to use than is a textual description or a spoken report*". Actually, visual representations are very efficient even in ordinary daily activities. The sign boards on pavements, streets, and subways are the most simple examples. Another good example is the maps that explain the railway lines of subways, which are likely to be understood by people not speaking the country's language.

The field of information visualization forms a whole research area in computer science. This discipline was formally recognized in the late 80's, coincidentally close to the time when the network and service management community started to grow. Card *et al.* [12] define information visualization as the use of computer-supported, interactive, visual representations of **abstract** data to amplify cognition. Ward *et al.* [13] define visualization as the process of representing data, information, and knowledge in a visual form to support the tasks of exploration, confirmation, presentation, and understanding.

The word "abstract" is highlighted in bold in the previous paragraph because it plays a major role in the definition of information visualization. Basically, the visualization field has been subdivided into two main subfields: scientific visualization and information visualization. While scientific visualization deals with scientific data, information visualization deals with abstract data.

Most of the time one distinguishes the areas based on the spatial domain of scientific visualization applications as opposed to a non-spatial (*e.g.*, a set of elements) domain of information visualization applications. According to Tory and Möller [14]:

- Scientific visualization is typically categorized by the dimensionality of the data values (number of independent variables), and whether the data is scalar, vector, tensor, or multivariate (having more than one dependent variable).
- Information visualization can be similarly organized by data type. Common categories are multi-dimensional databases (often containing more than three dimensions), text, graphs, and trees.

In this article, we focus on information visualization since the nature of management datasets are aligned with information visualization assumptions. Datasets such as texts (*e.g.*, logs or configuration settings) and graphs (*e.g.*, logical connections among IP addresses) are typical examples of data handled in network and service management tasks; they are clearly defined over a non-spatial domain and can be classified as abstract data.

Fig. 2 shows the classical reference model of visualization proposed by Card *et al.* [12]. This reference model outlines the main components present either in the use of a technique or the development of a new technique. In the first step, raw data (*i.e.*, collected or synthesized) is represented as data tables. In this phase, the raw data may be processed by other methods (*e.g.*, data mining techniques) to generate

the desired information. Next, information (*i.e.*, data tables) is manipulated and then transformed into one or more visual representations. Finally, the end-user manipulates and interacts with the visual representation in a view.

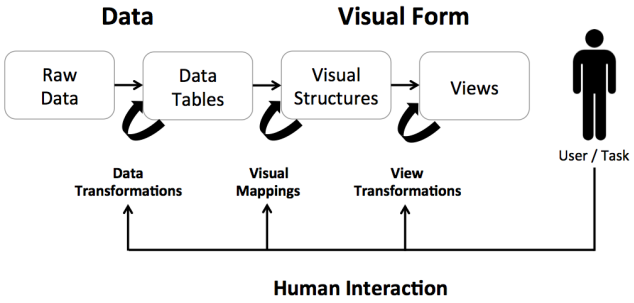


Figure 2. The reference model for visualization proposed by Card *et al.* [12].

From the visualization reference model, we go back to Fig. 1. Datasets obtained from the network monitoring process are input to the reference model, *i.e.*, the raw data. Users (in this case, network administrators) interact with the data representations to perform tasks and to browse the management information, by manipulating visual structures in a view. In summary, the entire process consolidates information visualization as a proper and important computational tool to support network and service management tasks.

III. Methodology

We have adopted the concepts of Systematic Literature Review (SLR) [6] as a means to structure and organize our research. As a first step, we defined an *ad-hoc* review protocol. Fig. 3 depicts the review protocol, and the following subsections describe each step of it.

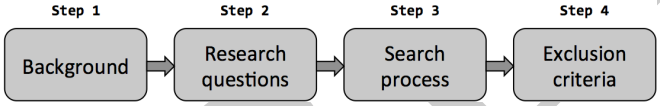


Figure 3. Review protocol of SLR.

A. Background

In the context of an SLR, background refers to the rationale for our survey. As previously mentioned, to the best of our knowledge, no other survey has shown the big picture of literature regarding the historical perspective and the state of the art in network and service management and information visualization in a comprehensive way. For this reason, we understand that there is an important gap in the current literature.

B. Research questions

The research questions are those that this survey intends to answer. Our questions are:

RQ1: What are the most explored topics on network and service management regarding the use of information visualization?

RQ2: What are the most employed information visualization techniques and tasks/interactions for network and service management?

RQ3: What related insights are revealed by the proposed classification? For example, what are the most widely used information visualization techniques for a given network and service management topic?

RQ4: What are the future research directions identified from this survey?

C. Search process

First, as shown in Fig. 4, we defined the keywords and the academic search engines as follows:

1) **Keywords:** "visualization AND network management", "network AND service AND visualization", "network visualization", "network AND visual", and "visualization AND security". The use of the "security" keyword was based on a previous analysis, in which a large number of works was identified in this network and service management subtopic (this issue will be addressed in the following sections).
2) **Academic search engines:** Google Scholar, Microsoft Academic Search, Scopus, IEEExplore Digital Library, and ACM Digital Library.

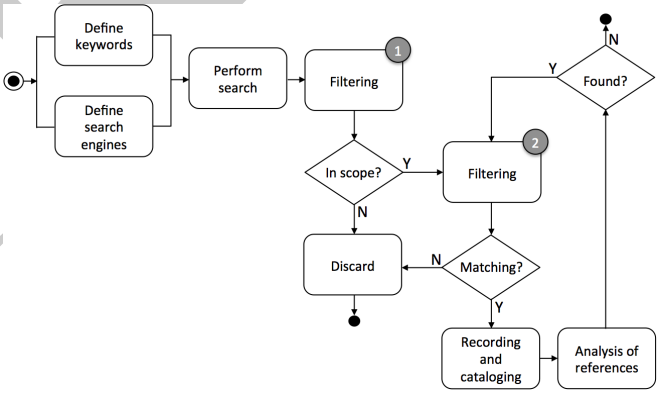


Figure 4. The flowchart depicts the search process defined as the Step 3 in Fig. 3.

After defining keywords and academic search engines, the search itself was performed. Hereinafter, in order to better explain each step after "Perform search" (see Fig. 4), we use an example where the Google Scholar is the search engine and "visualization AND network management" is the query. Basically, the first step of filtering (after "Perform search" in Fig. 4) refers to the analysis of the search results (*e.g.*, title and brief description) to identify articles and papers that are in or out of scope. By using the example, Google Scholar returned around 578,000 results (we do not differentiate patents and citations). We sorted such results by relevance and analyzed the first three hundred of them. We decided to analyze the first three hundred because we observed that, after the first hundred, the results started to be unrelated to the research goal.

Among the first ten results in our example, we list here as examples the work of Corchado and Herrero "Neural visualization of network traffic data for intrusion detection" [15],

PREPRINT

Le Grand and Soto "Information management-Topic maps visualization" [16], and Itoh *et al.* "Hierarchical visualization of network intrusion detection data" [17]. These articles/papers were selected for the second step of filtering. On the other hand, also among the first ten results, we found the title "Modes of Network Governance: Structure, Management, and Effectiveness" [18] which was directly discarded because it is out of scope.

In the second step of filtering, we analyzed the abstract and keywords of each paper that was selected by the first filtering. At this point, if the article/paper somehow matches with the research goal, it is recorded and cataloged. Otherwise, the article/paper is discarded. For each recorded and cataloged article/paper, its references were analyzed to seek for other relevant works in the field. In this stage, we verified the title and the publication venue of each reference. If the title and the publication venue of the reference were promising, the second step of filtering was performed over the article/paper selected from the reference. In essence, it was an iterative process, *i.e.*, for each new article/paper its references were also analyzed.

Taking into account the example mentioned above, [15] and [17] are examples of articles/papers that match with the research goal. Thus, they are stored and cataloged, and their references are verified. In the analysis of the references of [15], for example, we found the work of Koike *et al.* "Visualizing cyber attacks using IP matrix" [19]. On the other hand, [16] is an example of a work that was discarded after the analysis of the abstract and keywords (*i.e.*, the second step of filtering).

Once finished the search process, a set of 374 articles and papers remained selected. These publications are from a time interval ranging from 1985 to 2013.

D. Exclusion criteria

After recording and cataloging those 374 articles and papers, we performed a deeper analysis where we verified introduction, proposal overview, results, and conclusions of each one. This step aimed to identify articles and papers that match or not the five exclusion criteria defined for this research. The five exclusion criteria are defined as follows:

1) **Gray area for network and service management:** articles and papers that in our understanding are not clearly in the network and service management scope, *i.e.*, they could not be a consensus in the community. For instance, Veras *et al.* in "Visualizing Semantics in Passwords: The Role of Dates" [20] introduced an investigation into the semantic patterns underlying user choice in passwords. It is a very interesting work but falls under this criterion.
2) **Gray area for information visualization:** articles and papers that in our understanding do not present the used information visualization techniques clearly. For instance, the work proposed by Dinh-Duc *et al.* "Nviz - A General Purpose Visualization tool for Wireless Sensor Networks" [21].
3) **Surveys/Evaluation**: articles and papers that introduce a research addressing some topic in the field. For instance, Goodall in "Visualization is Better! A Comparative Evaluation" [22] introduced an interesting comparative evaluation of a visualization application and a traditional interface for analyzing network packet captures. Shivari *et al.* "A Survey of Visualization Systems for Network Security" [5] introduced a valuable survey of Visualization Systems for Network Security.
4) **Same as or related to**: articles and papers that were published in more than one venue (*e.g.*, journal, conference, etc.) or articles and papers that are improvements/variations of previous work. For instance, the works presented in "An Implementation of Visualization System for Visualizing Network Topology and Packet Flow in Mobile Ad-hoc Networks" [23], "MANET-Viewer: A Visualization System for Mobile Ad-hoc Networks" [24], "MANET-Viewer II: A Visualization System for Visualizing Packet Flow in Mobile Ad-hoc Networks" [25], and "MANET Viewer III: 3D Visualization System for Mobile Ad-hoc Networks" [26]. In these cases, we kept only the most recent work (*i.e.*, [26] in our example).
5) **Withdraw**: articles and papers that, although having passed in the first and second step of filtering, after a deeper analysis we concluded they are out of scope for this survey. For example, the work of Fang *et al.* "Automated Tracing and Visualization of Software Security Structure and Properties" [27].

Based on these five criteria, 89 articles and papers were left out of the survey. Thus, we selected 285 articles and papers from the originally 374 recorded and cataloged during the searching steps. These 285 articles were used for the classification described in Section V. Fig. 5 shows the number of surveyed articles and papers per publication year.

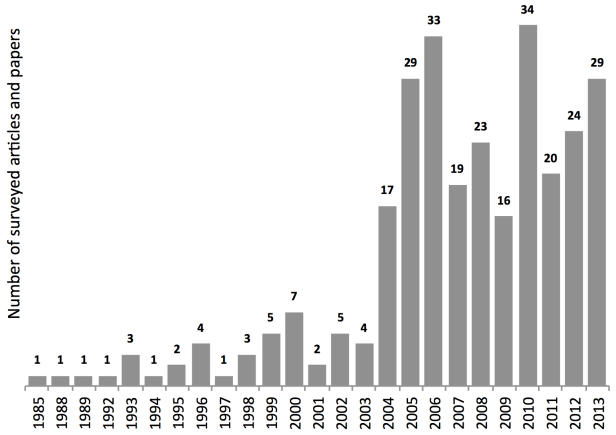


Figure 5. Number of surveyed articles and papers per year of publication.

IV. Literature Survey

In this section, we introduce the literature survey. Section IV-A is the historical overview. We start from articles and papers published in the 80s and 90s, and afterward, we focus on works between 2000 and 2008. In Section IV-B (State of the art), we address articles and papers in a time interval from 2009 to 2013. Both Section IV-A and IV-B are divided into two parts as follows: (*i*) Other fields - works that address other

PREPRINT

topics of network and service management instead of security management (*e.g.*, analysis of routing data [28][29][30] and configuration management [31]), and (*ii*) Security field - works focused on security management. In Section IV-A, this division is used only for the period between 2000 and 2008. In Section IV-B, this division includes the whole period between 2009 and 2013.

In short, the division mentioned above has emerged because publications from 2000s started to have a more evident characterization: a significant increase in efforts that address visualization for security management. Specifically after 2004, the number of publications addressing security issues has an expressive increase since at that year the first edition of VizSec forum has occurred. VizSec focuses on visualization and data mining for computer security, and it started as a workshop. Over the years, the event got bigger and, since 2010, VizSec began to publish proceedings with ACM International Conference Proceeding Series (ACM ICPS).

VizSec has a significant contribution to the field. For instance, we found a total of 33 articles and papers in 2006, where 16 were published in VizSec (*i.e.*, 48.5%). However, this behavior is not only because of VizSec. Articles and papers published in other venues were also focused on security issues. In 2007, for example, only one work did not address security management (*i.e.*, 5.26%). The period between 2009 to 2013 (state of the art) shows the same trend. Among 123 surveyed articles and papers in this time interval, there are 85 (69.11%) addressing security management. In 2009, from 16 surveyed articles and papers, there are only two articles/papers that address other topics of network and service management. Fig. 6 depicts these numbers in the time interval between 2004 and 2013.

Finally, in Section IV-C, we outline other initiatives in the field. In this case, we are interested in efforts that are not necessarily bound to publications of articles and papers. In essence, we focus on research groups, forums, and projects.

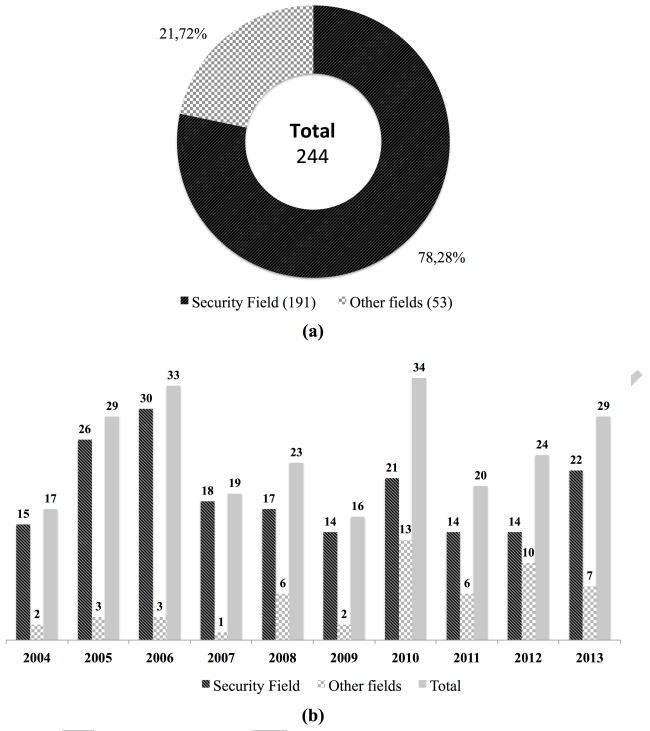


Figure 6. (a) Percentage of articles and papers addressing security and other fields in the time interval ranging from 2004 to 2013; (b) Distribution of articles and papers in the same time interval.

A. Historical overview

We start from the 80s as a symbolic time. At that time, the information visualization and network and service management fields were in their infancy. As previously explained (in Section II), information visualization has its beginnings as an area between the end of the 80s and the beginning of the 90s. At that time, communications networks were in expansion. The Internet Protocol (IP) and concepts related to network and service management were still incipient when compared to the great evolution happening years later with the Internet.

In 1985, Gilbert and Kleinöder [32] introduced the CNMGraf (Communications Network Management Graphics Facility), an architecture for network management. They focused on how to efficiently manage large quantities of management data and how to view this data at a user-defined level of detail. In that context, they proposed an algorithm to produce the network layout by using a graph representation (*i.e.*, node-link). Three years later (1988), Kar *et al.* [33] introduced an improved algorithm for the CNMgraph representation, highlighting that the new approach would spend less time to produce and display the network layout. In 1989, Anderson and Linebarger [34] also highlighted the volume of data that should be examined as a challenge for network management. They took a step further by proposing a display program with capabilities such as digraph representation (*i.e.*, node-link representation of the network), color modulation (*i.e.*, a color range to represent load to capacity ratio), hierarchical structure of the network, and node icons.

The 90s were characterized by relevant contributions from the AT&T Bell Laboratories team. We found that the first manuscript was presented by Becker *et al.* [35], in 1990. In that work, they introduced the first insights that conducted to the development of the SeeNet tool, by describing several dynamic graphical tools. Later, Becker *et al.* [36] described three complementary graphical techniques (linkmap, traffic matrix, and nodemap) to display network data through the SeeNet tool. In 1995, Becker *et al.* [2] described in details the visualization concepts applied in the development of the SeeNet tool and closed the loop of previous works. The work presented by Becker *et al.* [2] is the most cited publication regarding visualization and network and service management. Up to now, this manuscript has 440 citations (according to Google Scholar database). Several visualization techniques were proposed such as link maps (that represents network connections), node maps (that displays nodes by showing a glyph or symbol with characteristic such as size, shape, and color), and matrix display. A set of interactive tools was also presented such as manipulating line length between links, line thickness, symbol size and color, animation speed, zooming,

PREPRINT

and brushing. Additionally, the authors showed two examples of situations where the SeeNet tool was applied: the CICNet packet-switched data network and an email communications network. Fig. 7(a) depicts an overview of SeeNet visualization.

Still on contributions of the AT&T Bell Laboratories team, Cox and Eick [37] introduce a case study of a 3D approach to display the globe surface and arcs that represent connectivity and traffic between fifty countries over the NFSNET/ANSnet backbone. Eick [38] improves previous work [37], using three different strategies: dynamic parameters focusing, positioning and linked filters, and a 3D layout. Abello *et al.* from AT&T Labs - Research [39] described two approaches for large scale network visualization: a project in large-scale graphics and network displays, and an experiment with a novel graphical representation of networks using a hierarchy of 3D surfaces that forms a hierarchical graph surface. Koutsofios *et al.* [40] [41] introduce SWIFT-3D, an integrated data visualization and exploration system created at AT&T Labs also for large scale network analysis. SWIFT-3D employs a set of different visualization techniques such as statistical 2D (line graphs, histograms, etc.), pixel-oriented 2D, and dynamic 3D visualizations. Fig. 7(b) shows an overview of SWIFT-3D visualization.

There were several other efforts in the 90s. Zinky and White [42] describe an environment and a prototype (named as SpyGlass) for visualizing packet traces to simplify troubleshooting protocol implementations. Consens *et al.* [43] [44] introduce the Hy$^+$ system, which provides support for query visualization over management datasets. Basically, they focus on hygraph, an extension of the notion of a traditional graph by incorporating blobs (*e.g.*, the subnet is a blob node since it contains other network nodes) in addition to edges. Interactive features are provided to manipulate hygraphs, such as panning, zooming, and moving. Crutchet *et al.* [45] and Feiner *et al.* [46] describe a system that uses a 3D virtual world as user interface for managing a large Gigabit ATM network. They combine high-performance 3D graphics processors with 3D displays and interaction devices to create a virtual worlds for network management.

Some proposals were developed addressing real-time visualization. Nakai *et al.* [47], from NEC Corporation, present an approach to visualize networks in real-time using a bifocal display technique. Lamm *et al.* [48] propose a real-time approach of visualization to support World Wide Web (WWW) performance analysis. They use a virtual reality framework called Avatar to develop three different display metaphors for performance data: time tunnels, scattercubes, and geographic displays. Parulkar *et al.* [49] introduce a Network Monitoring, Visualization, and Control (NMVC) system that allows network administrators to calibrate and fine-tune network and application parameters in real time. They present a visualization system called View Choreographer, which performs user-specified mappings of network events.

Munzner *et al.* [50] show a case study of visualizing the global topology of the Internet Multicast Backbone exploring 3D concepts to build an interactive map of the Internet Multicast Backbone tunnel structure. To do that, the tunnels are represented as arcs on a globe. The endpoints of the tunnels are drawn at the geographic locations of backbone routers. Oetiker [51] describes the history and operation of the Multi Router Traffic Grapher (MRTG) and the Round Robin Database Tool. Although MRTG provides charts in a standard 2D representation, this tool is still widely used by the network and service management community to monitor Simple Network Management Protocol (SNMP) network devices.

Works on visualization for security field are also found in the 90s. Swing [52], from the National Security Agency (NSA), describes an application called Flodar (short for Flow Radar) that monitors traffic flows. Display modes in this tool are: "platter" (servers are represented by a cylinder and arranged radially around a disc), 3D geographic view (each remote server is mapped to its geographic location), 3D building displays (each server is represented by cylinders at its physical location in the building), and hyperlinks representation (showing a network traffic flowing from a selected server to a set of other buildings). Girardin and Brodbeck [53] describe an experimental system based on unsupervised neural networks and spring layouts to classify automatically network events contained in logs. This work also introduces iconic representation in a grid, where each cell depicts some characteristics of events, and parallel coordinates to understand the correlation among several attributes of an event. Afterward, Girardin [54] introduces an intrusion detection approach and a visualization system based on a colored map. This map is formed by squares within a grid and properties such as foreground color, size, and background color are used to define an event and the characteristics of their attributes.

At this point, we finish the historical overview of the 80s and 90s. As previously mentioned, the interval between 2000 and 2008 is divided into two parts as follows.

*1) **Other fields**:* We start from the employment of information visualization based on routing data, specifically from the Border Gateway Protocol (BGP). Burch and Cheswick [28] and Cheswick *et al.* [55] introduce an approach that uses, among other information, BGP data to draw the Internet graph. The main goal is to outline the size and complexity of the Internet. They use a force-directed method to layout the graph, where each link represents a path, and its color represents a specific network. Teoh *et al.* [29][56] use BGP to develop a visual method to aid in anomaly detection. A quadtree mapping is used to represent the entire space of 32-bit IP address. Attributes such as color, hue, and brightness on the squares are used to determine specific behaviors. Other features such as animation and 3D representation (with rotation, translation and zoom/pan operations) are provided. Au *et al.* [57] show a tool called VLNT (Visualizing Large Network Topologies), which helps network managers to analyze complex routing topologies. They describe an approach for graph layout using BGP routing data.

Colitti *et al.* describe an on-line service (called BGPlay) to visualize the behavior and instabilities of Internet routing at the autonomous system level [30]. They define two types of information to be displayed, namely routing status and routing events, and their requirements, which are based on analysis of BGP protocol features. A graph layout is used, where Autonomous Systems (AS) labeled by their numbers

PREPRINT

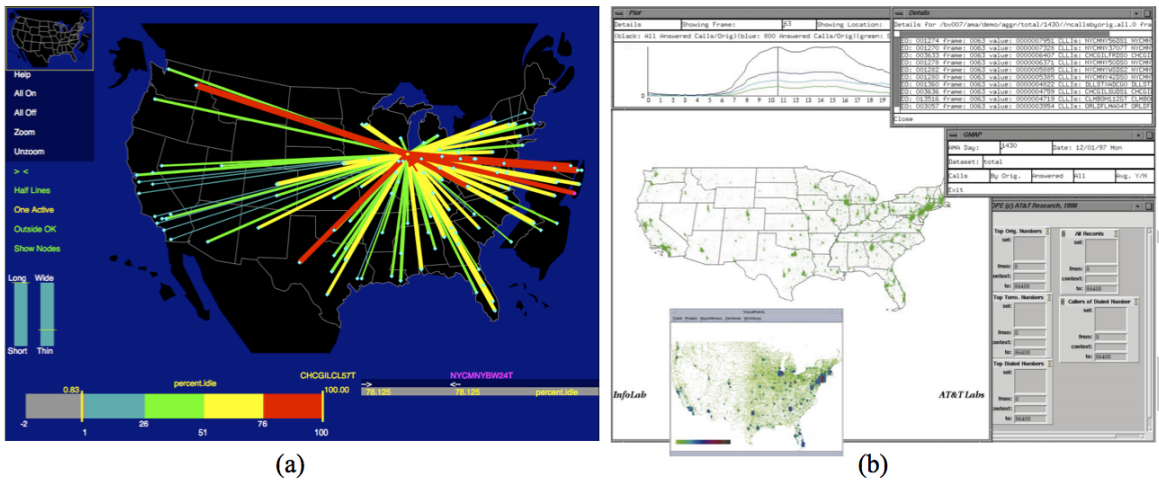


Figure 7. (a) An overview of SeeNet visualization [2]. A node-link representation where nodes are geographically plotted. Thickness and color of links mean the percentage of idle capacity; (b) An overview of SWIFT-3D visualization [40]. A 2D line plot is shown at the top. In the middle, a 3D display where histogram bars are geographically plotted for each location. In a pop-up window, a 2D overview, which depicts each location as a single pixel color.

are nodes and AS-paths are links. This tool also provides animations of routing events. Lad *et al.* [58] propose a tool to visualize Internet routing changes at the global scale (named as Link-Rank). This tool uses messages exchanged from BGP. The visualization approach is also based on a 2D graph layout, where ASs are nodes and connections among ASs are represented by links. Each link has a weight that represents the number of routes using that link. Line style (*e.g*, solid or dashed) and color (*e.g.*, red or green) are used to represent link states. Additionally, this tool provides activity plots that use bars on a horizontal axis time to summarize routing changes in the graph layout.

Visualizations were also explored to analyze network flows. Xiao *et al.* [59] describe an approach to discover patterns in network traffic flow data. Once a pattern is recognized, the analyst may store it in a knowledge database for future analysis. They use a traditional 2D scatterplot to map visual attributes obtained from flow data. Minarik and Dymacek [60] propose a visualization tool based on graphs to display network traffic flow data from NetFlow data records. This tool offers a standard 2D display and provides filtering feature using parameters of pure NetFlow data.

Gubin *et al.* [61] [62] introduce a tool called PingTV, which uses the Ping utility to quantify network metrics such as round-trip time, reachability, packet loss, quiescence, and unpredictability. Based on measurements of these metrics, colored symbols (representing the network status) are plotted as an overlay of a geographical image of the location from the user perspective (*e.g.*, buildings). The proposal of Dimopoulou *et al.* [63] is also focused on network performance metrics, but in the context of QoS-aware IP networks. They introduce a tool called QoS Management Tool (QMTool) to address the heterogeneity, complexity, and dynamic behavior of such networks. The visualization features are 2D charts to display network performance data, node-link representation of the network topology, and icons to represent network elements.

Schönwälder *et al.* [64] introduce a discussion on how to perform large-scale SNMP traffic measurements to develop a better understanding of how it is used in production networks. They use a set of tools to conduct this research, among them we highlight graph layout representation to analyze the SNMP protocol behavior. Although static, these views are helpful to represent, for example, the relationships between SNMP managers and agents as well as to increase the potential analyzes from experts. Following the same topic, Salvador and Granville [65] [66] introduce three visualization techniques to help in SNMP traffic analysis. In the visualization of management network topologies, attributes of nodes are encoded by color and size, and line style and color denote link attributes. MIB-tree visualization represents the Management Information Base (MIB) in a tree view and combines histograms that count the number of messages where each MIB object appears. The last visualization uses bar histograms to visualize SNMP Messages per 1-hour intervals.

Douitsis and Kalogeras [67] introduce the use of web-based technologies such as Scalable Vector Graphics (SVG) markup language and Asynchronous Javascript and XML (AJAX) to develop interactive graphs focused on network management. Valle *et al.* [68] also propose a visualization tool that uses web-based technologies (such as SVG), but to display Wireless Mesh Network (WMN) topologies. The tool plots a mesh network visualization using a graph layout and presenting the link quality over the network topology map.

The proposal of Estrin *et al.* [69] is centered on a network animator called NAM, which provides several features to aid in designing network protocols. NAM provides a network graph where nodes are devices and links are used to connect those devices and to show the packets' animation. Also using animation, Brown *et al.* [70] propose a visualization tool (called Cichlid) to provide insights over network performance data sets. The tool supports 3D bar charts and a vertex-edge graph (also in 3D).

Burns *et al.* [71] propose an approach based on an Ecological Interface Design (EID) to aid in network management through visualization. This proposal uses a polar star diagram to display metrics of network devices in a 3D view. Addition-

PREPRINT

ally, a 3D view draws physical topology and layout of devices within the experimental network (a portion of a university campus network).

Yip *et al.* [72] use the Cooperative Association for Internet Data Analysis (CAIDA) data sets to construct a graph for visualizing the Internet as a network of ASs. An interesting point of this approach refers to the use of a three-dimensional spherical display, where a 3D graph of the AS Internet connections is displayed on the globe.

*2) **Security field**:* We start the review of security field from proposals based on Intrusion Detection Systems (IDS). Erbacher *et al.* introduce an approach to deal with attacks and misuses of computer systems [73][74][75][76][77][78]. They use the Hummer intrusion detection system, which provides data through normal log files. These log files have statistics and other available information about the monitored systems (*e.g.*, hosts, services, etc.). From these log files, they create glyphs as a visual representation of each type of system. These glyphs encode visual attributes such as the number of users, system load, status, and unusual or unexpected activity. Besides to glyphs, lines with specific appearances are used to determine a pre-defined set of activities in the monitored environment. For example, a thick line in a red color represents a port scan. Fig. 8(a) depicts an example of this visualization.

Nyarko *et al.* [81] introduce a tool called Network Intrusion Visualization Application (NIVA) to help in extracting meaningful insights from the masses of network intrusion data. They combine the haptic technology to key principles of information visualization techniques, such as 3D representation, colors, and shapes. Stolze *et al.* [82] use IDS events to propose visual tools to help in security event troubleshooting. The visualization system supports the task of new event triage. Two types of visualization techniques are combined: scatterplots and parallel coordinates.

Abdullah *et al.* [83] introduce the IDS Rainstorm, a tool to deal with alarm data generated by IDS through visualization. They use a 2D representation based on eight vertical axes to represent the IP address range. Horizontal lines are employed to divide class B IP addresses, and IP addresses range of each department (from the environment used in the experiment). Circles representing events are displayed between each vertical axes. Additionally, lines are used to connect circles to vertical axes, outlining the relationship between an event and an IP address. Features such as zooming, glossing and filtering are also provided.

Itoh *et al.* [17] introduce a hierarchical data visualization to deal with incidents originating from IDS. The visualization approach is based on leaf nodes and branch nodes. Leaf nodes are black square icons, and branch nodes are rectangular borders that enclose leaf nodes. They use this approach to group computers according to their IP addresses, where the hierarchy is given by the byte order of the IP address. An experimental implementation uses a 3D display.

Other proposals were developed using network flow data. Yin *et al.* [79] use NetFlows records and visualization features to enhance the ability of human network administrators to detect and investigate anomalous behaviors in the managed network. As a result of this design, they show a tool named VisFlowConnect. Basically, a parallel coordinate system with three axes is used, where each vertical line corresponds to, respectively, the originating domain of network traffic coming into the internal network, the machines on the internal network, and the destination domain of outgoing traffic. The tool also provides animation mechanism and zooming. Fig. 8(b) shows the main display of VisFlowConnect.

Lakkaraju *et al.* [80][84][85][86] propose a tool named NVisionIP that uses NetFlow data to display a visual representation of the network traffic. The main goal of the NPVision is to increase the security analyst's situational awareness employing visual features. They argue that NPVision enables analysts to visualize the current state of the network regarding security threats quickly. NVisionIP provides a central display (named as Galaxy view) that has three main layouts (*i*) a coordinate system, where subnets are listed on X axis and the hosts in each subnet are listed on Y axis, and the color of each host represents characteristics of interest, (*ii*) a cluster view, where hosts are grouped according to their functions, and (*iii*) a treemap view, where hosts are represented by rectangles, and the size of the rectangle reflects the characteristic of interest (*i.e.*, a large rectangle represents a more important characteristic of interest). Additionally, this tool provides, for example, 2D bar charts with detailed information on single hosts and animation. Fig. 8(c) depicts the main display of NVisionIP.

Fischer *et al.* [87] use NetFlow records with an IDS to enable efficient exploration of suspicious activity. As a result, they describe a tool named NFlowVis. This tool maps the monitored network to a treemap visualization in the center of the display and arranges the previously selected attackers at the borders. Fig. 9 shows an example of visualization on NFlowVis.

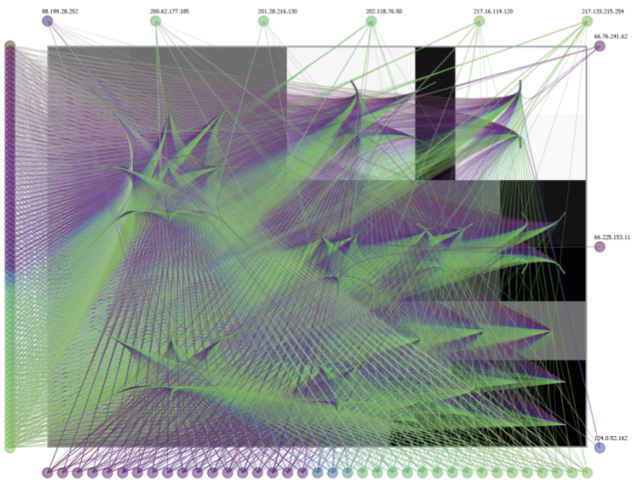


Figure 9. A case study of a massive distributed SSH attack originating from a Botnet using NFlowVis [87].

Phan *et al.* [88] describe the system Isis that uses network flow data to aid skilled analysts in the investigation of intrusions. They developed a standard 2D display containing a timeline. In this timeline, time is mapped left-to-right along the X-axis, and the Y-axis represents the amount of traffic to and

PREPRINT

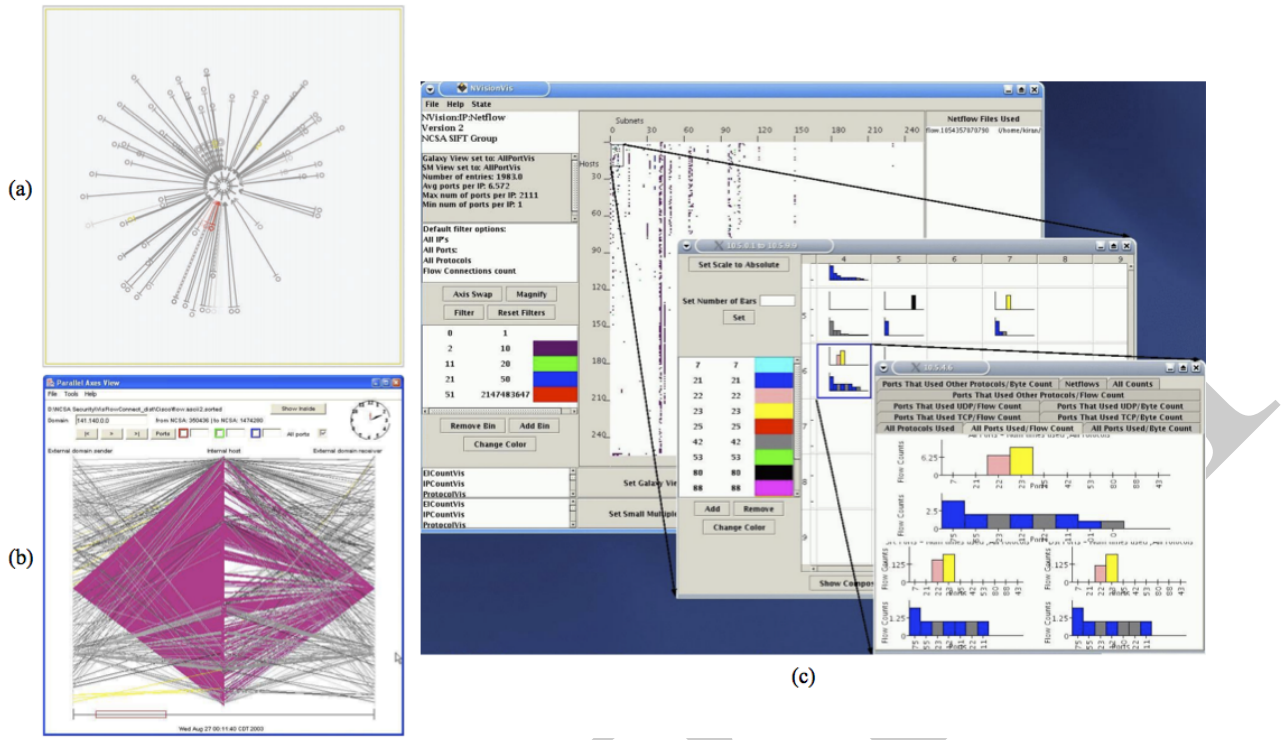


Figure 8. (a) Visual representation of network and system activity proposed by Erbacher [73]; (b) The main display of VisFlowConnect [79]; (c) Three NVisionIP [80] views: galaxy view (2D scatterplot), small multiple view, and machine view.

from a desired IP address. The tool also provides interactions such as brush and details on demand.

Some investigations were conducted aiming at network attack graphs. Noel and Jajodia [89][90] explore this topic proposing a framework for managing network attack graph complexity through interactive visualization. They propose techniques to improve the graph representation of a network attack graph. Moreover, glyphs and colors to represent nodes and exploit set are used. Later, O'Hare *et al.* [91] describe several visualization improvements for this proposal.

Williams *et al.* [92][93] introduce a visual tool to provide a simplified and more intuitive understanding in the attack graph analysis. They merged a treemap visualization with a node-link graph layout. For example, nodes in the same link are grouped together into a rectangular area that typically represents all hosts in a subnet. Lines connecting nodes are analogous to a link in graph layout. Grouping, color, and size are examples of node attributes. They also use a graph layout to represent the attack graph, where icons represent nodes.

Visualizations to support network administrators to assess network policies are explored by Bertini *et al.* [94]. They introduce a visualization tool called SpiralView. This tool uses a spiral to represent the evolution of alarms in time. All generated alarms are displayed starting from the older alarms in the center up to the newer ones in the outer ring. Color is used to represent alarm type, and size represents the alarm severity. The system also provides interactive bar charts to display other alarm attributes (*e.g.*, alarm category) and interactive zooming.

Xu *et al.* [95] also show a visualization-based policy analysis framework that helps human operators to identify policy violations. This framework is based on policies defined in Security-Enhanced Linux (SELinux) configurations. Visualization features are provided by matrix-based visualization layouts and graph layouts. Additionally, graph nodes are represented by different shapes (*e.g.*, circle or rectangle) and links by different colored lines.

Takada and Koike introduce two visualization proposals for browsing and inspecting computer log files. In the first one [96], they present a tool called MieLog that uses the standard 2D display to inspect log messages. In the second [97], they propose a system called Tudumi. This tool employs an approach based on concentric disks in 3D space, where specific icons represent hosts and users, and line types mean different access methods.

McPherson *et al.* [98] introduce a tool called PortVis (also described by Muelder *et al.* [99]). This tool aims at controlling the activity on TCP ports to support security management. The main visualization is based on a dot matrix (256x256) that represents the 65,536 ports. Each point corresponds to a particular port, and it is painted with a color according to the number of sessions on the port. Moreover, the tool provides some additional features such as a timeline, a histogram, and a gradient editor.

Goodall *et al.* [100][101] introduce the Time-based Network traffic Visualizer (TNV), a tool for aiding the packet-level analysis in intrusion detection. The main visual component of TNV is based on a matrix display. Time is displayed on the X-axis, and all host IP addresses are displayed on the Y axis. For each time interval, the number of packets of a host is

PREPRINT

encoded as a colored box in the respective host row. Network links between hosts within a single time period are plotted in a matrix view to providing more information about the nature of the data. Features such as zooming and details on demand are also provided.

Foresti *et al.* [102][103] introduce a tool called VisAlert. The goal of this tool is to use log and alert files to exhibit an enhanced visualization in order to increase operator's situational awareness about network activities and security issues. They use the W^3 (when, where, and what) premise to visually correlate multiple alerts. Fig. 10 shows a VisAlert visualization.

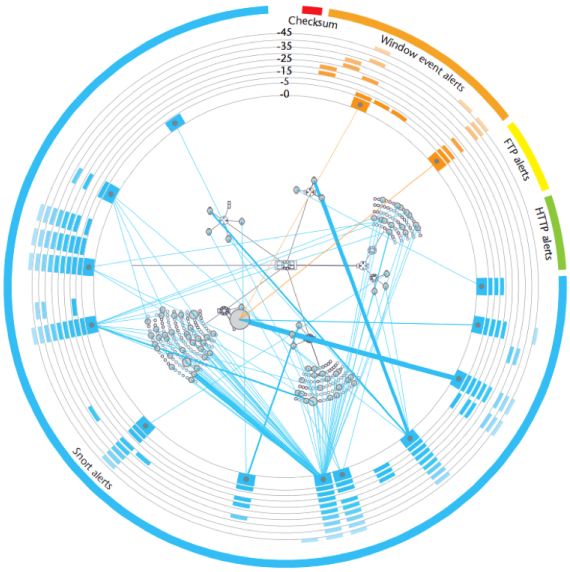


Figure 10. VisAlert visualization [102]. In the center of the circle is a graph layout of the network. The circle's radial sections moving from most recent (closest to the topology map) to the least recent. The outside circular element determines the alert type.

Arvanitis *et al.* [104] propose a procedure called Logical Network Abridgement (LNA), based on Resilient Recursive Routing (R^3) protocol, to determine an end-to-end resilient path and to provide performance measures regarding the network health. They propose a 3D graph layout to show network's resiliency through the LNA procedure.

Mansmann *et al.* [105] introduce an approach called Hierarchical Network Maps (HNMaps) which is based on treemap visualization concepts. They demonstrate the feasibility of their approach by comparing with other related ones. Four case studies in network and service management using HNMaps are shown: resource location planning, monitoring large-scale traffic changes, botnet spread propagation, and expert knowledge.

Wang and Lu [106] propose an interactive visualization of wormholes, to monitor and detect such attacks in large-scale wireless networks in real time. The main visualization depicts the wireless network topology in a 3D graph layout. Nodes with wormhole indicator are highlighted in red color. Several interactive tasks are provided, such as zooming, rotating, and selecting regions-of-interest.

B. State of the art

As a state-of-the-art report, we review articles and papers published between 2009 and 2013. We start from other fields, *i.e.*, works that do not address security management, and then, we describe works in the security field.

*1) **Other fields**:* Hofstede and Fioreze [107] developed a monitoring tool, called SURFMap, which provides network traffic information at a geographical dimension by using the Google Maps API. SURFMap obtains the network information from NetFlow records. The geographical dimension is obtained from the IP2Location utility. Markers (nodes) are used to represent IPv4 addresses and their geographical location. Lines that connect markers (links) provide information about network flows. This tool also provides interactive zooming and details on demand.

Dobrev *et al.* [108] introduce some experiments using visualization to understand the dynamics recorded in NetFlow traces. Additionally, they also explore SNMP traces. For example, one of the experiments uses a network animator (called nam) to visualize the exchange of SNMP messages between managers and agents in order to highlight how SNMP monitoring engines distribute the polling load over time. In this case, a 2D graph layout is employed.

To explore BGP routing policies, Lee and Kim [109] propose a system that helps decoding network configurations by interpreting low-level fragmented configurations and use them to present high-level inter-domain routing policies information for network operators. The system visualization provides policy units within a grid. The horizontal axis lists the egress links, and the vertical one lists the ingress links. Icons are used to indicate the most preferred and the least preferred links. Papadopoulos *et al.* [110] propose a visualization system to visualize routing changes using AS paths of the BGP announcements. This approach adopts a hierarchical visualization scheme (based on hierarchical clustering) displayed in a 2D graph layout.

Ramachandran and Street [111] introduce a library called Pathsift that provides features to generate and to analyze viable data forwarding routes in an IP network, resulting from different routing policies (*e.g.*, BGP) without packet-level protocol simulation. In conjunction to Pathsift, they present two visualizations to gain insights about paths between endpoint pairs. The first one is a network diagram to expose notable subgraphs, attributes of interest, and pathset overlays. The second refers to statistical plots (*e.g.*, heatmaps of pathset metrics) that summarize numerical data computed on large pathsets.

Inoue *et al.* [24][25][23][26] explore visualizations in the context of Mobile Ad-hoc NETworks (MANET). They propose a system called MANET Viewer. In the first version of MANET Viewer [24], they show a 2D graph layout in three modes: (*i*) a hop tree that displays the number of shortest hops from a given node in a hierarchical way; (*ii*) manual, which displays the network diagram, and (*iii*) GPS that displays the real location of nodes. In MANET Viewer II [25], the first version is improved by the visualization of the packet flow. In MANET Viewer III [26], they propose a 3D visualization to display network topology, node information, link quality, and

PREPRINT

packet flow. The nodes in the network topology are represented by colored spheres, in which colors represent the remaining quantity of the battery.

Bi [112] introduces a framework for modeling and simulating WSNs, where visualization is used to assist the design and monitoring of WSNs. The visualization allows 2D or 3D objects and displays in the scene the layout background, the distributed sensors, the connectivity, the represented sensing data, and the trend of data changes over sensors. Ma *et al.* [113] present a tool called NetViewer. This tool aims at helping in the development of WSNs, providing a universal visualization. They describe a generic XML scheme, which specifies the requirements of packets analysis in a WSN domain. In turn, a visualization tool translates network packets according to the XML specification and displays the WSN topology using a 2D graph layout and a 2D line chart.

Kumata and Koyama [114] propose a visualization system to help WMNs management, using a graph layout to show neighboring nodes. The nodes are represented by icons and positioned on their physical location. Riggio *et al.* [115][116] introduce a distributed network monitoring toolkit for wireless multi-hop networks called OBELIX. This tool offers a web-based management dashboard that allows network administrators to monitor and manage network conditions. A central view is used to display the network topology geographically on a Google map in real-time. Icons are used to display nodes. OBELIX also provides 2D line charts to view historical values from monitored network objects.

Yang *et al.* [31] introduce visualization features for home network management through a system called Eden. They argue that the network has moved into the home, and home users are not skilled to operate advanced network management tools. Eden uses visual features to depict the home network topology, and the house is visually represented by various separated rooms. Users' devices and network devices are represented by icons and placed within the house representation. Links are used to connect these devices. In essence, a traditional 2D graph layout is used.

Qiu *et al.* [117] introduce an approach to deal with network router syslogs. They describe a system called SyslogDigest that uses data mining techniques to interpret automatically low-level minimally-structured syslog messages into high-level network events. From information generated by SyslogDigest, a network health visualization is provided through a 2D graph layout on a geographical map. Each node represents a router, and each link represents the connections between these routers. The color of the node denotes the event severity, and size indicates the number of events.

Wang [118] describes a visualization system to manage large-scale networks. This system provides a visual representation of network topology, device and connection information, and representation of monitoring messages. A 2D graph displays the network layout. Nodes may be customized for different types of device icons, and interactive zooming is provided.

Liao *et al.* [119][120][121] describe a tool called ENAVis that provides visualization features to aid network operators in monitoring the network activities of hosts/domains, users, and applications. They use graph theory, context information, and data mining techniques to achieve the W^4 (who, what, when, and where) concept as follows: know what is happening on the network, *i.e.*, who (which users) is running what (applications) on where (which hosts) at when (what time). Heterogeneous 2D graph layouts (*i.e.*, each node in the graph can be either domain, host, user, application or data) are used to display this information. Interactive features such as filtering and details on demand are also provided. Fig. 11(a) depicts an example of heterogeneous graph layout.

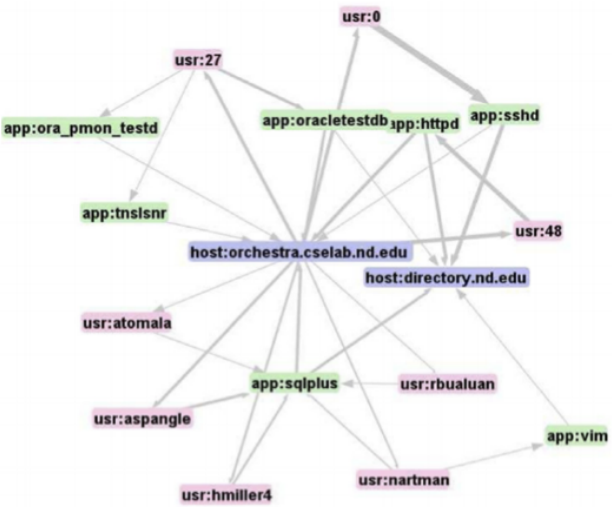
Barbosa and Granville [122] introduce a set of interactive information visualization techniques to visualize SNMP traffic traces. A network management topology visualization depicts the relationship between SNMP managers and agents. This view uses a 2D graph layout, where nodes are represented by circles. The edges of the graph represent traffic flows among managers and agents. The graph is integrated to a scatterplot or a bar histogram by a linking and brushing technique. SNMP objects and their relationships are displayed using a force-directed graph layout, in which objects that have greater affinity tend to appear closer. Fig. 11(b) shows the management network topology integrated with the scatterplot/histogram view.

Bartolini *et al.* [123] introduced a decision support tool for performance and business impact analysis and assisted redesign of Information Technology (IT) support organizations, called Symian-Web. The Symian-Web visualization is a graph-based representation that maps the support groups of the IT support organization. Each node represents a support group, and each edge represents the presence of ticket escalations between the corresponding support groups. Additionally, several metaphors to improve the visual communication were adopted, such as node proximity represents the interaction between the corresponding support groups, node size represents the amount of work, and edge size represents the flow of tickets between corresponding support groups. Interactive features are also provided, such as zooming and moving.

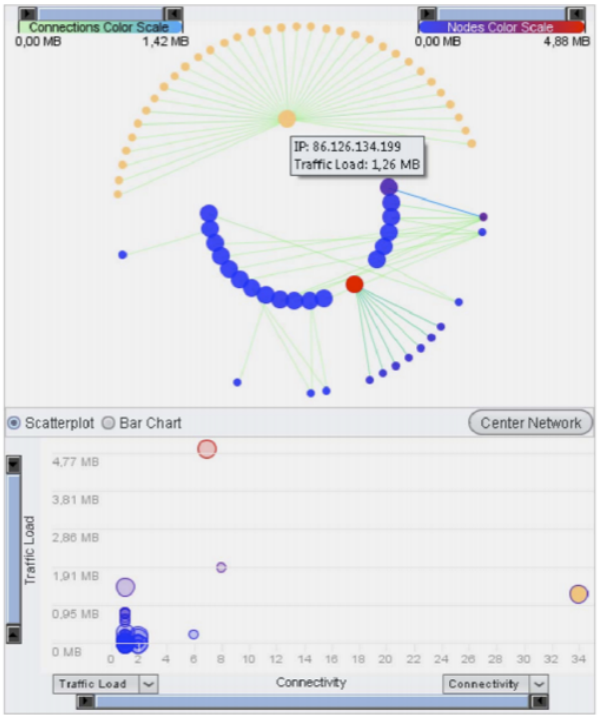
Kamamura *et al.* [124] propose the managed self-organizing network concept to satisfy future network requirements. These networks are formed by multiple virtual networks running on a single optical infrastructure. In this proposal, visualization is helpful because it provides an integrated view of the network resources (*e.g.*, topology and available resources), the allocated resources for each service network (*e.g.*, wavelength paths), and the virtual network topology of service networks (*e.g.*, the utilization of IP links). To achieve that, a 2D graph-based layout is used. Nodes are represented by icons (*e.g.*, router icon and cloud icon to represent networks). Links connect nodes, and their colors indicate, for example, if the link is shared by other virtual networks.

Sedlar *et al.* [125] describe an IPTV network monitoring system. This system uses a highly distributed system of probes, deployed at the end users' equipment, to monitor the state of an IPTV network. By its nature, this tool collects a large amount of monitoring data that is analyzed through a set of visualizations, for example, a web-based dashboard for interactive visualization of different error types. In this display 2D line charts (containing error statistics) are showed along a map

PREPRINT



(a)



(b)

Figure 11. (a) Heterogeneous graph layout showing connectivity between hosts, users, and applications [119]; (b) The management network topology integrated with the scatterplot/histogram view [122].

view of probes which is overlayed on Google maps. A graph-based layout is used to represent IPTV network topology (nodes are represented by circles and their colors indicate the percentage of the transport stream errors). Moreover, a 2D heatmap of error severity is provided.

Kim *et al.* [126] describe the design and implementation of a GUI-based management system for Service-Oriented Networks (SON). They argue that SON management becomes more complicated than traditional networks. Thus, an advanced GUI together with sophisticated management functions can reduce the operational complexity of network management. They use a 3D node-link representation to display network topology connections (physical and logical). Icons are used to represent nodes (*e.g.*, a server cluster is represented by a grouping of server icons). Additionally, performance data are displayed in gauges for each node. The color of nodes is used to encode, for example, the workload.

Tateishi *et al.* [127] propose a method to visualize network information in space and time to support network operators to recognize causal points of failure and affected areas. In summary, this method uses 3D spatial and temporal axes to explain geographic information, hierarchical information, physical and logical connections, and time variance of a network.

Himura and Yasuda [128] introduce a methodology that statically validates network device configurations before deployment in the context of multi-tenancy, *i.e.*, multiple virtual networks of different customers (tenants) are consolidated over a single physical infrastructure. They show a prototype implementation that displays the virtual resources and their interconnections in graph layout. This view provides, for example, information such as in the case of inter-tenant misconnection. In this case, corresponding nodes are highlighted to help detecting which virtual resources of which devices are actually about to cause such violation.

*2) **Security field**:* Herrero *et al.* [129] [15] introduce an approach based on artificial intelligent techniques to identify intrusions in computer networks. Several real anomalous situations related to the SNMP protocol are experimented to highlight its potential danger. A 3D matrix visualization is used to display information about the analyzed traffic. Another aspect of this approach is to provide visualization in mobile devices.

Mansmann *et al.* [130] focus on visualizations for network attacks. They describe a comparison between a treemap representation, previously used by Fischer *et al.* [87], and standard graph representation to understand such attacks. Additionally, they present three case studies (service monitoring, distributed SSH attack, and investigating blacklisted hosts) to demonstrate the applicability of these techniques in large-scale environments.

Choi *et al.* [131][132] introduce a Parallel Coordinate Attack Visualization (PCAV) for detecting unknown large-scale Internet attacks including Internet worms, DDoS attacks and network scanning activities. Parallel coordinates are used to display Internet attacks using four packet header fields: source IP address, destination IP address, destination port, packet length. From this information, attacks can be recognized since each attack has a unique graphical pattern on the parallel coordinate system. Fig. 12 depicts four examples of attacks and their graphical pattern on parallel coordinates.

Celenk *et al.* [133] describe an approach for predicting network anomalies (*e.g.*, worm outbreaks and DoS attacks) that uses short-term observations of network features and their respective time averaged entropies. They analyze network flow data to identify the signal corresponding to network anomalies. The visualization uses horizontal histogram bars in a 2D standard view. The colorization of histogram bars is designed

PREPRINT

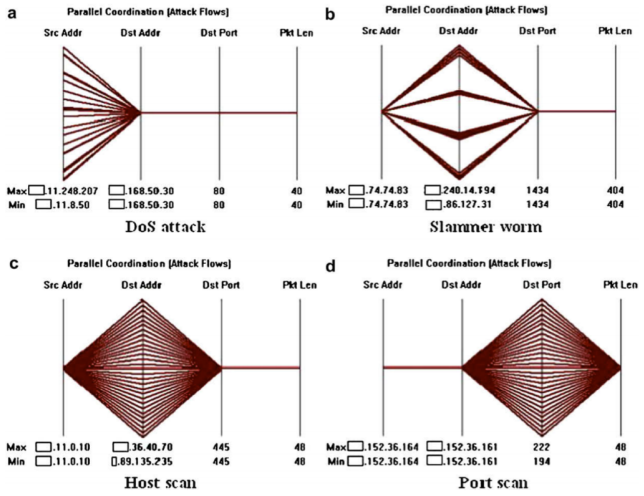


Figure 12. Four examples of graphical attack signatures in parallel coordinates visualization [131].

to aid analysts to reason about the level of interest in the anomaly. For example, a brighter red bar indicates a high level of interest in the anomaly while a brighter blue bar tells that the information is highly variable and indicates a need for more detailed traffic analysis.

Taylor *et al.* [134] explore visualization to perform forensic analysis of NetFlow data. They show a tool called FloVis that provides three visualizations. The first one is activity plots, where the activities of individual hosts are plotted against time in a simple two-dimensional grid. Color is used to encode the host's role. The second visualization is a bundle diagram, which displays connections entities in a network. NetBytes viewer provides the third visualization. This view shows flow volumes over time. It utilizes a 3D impulse graph with time, port, and volume dimensions. Interactive features such as zooming and filtering are available in the NetBytes viewer.

Kintzel *et al.* [135] also employ visualizations from NetFlow data to monitor large IP spaces looking for anomalous behaviors. They show a system called ClockView. Four-time series representations are used to display all internal hosts with their traffic at a granularity of one hour for a timespan of one day. We highlight the glyph in the style of a clock which is a circular representation subdivided into 24 segments, each of them showing the traffic of one hour encoded in color. Moreover, the network overview is arranged in a 2D matrix that allows interactive zooming. Two focus visualizations are also available by Host Matrix (that details host activity using the granularity of 1 minute) and parallel coordinates (to display all connected hosts). Details are provided by Port Matrix that shows the detailed activity between two machines. Fig. 13(a) shows the graphical user interface of the ClockView system.

Instead of NetFlow traces, Boschetti *et al.* [136] investigate visualizations to reveal hidden patterns from pcap, Wireshark, and Ettercap network traces. They show a tool called TVi, which provides five forms of visualizations. The 2D histograms show the distribution of TCP source ports during the detected anomaly. In a graph-based representation, nodes represent hosts and links are the connections among hosts. The matrix representation shows the destination IPs at the X axis and source IPs at the Y axis. The fourth visualization is a variation of the matrix representation, where the X axis shows the ports. The last form is a world-graph where each IP address is geolocalized using the GeoIP database.

Best *et al.* [137] describe two complementary views to provide situational understanding of real-time network activity to help analysts take proactive response steps. The first one is named as Correlation Layers for Information Query and Exploration (CLIQUE). This view is based on LiveRac [138], and it is used to display behavioral plots that allow to compare expected behavior against actual behavior. Moreover, an adaptation of the Symbolic Aggregate approXimation (SAX) technique is used to generate a set of glyphs that represent the trends occurring within the data, such as remaining constant, decreasing, increasing, peaks, valleys, and stair stepping. The second view is named as Traffic Circle, and it uses a circular time wheel metaphor to display flow records as arcs for large resolution displays. Fig. 13(b) depicts the Traffic Circle visualization.

Lu *et al.* [139] propose an intrusion detection approach for wireless networks. Specifically, they are interested in Sybil attacks. They employ four pattern reordering methods applied to a 2D matrix that represents the network topology. Each method provides a signature pattern of Sybil attacks in the matrix representation. Another visualization is based on a 2D histogram that reflects data properties along time-based on attack features, and assists users to analyze attack durations.

Zhao *et al.* [140][141] describe a visualization framework for intrusion detection system alerts. This framework works in real-time and uses a radial graph layout to represent an overall view of the security situation. The radial visualization is composed of five main parts as follows: servers and workstations, attack types, timeline and histogram, attack correlation, and other information. Servers and workstations are nodes arranged in circles in the center part of the radial graph, and their color and size determine the role of them in the infrastructure. The location of each node is based on its IP addresses. Alert types are showed in a color band in the edge of the center part of the radial graph. Colors are used to represent each alert type. Histograms represent the number of each alert type and are plotted below the alert type color arc in clockwise. Attack correlation is represented by lines (a triangle shape) that connect source node, the destination node, and the respective histogram bar. The outer ring shows additional statistical information to help network administrators using dots and triangles above the histogram bars. Fig. 14(a) depicts an example of this visualization.

Mansmann *et al.* [142] introduce a visualization tool to help network administrators in the understanding of firewall rules and object group definitions. The visualization tool is composed of three interface components. The first one depicts a hierarchical view on the firewall rules through a sunburst visualization. The second component shows the structured textual form of the firewall rules. The third component shows an interactive tree view to display the firewall access list and object group hierarchies. Fig. 13(c) depicts these three displays in the graphical user interface.

PREPRINT

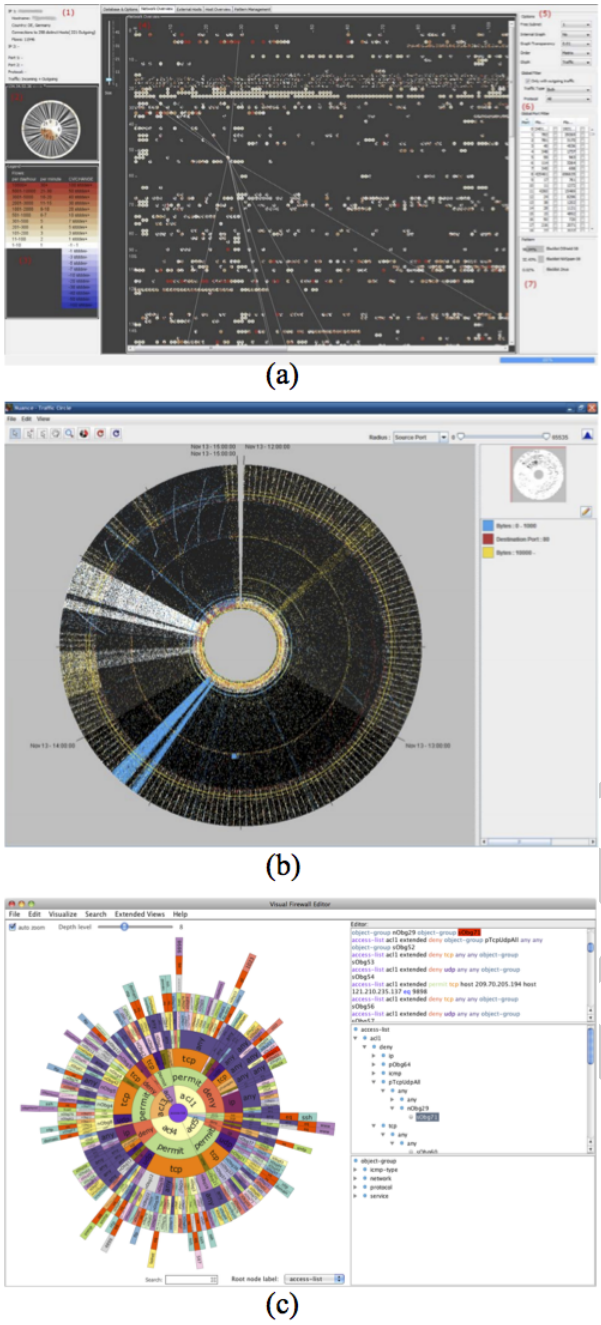


Figure 13. (a) The main interface of ClockView [135], where each area is described as follows: (1) host information, (2) subnet view, (3) color legend, (4) network overview, (5) options, (6) global filters, and (7) patterns; (b) Traffic Circle visualization [137], which was built to display large volumes of traffic flows, on very large resolution displays; (c) The sunburst visualization in the left side, the editor on top-right, the two tree views (access lists and object groups) on the bottom-right [142].

Inoue *et al.* [143] introduce a real-time 3D visualization engine called DAEDALUS-VIZ. The goal of this engine is to enable operators to understand visually alert circumstances on large-scale darknet monitoring (darknet is a set of globally announced unused IP addresses). In essence, DAEDALUS-VIZ is a real-time 3D visualization engine for DAEDALUS alerts as well as darknet traffic. The system has two main visual components: a central 3D sphere with a wireframe that represents the Internet, and several rings around the sphere that represent monitored organizations. Additionally, hundreds of comet-shaped darknet packets continuously drift from the sphere to the rings in real time. This visualization also provides interactive functions such as filtering and drilling down (deep dive). Fig. 14(b) depicts DAEDALUS-VIZ visualization.

Nunnally *et al.* [144] propose a visualization tool called P3D that uses 3D parallel visualization techniques to help network administrators in identifying and analyzing distributed scanning attacks that aim to distract them. P3D is based on a 3D coordinate system with colored links between two planes. One plane represents a range of source IP and ports, and the other plane a range of destination IP and ports. The color of links between the planes indicates the network connection type. Fig. 14(c) depicts an example of the source port confusion attack displayed in P3D visualization.

Harrison *et al.* [145] describe a web-based tool called NV. NV uses Nessus assessment tool to probe machines to obtain information about their potential vulnerabilities. The primary visualization is a zoomable treemap. In this view, IP addresses are grouped according to the severity of their vulnerabilities. For example, the largest and darkest-colored nodes in the treemap reveal the machines with the largest amount of severe vulnerabilities. Additionally, several histograms are provided with dual purposes: to give an overview of the data and to guide users in their analysis. Hao *et al.* [146] also describe a web-based visualization system designed for network security analysts at the U.S. Army Research Laboratory (ARL). This tool aims at visual support to the analysts to give better insights about security alerts for malicious activity within their systems. A set of 2D charts is provided, such as pie charts, bar charts, scatterplots, and Gantt charts. Interactive capabilities are provided by tooltips, zooming, and toolbars that allow customized glyph size, color, and shape, as well as other properties like title and size.

Fischer *et al.* [147][148] introduce the BANKSAFE, a situational awareness application for large-scale computer networks that explores big data technologies and provides several visualization modules. Briefly, BANKSAFE gathers monitoring data, and security datasets stored in Google's BigQuery database service and provides a web-based interface to display different visualization modules. These visualizations support network analysts in getting an overview, finding trends, and identifying suspicious events. TreeMap visualization displays the distribution of policy levels, enabling the analyst to have an overview of the network health. A colored pixel matrix is used to display temporal network health by the relation activity-policy, where the whole matrix represents one hour of data for one particular region. ClockMap (also presented by Kintzel *et al.* [135]) visualization represents time-series data of many hosts within their respective subnet or organizational hierarchy. Timelines are used to plot events from intrusion detection systems, where each timeline contains events from a specific IP address.

C. Other Initiatives

In this section, we intend to show some other initiatives that address the use of information visualization techniques to

PREPRINT

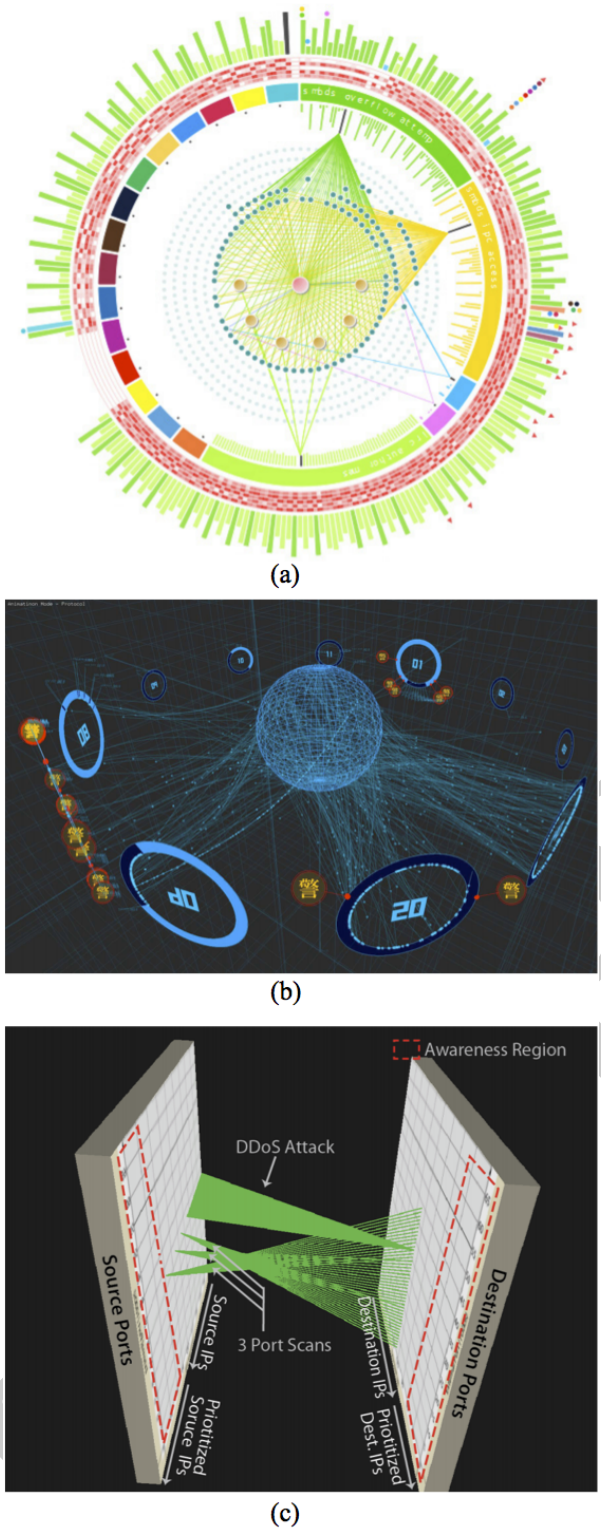


Figure 14. (a) The visualization proposed by Zhao [140]; (b) An overview of DAEDALUS-VIZ [143]; (c) An example of source port confusion attack represented by P3D visualization [144].

aid in network and service management tasks. Our goal is to highlight efforts that are not necessarily bound to publications in the field.

The Center for Applied Internet Data Analysis (CAIDA) is a collaborative undertaking among organizations with a strong interest in keeping primary Internet capacity and usage efficiency in line with ever-increasing demand. Among its research activities, CAIDA maintains a core of visualization research that aims at a better understanding of the Internet by using information visualization techniques. CAIDA promotes a long-term research in the field: its first publication was introduced in 1996 by Munzner *et al.* [50]. On the CAIDA website (http://www.caida.org) it is possible to find the results of their efforts in visualization research.

The Defense Research and Development Canada (DRDC) published a broad survey of network visualization tools [149]. This survey was the result of a contract report that examines research and development of network visualization techniques from available products (commercial and non-commercial) and a literature review about the topic. They describe a taxonomy of 139 products for network visualization as well as their attributes and screen captures. Additionally, they review 27 publications found in the literature search.

The portal SecViz - Security Visualization is a forum to share, discuss, and learn about security visualization. Basically, it was built for people that are working on log analysis, log mining and especially on visualization of security related data to exchange, discuss, and comment on techniques, methods, parsers, and sample graphs. This site is maintained by Raffael Marty, who also authored "Applied Security Visualization" in 2008 [150].

The report of the Visualization and Monitoring of Network Traffic Dagstuhl Seminar was published in 2010 [151]. The seminar brought together for the first time 36 researchers from Europe, USA, South Korea, Australia, New Zealand and Brazil. The researchers belong to the network and visualization community and discussed common grounds in capturing and visualizing network behavior as well as to exchange requirements and novel techniques.

Regarding projects, we present two security projects below, both supported by the Data Analysis and Visualization Group (http://research.dbvis.de). This group has made huge efforts on visual analytics concerning security issues and it appears in several publications presented in Section IV-B2.

- The VIS-SENSE - Visual Analytic Representation of Large Datasets for Enhancing Network Security (http://www.vis-sense.eu) project had as goal enhancing network security by using visual analytics of large datasets. To this end, the project aimed at researching and developing novel visual analytics technologies for the identification and prediction of complex patterns of abnormal behavior in computer networks.
- The VASA - Visual Analytics for Security Applications (http://www.va-sa.net) project has as main goal the use of visual analytics to disaster prevention and crisis response, with a focus on critical infrastructures in logistics, transportation, food safety, digital networks and power grids at national level. Among other objectives we highlight one in Information and Communication Technologies, in which they notice that, in the future, most critical infrastructures will rely on external telecommunication networks not under their control, generating new depen-

dencies that need adequate treatment.

M-Lab - Measurement Lab is a consortium of research, industry, and public interest partners dedicated to providing an ecosystem for the open, verifiable measurement of global network performance (http://www.measurementlab.net). M-Lab was founded by the New America Foundation's Open Technology Institute (OTI), the PlanetLab Consortium, Google Inc., and academic researchers. In summary, M-Lab is an open, distributed server platform on which researchers can deploy open source Internet measurement tools, and the data provided by those tools are released in the public domain. So, M-Lab is an open lab to build meaningful analyzes through visualization techniques.

BISmark - Broadband Internet Service Benchmark is a project led by Georgia Tech and the University of Napoli Federico II to develop an OpenWRT-based (Linux distribution for embedded devices) platform for performing measurements of ISP performance, as well as traffic inside the home (http://projectbismark.net). BISmark provides a network dashboard to help home users visualize properties of their home Internet connections. The active BISMark routers are plotted as a layer over Google maps and displays the world latency map. This view allows users to get detailed information from each router in a set of 2D charts.

V. Classification

In this section, we show the classification of the 285 articles and papers according to both a network and service management taxonomy and an information visualization taxonomy. First, we introduce the employed taxonomies, and afterwards, we present and discuss our classification.

A. Network and Service Management Taxonomy

Regarding network and service management, we have employed a taxonomy jointly defined by the Committee on Network Operations and Management (CNOM) of IEEE Communications Society, the Working Group 6.6 (IFIP WG 6.6) of the International Federation for Information Processing (IFIP), the Network Management Research Group (NMRG) of the Internet Research Task Force (IRTF), and the European Network of Excellence for the Management of Internet Technologies and Complex Services (EMANICS) [152]. Such taxonomy has two levels: the first one indicates a broad area, whereas the second level more precisely refines that area. Table I shows the network and service management taxonomy.

We choose this taxonomy because it is specific for network and service management, as well as being supported by that community. Moreover, keywords of the taxonomy are used by journals and conferences in the field, in two ways: (*i*) for authors to annotate their papers; and (*ii*) for researchers to indicate their area of expertise and interest. As such, this taxonomy matches with the purpose of this survey.

B. Information Visualization Taxonomy

Regarding the information visualization taxonomy, we have taken another way. We identified three main criteria to classify the surveyed papers as follows: (*i*) dataset types; (*ii*) information visualization techniques; and (*iii*) the available tasks/interactions for end-users. Although the information visualization field has a set of taxonomies described in the literature, some of them are either too specific for our purpose (*e.g.*, [153] and [154]), or do not cover the aforementioned criteria (*e.g.*, [155] and [14]).

Price *et al.* [153] presents a taxonomy for classifying software visualization systems in a hierarchy of categories from a high-level division in six categories ranging from the

Table I
Network and Service Management Taxonomy

Topic	Subtopic
Network Management	- Ad-hoc networks - Wireless & mobile networks - IP networks - LANs - Optical Networks - Sensor Networks - Overlay Networks - Virtual Networks - Software Defined and Programmable Networks - Data Center Networks - Smart Grids
Service Management	- Multimedia services (e.g., voice, video) - Data services (e.g., email, web) - Hosting (virtual machines) - Grids - Cloud services - Resource provisioning and management - QoE-centric management - Service discovery, migration and orchestration
Business Management	- Legal & ethical issues - Process management
Functional Areas	- Fault management - Configuration management - Accounting management - Performance management - Security management - SLA management - Event management
Management Approaches	- Centralized management - Distributed management - Autonomic and self management - Policy-based management - Federated network management - Pro-active management - Energy-aware network management
Technologies	- Protocols - Middleware - Mobile agents - P2P - Grid - Data, information, and semantic modeling - Cloud computing - Internet of Things - Human Machine interaction - Operations and Business Support Systems (OSS/BSS)
Methods	- Control theories - Optimization theories - Economic theories - Machine learning and genetic algorithms - Logics - Probabilistic, stochastic processes, queuing theory - Simulation - Experimental approach - Design - Monitoring & Measurements - Data mining and (big) data analytics

PREPRINT

scope of the software to the interaction it provides. Lee *et al.* [154] strongly focus on users' tasks: they describe a taxonomy of tasks for graph visualizations so we can use it to verify graph visualization techniques in terms of user tasks support.

On the other hand, Chi [155] and Tory and Möller [14], although proposing more general taxonomies, base their classifications on specific criteria. For example, Chi [155] actually proposes a reference model for visualization based on data transformation and then analyzes different techniques in terms of the operators they implement, while Tory and Möller [14] categorize visualization techniques based on their design models and not data, because at a certain extent a design model incorporates user needs, which is ultimately related to data.

Additionally, we observed that the taxonomy that covers those criteria [156], if applied alone, is not suitable for the purpose of our work. Keim's taxonomy [156] is based on a very general classification of data and, regarding interaction, there are some user tasks missing. Moreover, since 2002, taxonomies of users' tasks have been thoroughly discussed, and new application domains have contributed with new data types to this discussion.

Based on these issues, we have merged two taxonomies and a classification of dataset types to achieve the adequate framework needed for this survey. For the first criterion, we have used the dataset types classification proposed by Munzner [157]. For the other two criteria, we have used the taxonomies proposed by Keim [156] and Shneiderman [11], which is a classical one. Such taxonomies are widely accepted and referenced by the visualization community. We have chosen the taxonomy proposed by Keim to classify the information visualization techniques. This decision came from the fact that the taxonomy proposed by Shneiderman is focused on tasks and data types. Then, for the tasks/interactions criterion, we merged Keim's and Shneiderman's taxonomies. We have also added a new task called *Moving/Rotate* because this way we would include 3D visualization techniques. Table II shows the information visualization taxonomy defined for this survey.

Table II
INFORMATION VISUALIZATION TAXONOMY

Topic	Subtopic
Dataset types	- Tables [157] - Multidimensional tables [157] - Link/Node [157] - Trees [157] - Fields [157] - Geometry [157] - Static file [157] - Dynamic stream [157]
Visualization Techniques	- Standard 2D/3D displays [156] - Geometrically transformed displays [156] - Icon-based displays [156] - Dense pixel displays [156] - Stacked displays [156]
Tasks/ Interactions	- Overview [11] - Zoom/Interactive Zooming [11],[156] - Filter/Interactive Filtering [11],[156] - Details-on-demand [11] - Relate [11] - History [11] - Extract [11] - Linking and Brushing [156] - Moving/Rotate

C. Results and discussion

First, we highlight that the classification on taxonomies subtopics is not mutually exclusive. Thus, the same article may appear on more than one subtopic of each taxonomy.

We began the classification analysis from the network and service management taxonomy. Fig. 15 shows the number of classified articles/papers in each subtopic of such a taxonomy. Moreover, Appendix B presents how each subtopic of the taxonomy is filled regarding the surveyed articles/papers (see Tables IV-X). Our discussion pervades each topic of the taxonomy as shown below.

1) **Network management (Table IV):** IP networks prevails over other subtopics with 255 classified papers. This result is expected since the IP protocol is widely adopted. On the other hand, there are almost no works in hot topics such as virtual networks, data center networks, and software-defined networks. These topics may be promising to use information visualization for. For instance, virtual networks might have a multitude of different layers over the same physical infrastructure. Visualizations that enable to display a large number of virtual network nodes and their connections, on multiple layers representation, and in near real time may improve diagnoses and reactions of network administrators. Still in the network management topic, it is possible to identify some efforts on wireless and mobile networks.
2) **Service management (Table V):** here, the most frequent topic is Data Services (*e.g.*, e-mail, web) with 19 classified articles/papers. Indeed, we were curious regarding the service management topic because data services, multimedia services, hosting, and cloud services are consolidated for the industry as well as the academic community has widely researched them over the last years. Thus, we expected much more efforts in these fields since they are aligned to the myriad of services currently offered by providers. In such cases, visualization techniques could also provide rich tools in order to help network administrators, for instance, for multimedia services (*e.g.*, video streaming), a GIS-based map that shows the Key Performance Indicators (KPI) (*e.g.*, one-way delay, round-trip time, packet loss, and jitter) measured for points of interest in the network (*e.g.*, a border router). Such map can assist network administrators to quickly reacting on events of quality degradation. Furthermore, a timeline with long-term historical data over the same view can aid in capacity planning since overloaded points of the network could be easily identified and analyzed.
3) **Business management (Table VI):** based on this classification, we can state that this topic is off target for both communities, and it may be regarded as an open issue.
4) **Functional areas (Table VII):** as previously stated, security management is predominant in this topic. Here, we also highlight SLA management and account management because there are a few efforts regarding information visualization for these topics. In the age of Cloud

PREPRINT

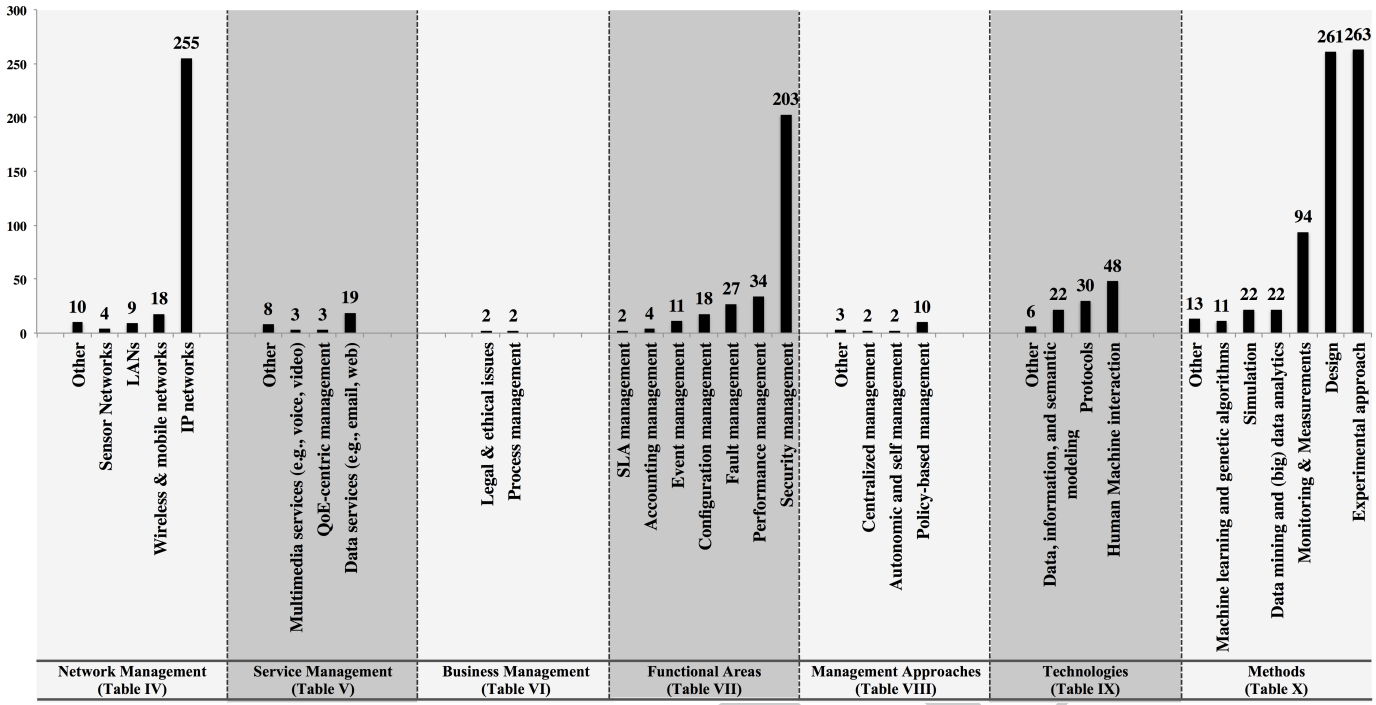


Figure 15. The 285 surveyed articles and papers classified following the network and service management taxonomy. Each topic of the taxonomy is identified in the bottom of the chart, together with the reference to its table in Appendix B. Moreover, subtopics are separated by dashed lines. Black bars depict the number of articles and papers classified in the taxonomy subtopics.

computing, SLA management, and account management are important management areas, since a huge amount of tools and applications are offered as a service and in a pay-per-use model. Thus, we believe that information visualization could be helpful for network administrators in SLA and account management. For SLA management, for example, an integrated map view that shows the infrastructure (*i.e.*, physical or virtualized devices and their connections) and the SLAs that are supported by such infrastructure could be imagined. Thus, based on the Service Level Specifications (SLS) of each SLA, the integrated view highlights (*e.g.*, through color, shape and sound alert) the SLAs that are near to be broken, and the devices that are affecting such SLAs. Regarding account management, a dashboard (*e.g.*, composed of a set of charts) with statistics about customer usage can aid network administrators to take short-term decision (*e.g.*, reallocation of resources) for optimizing resources usage without impacting the customer services.

5) **Management approaches (Table VIII):** the numbers reveal fewer efforts in this topic. The most frequent topic is policy-based management that appears with only 10 classified articles/papers. Autonomic and self-management, centralized management, and distributed management show only five articles/papers. We also highlight that there are no works addressing energy-aware network management. We highlight energy-aware network management as an interesting topic to be explored through visualizations, in special for green awareness management. For instance, a heatmap could represent a datacenter infrastructure where darker cells show a poor green performance, and lighter cells show a better green performance. Such heatmap could aid network administrators, for example, to identify in a more easier way regions where the energy consumption (*e.g.*, the energy consumption of devices and/or of refrigeration system) achieves higher levels and, consequently, worsening green performance.
6) **Technologies (Table IX):** here, the most frequent topics are human machine interaction (with 48 classified articles/papers), protocols (with 30 classified articles/papers), and data, information, semantic modeling (with 22 classified articles/papers). We highlight again a low number of articles/papers addressing Cloud computing. Additionally, there are almost no articles/papers on subtopics such as grids and peer-to-peer. For peer-to-peer networks, for example, we understand that information visualization could be helpful to understand the behavior of each peer and their role in the network as a whole. To achieve that, we believe that a near real-time graph is a feasible approach, in which nodes represent the peers and links represent the connections among peers.
7) **Methods (Table X):** in this topic, the two predominant subtopics (design and experimental approach) appear in almost all articles/papers. In general, surveyed articles and papers are structured describing the design of the proposal, and experimental approaches are used to show obtained results. Regarding monitoring & measurements subtopic, we expected to find more than 95 articles/papers (33.33% from the total of 285 classified articles and papers) in this subtopic due to the fact that Monitoring & measurements are one of the pillars of network and

PREPRINT

service management. Moreover, monitoring & measuring generate a plentiful amount of data that network administrators need to analyze to extract relevant information and, then, perform management tasks. As a last point, we highlight data mining and (big) data analytics. Specifically, we believe that big data analytics will receive even more attention from the network community, and information visualization techniques are promising for browsing in the world of big data.

For the classification following the information visualization taxonomy, we also discuss each topic of the taxonomy as shown below. Fig. 16 shows the number of classified articles/papers in each subtopic of such a taxonomy. Moreover, Appendix C presents how each subtopic of the taxonomy is filled regarding the surveyed articles/papers (see Tables XI-XIII).

1) **Dataset types (Table XI):** in this topic, tables and static files prevail over other subtopics, followed by link/node and dynamic stream. Tree appears only in a few works. In general, during the analysis of the surveyed articles and papers, we observed that some works do not clearly explain the used dataset. Thus, in such cases, we were challenged to analyze some peripheral information along the article/paper to infer about the used datasets. We point out this finding because information regarding the dataset types could be helpful in two ways at least: (*i*) for researchers that are interested in comparing/reproducing experiments using the same dataset type; and (*ii*) for general readers, since information about datasets make clear from which data the proposed visualizations are built.
2) **Visualization techniques (Table XII):** in this topic, standard 2D/3D displays subtopic prevails. We observe several works using 3D views to allow better visual analysis. Icon-based displays are also found in several works. In this subtopic, Glyph-based representations appear in many cases. For instance, in a graph layout, nodes have a specific shape according to their role or status. Dense pixel displays are represented by colored pixel maps. Geometrically transformed displays are represented by parallel coordinates. In essence, several works use parallel coordinates to outline patterns and behaviors. Stacked displays appear through TreeMap views.
3) **Tasks/interactions (Table XIII):** in this topic, three subtopics prevail as follows: overview, filter, and zooming. Moving/rotate, details on demand, and linking and brushing features are proposed only in a few works, in special comparing with the total of 285 surveyed articles and papers. History and extract each appear once, in only one article. We also point out that there is a significant number of articles and papers (specifically, 110 articles and papers) that we did not classify into Tasks/Interactions topic. In several cases, we are unsure whether authors do not highlight these features (*e.g.*, to save paper space in order to show other relevant information) or, in fact, the proposed visualization does not provide such features. Based on these findings, we observe that tasks and interactions could be an important issue to be addressed in future proposals.

After showing how surveyed articles and papers fit in both taxonomies separately, we correlate visualization techniques and tasks/interactions topics. Specifically, we intend to highlight how each tasks/interactions subtopic is explored in the scope of visualization techniques. Fig. 17 shows the number of papers that use each tasks/interactions subtopic for each of the visualization techniques. We believe that this correlation may provide useful insights such as (*i*) few articles and papers that have explored standard 2D/3D displays use linking and brushing interaction; and (*ii*) overview appears as the most explored task/interaction for all visualization techniques.

Finally, we map how each network and service management taxonomy subtopic is related to information visualization taxonomy subtopics. Fig. 18 shows a heatmap where rows depict the network and service management taxonomy and columns the information visualization taxonomy. Such a representation outlines the big picture regarding information visualization for network and service management. Based on Fig. 18, one can extract insights such as: (*i*) in security management the most used visualization techniques are standard 2D/3D displays and Icon-based displays, (*ii*) in monitoring & measurements only 8 surveyed articles and papers have used geometrically transformed displays, and (*iii*) by correlating Fig. 18 and Fig. 15 we observe that all works addressing performance management (*i.e.*, 34 articles and papers) have used standard 2D/3D displays as a visualization technique.

Although this subsection shows the indicators and the related discussions obtained from the proposed classification, we believe that the issues discussed here do not close the loop. On the contrary, we hope that this classification may trigger other insights from both research communities (network and service management and information visualization), and, then, reveal research opportunities.

VI. Future Research Directions

In this section, we discuss some future research directions regarding information visualization as a tool to help in network and service management tasks. The following topics will be addressed: Internet of Things (IoT), Big Data, Cloud computing, Software Defined Networking (SDN) and human-centered evaluation. These topics are based on information collected during the development of this work. We found few works addressing these topics in the context of information visualization for network and service management, which highlights them as opportunities for both communities.

The choice of IoT, Big Data, and Cloud computing was reinforced by analyzing Gartner's Hype Cycle Special Report for 2014 [158]. In that report, the market promotion and the perception of value were evaluated in over 2,000 technologies, services and trends in around 119 areas. By analyzing the Gartner's Hype Cycle, these topics appear as the main trend topics over the last three years. Regarding SDN, we foresee a disruptive paradigm in the network and service management field. Indeed, this topic may bring valuable research opportunities on information visualization for network and

PREPRINT

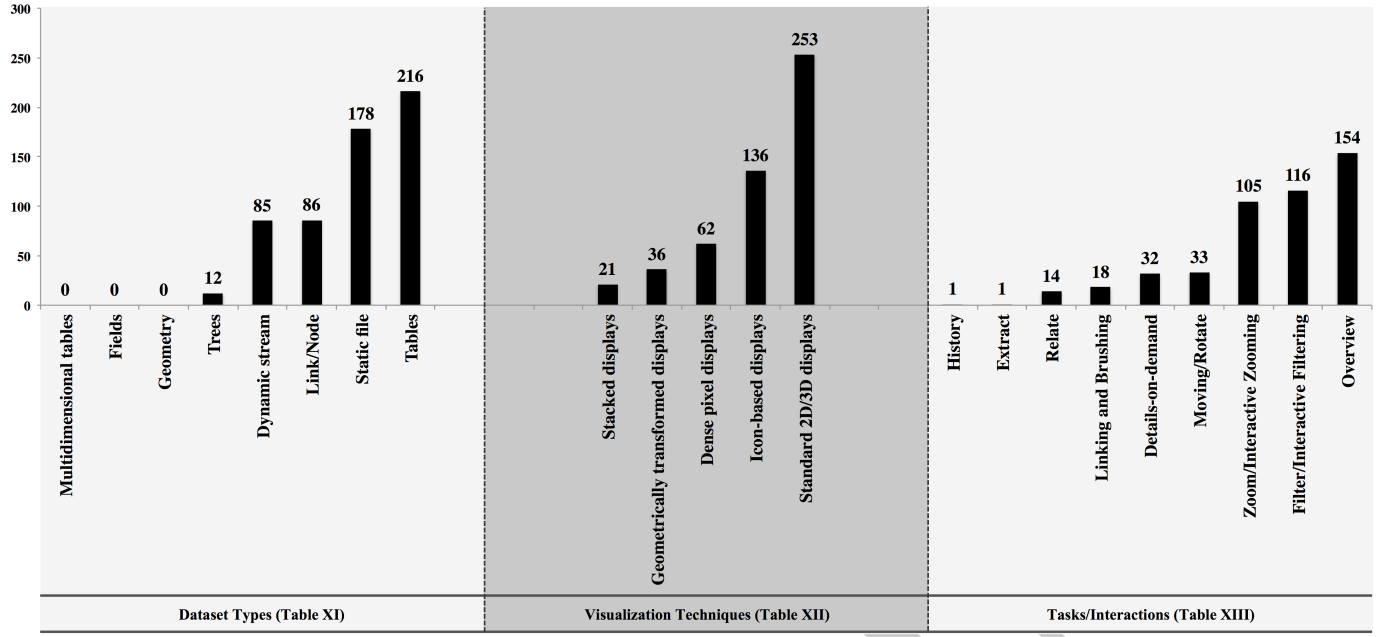


Figure 16. The 285 surveyed articles and papers classified following the information visualization taxonomy. Each topic of the taxonomy is identified in the bottom of the chart, together with the reference to its table in Appendix C. Moreover, subtopics are separated by dashed lines. Black bars depict the number of articles and papers classified in the taxonomy subtopics.

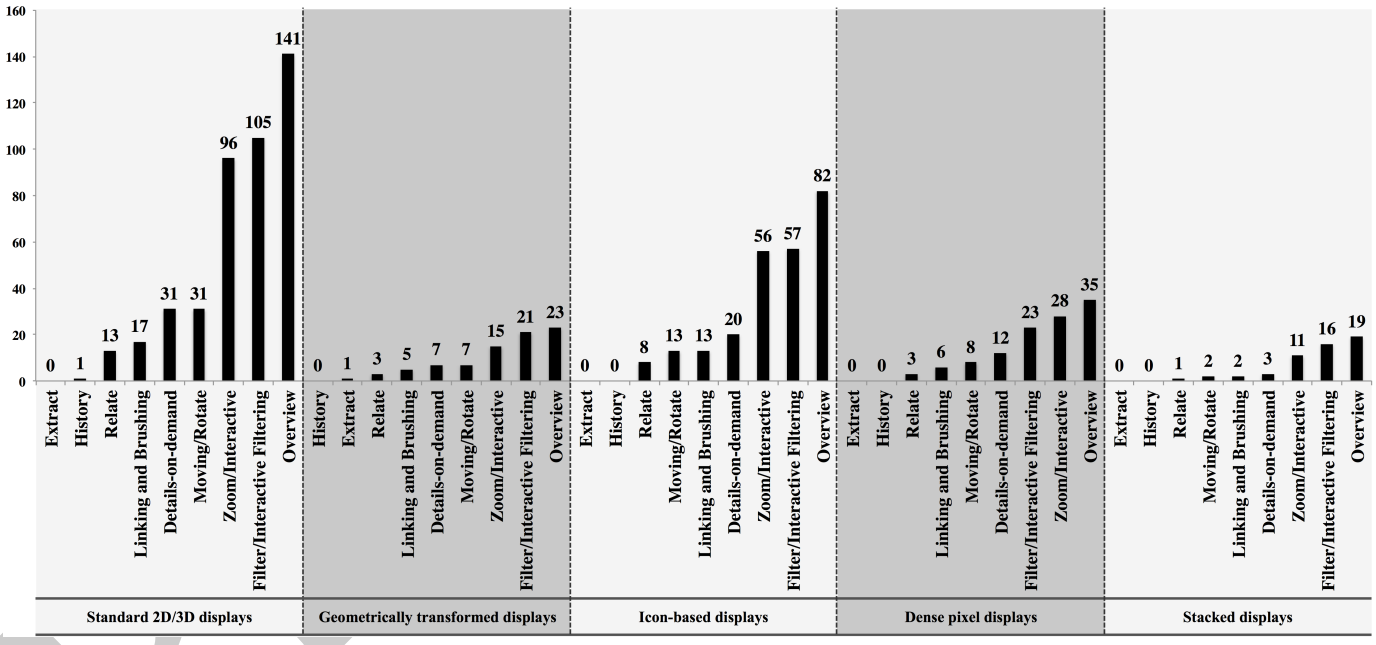


Figure 17. A classification that shows how tasks/interactions subtopics appear together with subtopics of the visualization techniques topic. Each subtopic of visualization techniques is identified in the bottom of the chart. Moreover, visualization techniques subtopics are separated by dashed lines. Black bars depict the number of articles and papers that use each subtopic of the tasks/interactions topic.

service management. For the last topic, we observed that, in most cases, human-centered evaluation is left out or has less attention during the development of visualizations for network and service management. Here, it is also important to highlight that human-centered evaluation can be regarded as a more horizontal topic, *i.e.*, it can be explored in the scope of different fields (*i.e.*, also for IoT, Big Data, Cloud computing, and SDN).

A. IoT

The name IoT is, in fact, fuzzy as well as its definition is not a consensus. Perera *et al.* [159] stated that research on the IoT is still in its infancy and, so, there are not any standard definitions for IoT. Here, we use the definition introduced by Gubbi *et al.* [160], in which the IoT is the interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework,

		Dataset types								Visualization Techniques					Tasks/Interactions								
		Tables	Multidimen-sional tables	Link/Node	Trees	Fields	Geometry	Static file	Dynamic stream	Standard 2D/3D displays	Geome-trically transformed displays	Icon-based displays	Dense pixel displays	Stacked displays	Overview	Zoom/ Interactive Zooming	Filter/ Interactive Filtering	Details-on-demand	Relate	History	Extract	Linking and Brushing	Moving/ Rotate
Network Management	Ad-hoc networks			1					2	3		2	1		3	2	2	1	1			1	2
	Wireless & mobile networks	9		8				8	7	18		9	3		11	6	5		3			1	3
	IP networks	195		66	10			156	72	213	32	116	58	20	127	89	98	27	9	1	1	15	28
	LANs	8						7	2	7	2	5			6	5	4	1				1	1
	Optical Networks	1							1	1		1			1		1						
	Sensor Networks			3				1	2	4		1			3	2	2						
	Overlay Networks																						
	Virtual Networks			1				1		1		1			1		1						
	Software Defined and Programmable Networks			1					1	1		1			1								
	Data Center Networks	1		1				3		2	1	1			1							1	
	Smart Grids			1					1	1					1	1	1	1	1				
Service Management	Multimedia services (e.g., voice, video)	1		1				2	1	3		2	1		1	1							
	Data services (e.g., email, web)	11		6	1			12	6	19	1	8	2	2	11	3	11	1	1			1	5
	Hosting (virtual machines)	1		1				1	1	2		1			2		1						1
	Grids																						
	Cloud services	1		1				1		2		2			1	1						1	
	Resource provisioning and management			2				1		1		2			2	1	1	1					1
	QoE-centric management	1		3				1	2	3		1	1		1	1							
	Service discovery, migration and orchestration	2		1				1	1	2		2			1	1	1						
B.M.*	Legal & ethical issues	1		1				2		2					1	1							
	Process management	1		2				1		1		2			2	1	1	2	1				1
Functional Areas	Fault management	19		7				17	9	25		17	2	1	11	5	7	1				2	3
	Configuration management	10		6				10	8	17	1	13	2		3		3					1	
	Accounting management	3		1				2	2	4		2			2	1	1	1					
	Performance management	23		8				15	17	34		18	3	2	14	9	11	4				3	5
	Security management	164		53	8			129	60	173	34	90	55	20	111	76	91	20	11	1	1	13	24
	SLA management	1		1					2	2		1			1	1	1	1					
	Event management	9		4	1			6	5	11	2	7	1		4	1	4	1					1
Management	Centralized management			2					1	2					1	1							
	Distributed management								1	1		1											
	Autonomic and self management	1		1				1	1	2		1	1		2		2						
	Policy-based management	5		3	2			4	3	9		5	1		4	3	3	1				1	2
	Federated network management	1							1	1			1		1		1						
	Pro-active management	1						1		1		1	1		1	1	1						1
	Energy-aware network management																						
Technologies	Protocols	19		15	4			22	7	28	1	17	7	2	11	7	9	1	1	1		2	2
	Middleware																						
	Mobile agents																						
	P2P	2		1				2		2		2			2	1							
	Grid							1			1												
	Data, information, and semantic modeling	18		5	1			15	5	20		12	2	2	11	8	13	4	1			1	
	Cloud computing			1	1			2		2	1	1			1	1	1						
	Internet of Things																						
	Human Machine interaction	36		12	1			28	18	40	8	26	10	5	35	22	29	7	3			5	11
	Operations and Business Support Systems																						
Methods	Control theories							1		1					1		2						1
	Optimization theories	1		2				1	1	2					1		1						
	Economic theories																						
	Machine learning and genetic algorithms	10		4				9	2	8	2	5	5		5	1	5	2	1				2
	Logics																						
	Probabilistic, stochastic …**	5		5				6	3	8	2	2	3		3	1	3	2	1			2	
	Simulation	13		12				15	3	20	2	10	6	1	14	10	9	2	2			2	5
	Experimental approach	199		81	12			165	78	235	30	124	55	18	142	96	105	30	10	1		15	31
	Design	200		79	11			164	76	235	28	127	57	18	140	97	102	30	9	1	1	16	28
	Monitoring & Measurements	75		21	3			51	40	83	8	38	27	10	52	36	35	11	2			5	9
	Data mining and (big) data analytics	18		6				17	3	21	1	12	4	2	11	7	10	1	2		1	1	2

** Business Management (B.M.)*

*** Probabilistic, stochastic processes, queuing theory*

0	1-5	6-15	16-20	21-25	26-40	41-65	66-200	> 200

Range of values

Figure 18. The heatmap relates subtopics of the network and service management and information visualization taxonomies. Each row corresponds to a network and service management subtopic. Each cell shows the number of classified articles and papers. Moreover, cells are filled with a color ranging in a grayscale according to the caption at the bottom.

developing a common operating picture for enabling innovative applications. This is achieved by seamless ubiquitous sensing, data analytics and information representation with Cloud computing as the unifying framework.

The above definition places the IoT as an essential part of the Future Internet. Indeed, a few years ago, the IoT would be only a promise of research, but now it is a reality. This finding is reinforced by the Gartner hype cycle of 2014, in which the IoT is at the top of the hype cycle. In essence, they announce that the IoT will reach its final stage of maturity in five to ten years. By this expectation, we believe the IoT will be a breeding ground filled with network and service management challenges, in which information visualization could be quite helpful to aid network administrators.

Gubbi *et al.* [160] suggest a GIS-based visualization to cope with data collected within the IoT, once they are geo-related and are sparsely distributed. This is a relevant use of visualization for the IoT. However, we are interested in visualization for network and service management activities. As shown in Table IX, there are no works in this subtopic. Thus, as a starting point for discussion, we take the SOA-based architecture for the IoT middleware proposed by Atzori [161]. This middleware is composed of five layers as follows (bottom to up): objects, object abstraction, service management, service composition, and applications. We are primarily interested in the middle layer, *i.e.*, service management.

As highlighted by Atzori [161], the service management layer is responsible to provide the main functions to allow management of IoT objects. Based on that, a set of management tasks encompasses (but is not limited to): object dynamic discovery, status monitoring, service configuration, Quality of Service (QoS) management, and policy and context management.

Regarding such management tasks, we envisage some challenges for the IoT visualization beyond the huge increase in the number of devices/objects communicating over the network. The first one is related to the variety of technologies/protocols involving IoT communications (*e.g.*, LTE, WiFi, WiMax, Bluetooth, and ZigBee). Moreover, some of these technologies/protocols operate in Low-power and Lossy Networks (LLN), such as IEEE 802.15.4. As a consequence, the management of IoT environments is a complex task, especially to maintain the environment secure and to provide fault tolerance. In this context, the use of visualization may be at once helpful for network administrators as well as a challenge for visualization designers.

The second challenge is related to the resource constraints of IoT devices/objects. Such devices may have limitations in terms of processing, memory, and power supply. For this reason, online or near real-time visualizations must be designed not to overwhelm these devices. The third challenge refers to the dynamicity of services provided by IoT devices/objects. Briefly, the IoT presupposes that any real object can collect and exchange data to extend available services or to create new ones. In such a context, the visualization must be prepared to deal with this dynamicity by avoiding, for example, a cluttered view of the services and devices relationship caused by changes in the composition of services.

Additionally, we introduce three promising usages of information visualization within the context of the IoT:

1) **Topology view:** understanding the network as a whole by visualizing objects position, their semantic and relationships in near real time is, indeed, a long-term dream of network operators. In the context of the IoT, it will be a claimed visualization tool. Additionally, interactive features with enhanced usability are mandatory, such as zooming, filtering, relating, and details on demand.
2) **Objects monitoring:** health care, urban traffic, and energy supply are few examples of services envisioned by the IoT. Object monitoring is a fundamental task in two ways: the monitoring of the object itself and the monitoring of the information provided by the object. In both cases, information visualization is helpful. In the first one, visualization is useful to display object status. For example, a view can display the shape of a body filled with glyphs/icons that represent the status (*e.g.*, network availability and energy consumption) of each sensor that monitors a given patient in a home care service. In the second case, a proper visualization to display an event receiver could be essential to aid the network analysts to recognize traps and notifications from objects.
3) **Security and privacy:** management of trust, privacy, and security is one of the key challenges in IoT. In fact, sensitive and confidential information can be a serious barrier to the growth of the IoT. As shown in this survey, several proposals addressing visualization for security issues on the current Internet are available. Thus, besides being a trending topic, the IoT is a great opportunity for the security community to revisit and adapt their current proposals. Here, we use the proposal of Mansmann *et al.* [105] (previously described in Section IV-B1) as an example. In the context of IoT, that proposal would be used to show policies and access lists for a set of smart things instead of displaying firewall rules. In this case, a simple adaptation of an existing visualization could be enough to help in the security management of IoT.

B. Big Data

Over the last three years, Big Data has been also at the top of Gartner hype cycle. In essence, Big Data is a general term to refer to a set of technologies that aim at extracting relevant information from a huge amount of unstructured or multi-structured data. Hu *et al.* [162] decompose a typical big data system into four consecutive phases as follows: data generation, data acquisition, data storage, and data analytics. They also highlight data analytics as the most important stage of the Big Data value chain, since it allows extracting useful values, suggesting conclusions and/or supporting decision-making. In this context, information visualization is one of the tools that allows and/or improves Big Data analysis.

On the other hand, network and service management can be regarded as a typical scenario of management of Big Data. For instance, the transmission capacity of current networks (*e.g.*, gigabit networks) associated with a huge amount of interconnected devices (*e.g.*, network devices, servers, desktops, smartphones, etc) generates large management datasets.

PREPRINT

The network and service management community is already focusing on this concern. For example, the theme of the 14th IFIP/IEEE Symposium on Integrated Network and Service Management (IM 2015) is the age of Big Data. Basically, with this theme the community will examine the potential of Big Data to improve the quality of network and service management.

From that context, exploring information visualization over large network management datasets by employing Big Data concepts is truly promising. Fischer *et al.* [147], in a very interesting work, share experiences on how to apply big data technology in a visual analytics application, more precisely, a network security application. We believe that there are several research opportunities in this field, beyond the security management.

For instance, passive measurements typically generate a plentiful amount of data. In this measurement method, traffic flows are captured either by a specific probe or network device (*e.g.*, a router) positioned in a key point of the network. Now, let's suppose a passive measurement (*e.g.*, flow monitoring) in the network core of a large provider that operates on a transmission rate of 1Gbps. Additionally, the collected traffic is exported in an interval of five minutes. This hypothetical scenario exemplifies the huge amount of measurement data that can be generated after one day of measurements in a production network. In such a context, Big Data technologies in conjunction with information visualization techniques could be a powerful tool to browse through these measurements datasets.

In summary, we believe that the usage of Big Data technologies and information visualization concepts to help on network and service management tasks is not only a trend but a reality for the next years.

C. Cloud Computing

A cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers [163]. In fact, Cloud computing is a new paradigm in which hardware, infrastructure, platform, and applications are offered as a service for end-users. Typically, theses service share a pool of computational resources to, for example, optimize resource allocation and decrease operational costs.

As observed in Section V, we found a few number of works addressing information visualization to aid in the network and service management tasks in cloud environments. Based on this finding, we select four cloud research challenges pointed by Zhang *et al.* [164]. For each one of them, we outline research opportunities involving network and service management and information visualization.

1) **Automated service provisioning** refers to the cloud capabilities to acquire and release resources on-demand. In this context, service providers need to maintain their Service Level Objectives (SLOs) and, at the same time, perform resource provisioning decisions in near real-time. Under this scenario, information visualization can help cloud analysts in both proactive and reactive resource control. For instance, an infrastructure map (2D or 3D) could display physical and virtual computational resources and their relationships. Moreover, this map could exhibit the resources load and its impact on the current Service Level Agreements (SLA). For a reactive approach this map could be refreshed online and display visual (*e.g.*, by color and shapes) and sound alerts when a new resource request impacts on current SLAs or requires setup of more resources. In a proactive fashion, this map combined with an appropriate heuristic could make an animation to display a more optimized resource allocation considering simulated sets of resource requests.
2) **Virtual machine migration** enables a virtual machine migration across the data center to get load balance. However, detecting workload hotspots and initiating a virtual machine migration is a hard task, especially to respond to sudden workload changes. In this sense, the same hierarchical map suggested in the previous item could generate a visual warning about overload hotspots, and suggest a possible destination for the virtual machine migration. Moreover, cloud analysts could simulate virtual migrations using this map view.
3) **Energy management** is a major issue in Cloud computing, in particular because it represents a significant amount of the cloud operational expenditure. Additionally, service providers are faced to meet government regulations and environmental standards. On the other hand, software mechanisms for saving energy are not obvious since they must deal with the trade-off between energy savings and application performance. Thus, energy management can be improved by human reasoning from visual analysis. For instance, a heat map of the physical infrastructure (*i.e.*, representing the physical distribution of the data center and providing historical data) could be helpful to cloud analysts. From this visualization, they could take decisions in order to decrease the energy consumption. For example, based on heat areas, they can get insights about how to decrease heat dissipation in that area and, consequently, decrease cooling consumption.
4) **Traffic management and analysis** is a long-term research issue also for traditional network environments. However, the density of links in Cloud computing is higher than in traditional environments, and the traffic patterns are also different. In this sense, information visualization techniques could be regarded as a powerful tool to understand better measurements and patterns of cloud traffic. The parallel coordinates technique could be exploited in the same way as it was exploited to understand attack patterns in the security field. Additionally, proper visualization techniques to display flow data as a live stream are also helpful. It may be achieved by standard 2D visualizations, such as line charts refreshed in near real-time. A more sophisticated approach may be a node/link layout, in which links vary their attributes (*e.g.*, thickness, color, and direction), according to net-

PREPRINT

work traffic flow. In this approach, animation with replay feature could be also interesting, especially to recognize the unusual behavior.

D. SDN

Software Defined Networking (SDN) is a new networking paradigm, related to the idea of programmable networks, in which the forwarding hardware is decoupled from control decisions [165]. According to the Open Networking Foundation (ONF) [166], SDN is the physical separation of the network control plane from the forwarding plane, where a control plane controls several devices. Traditionally, a network device (*e.g.*, routers, switches) is composed of two planes: the forwarding plane is responsible for receiving incoming packets and forwarding them to their destination according to routing policies; the control plane is responsible for managing routing policies, device configurations, and QoS rules, among other control functions.

SDN decouples these two planes. The control plane is delegated to an external entity called controller. The controller handles the control of a set of network devices. In turn, a network device performs only the forwarding plane functions according to rules configured by its controller. If a network device receives a packet and there is no routing rule to forward it, the network device sends the packet to its controller. The controller will decide between a forwarding rule only for that packet or the installation of a new forwarding rule for all packets with the same attributes.

From that perspective, SDN is a clean slate approach making possible innovations that are not feasible in current networks. For instance, network administrators can experiment with new algorithms for QoS provisioning with no changes in the network devices. Only the controller needs to know the algorithm since it will be responsible to set the forwarding rules in the network devices.

We identify three research directions concerning information visualization as a tool to aid in management of SDN-based networks, as follows:

1) **Control information:** since all network rules are triggered by the controller, visualizations that improve the understanding of the controller behavior could be paramount for the management of SDN-based networks. For instance, network operators need to be aware of which forwarding rules are run on each network device. A proper visualization of this information could be through a network map. In this map, each device could be queried to show the installed forwarding rules. Additionally, its neighbors would be automatically highlighted if there is a path to them.
2) **Network traffic management:** as introduced in Section VI-C, network traffic management is an essential task. In the context of SDN, beyond the traffic among network devices, the traffic between the network device and the controller is also crucial. The pattern of traffic between a network device and its controller may suggest some insights. For example, a significant volume of control traffic may indicate that the forwarding rules do not match with the significant amount of traffic. From another point of view, this may indicate a high polling rate set in the controller to collect flow statistics from a network device. Additionally, a huge amount of control traffic could be an attempt of DoS attack. Thus, visualization systems to address these issues could be very helpful for network operators.
3) **Multiple Controllers:** in large networks, the control tasks may be distributed among several controllers. For this reason, visualizing the network structure may be a hard task, for example, in a large SDN network composed of several physical devices running a large number of virtual devices, and controlled by several controllers. Understanding this hierarchy along with its connections may be a challenging task for network operators. A proper visualization of this structure could significantly decrease the workload of network administrators for troubleshooting as well as increase their possibilities to recognize unexpected conditions.

E. Human-centered evaluation

As previously introduced in Section II, information visualization uses visual representations of data to amplify cognition. From this definition, it is easy to infer that this discipline is strongly centered on human reasoning, *i.e.*, a given visualization technique will be effective if its visual and interaction capabilities satisfy its target audience. In this context, we envisage the human-centered evaluation of information visualization techniques as a key research challenge to improve the use of such techniques to support network administrators in the network and service management tasks.

Freitas *et al.* [167] discussed four main problems with usability evaluation of information visualization techniques:

1) The diversity of methods used for evaluating information visualization techniques is quite limited.
2) As a consequence of the previous problem, evaluation happens too late because user testing is mainly applied in later stages of development.
3) In general, an evaluation process for information visualization techniques does not follow a general usability evaluation methodology.
4) Information visualization techniques have been usually developed (and evaluated) following a technology-oriented perspective rather than a user-centered perspective.

Besides to these problems, we take into account the operational overhead of user-centered evaluation. For instance, gathering a group of network administrators that operate production networks is not an easy task. Normally, they are quite busy, and the evaluation process requires much time to achieve its goals.

Another aspect (more subjective) refers to the traditional tools commonly used by network administrators. Usually, many of these tools are based on Command Line Interfaces (CLI) (*e.g.*, prompt commands and log analysis), web-forms (*e.g.*, devices configuration), and static views (*e.g.*, reports).

PREPRINT

Network administrators are familiar with these types of interfaces. Enhanced visual interfaces that use information visualization techniques must be designed and evaluated aligned to the network administrators expectations to prevent these interfaces of being relegated to a secondary plane by them.

The aspects mentioned above highlight the need for user-centered evaluation. Specifically, we highlight the second problem of the list above (item 2), which emphasizes that the evaluation happens too late. Indeed, we believe that a proper assessment process needs to start jointly with the earlier stages of development (*e.g.*, with the requirements analysis stage) to achieve better results. Otherwise, a promising information visualization proposal may be ignored by network administrators because it was not designed and evaluated based on their requirements.

During this survey, we found some initiatives that address the evaluation of information visualization for network and service management [168] [22] [169]. However, all these efforts are focused on security issues. Foresti and Agutter [168] apply an interdisciplinary methodology that comprises several roles, such as the client, the applications team, the design team, the psychology team, the computing team, the administration team, and consultants. In this context, network administrators are part of the applications team and translate the client's needs and requirements into software programming needs.

Goodall [22] introduced a comparative evaluation between a traditional tool for packet analysis (in that case, Wireshark) and the TNV tool (a visual network packet analysis tool). In that research, eight Information Systems undergraduate and graduate students participated.

Stoll *et al.* [169] used the Personas Method, which consists of identifying and capturing significant details that shape the users' needs. In summary, the persona is a fictional character that simulates a real one. In this context, the authors have used characteristics of cyber-security analysts to model and create a persona.

We believe that the user-centered evaluation of information visualization for network and service management is a breeding ground for research and development. Moreover, we understand that user-centered evaluation will be more and more crucial for proposals addressing information visualization as a tool to support the network and service management tasks. In essence, a well-conducted user-centered evaluation allows to engage network administrators in the loop and ensure that their requirements for visual displays will be properly achieved.

VII. Conclusion

Traditionally, network and service management is accomplished using tools that help network administrators in their tasks. Information visualization techniques applied to management datasets can be a powerful tool to aid network administrators to recognize behaviors and patterns, especially in situations where human reasoning is essential.

In this paper, we present a comprehensive survey of efforts regarding information visualization techniques as a tool to help in network and service management. To this end, we have carried out a systematic literature review of 285 articles and papers published between 1985 and 2013 and classified them along two taxonomies on information visualization and network and service management.

We observe that efforts on information visualization for network and service management have started in the 90s. At that time, the AT&T Bell Laboratories team had relevant contributions, especially in the work presented by Becker *et al.* [2]. Until 2004, we can not characterize specific topics of interest since investigations were scattered on different network and service management topics. On the other hand, from 2004, when the VizSec forum started, investigations on information visualization for security management have prevailed. Thus, the state of the art from the network and service management perspective can be branched as follows: (*i*) several works addressing security, and (*ii*) scattered efforts over other fields. In the same context, information visualization was explored in several ways, without focusing on specific techniques.

In this section, we go back to the research questions presented in Section III-B, and outline conclusions and lessons learned along our study.

RQ1: What are the most explored topics on network and service management regarding the use of information visualization?

We can confirm that investigations on security management prevail. Translating to numbers, we found 203 works addressing this field, *i.e.*, around 71% of the total number of surveyed articles and papers. Regarding the number of classified works, other taxonomy subtopics could be highlighted, such as experimental approach (263), design (261), IP networks (255), and monitoring & measurements (94). However, the high number of works in such subtopics occurs because, in most case, they are explored jointly with other subtopics. For example, given work focusing on SLA management might be also classified as the IP networks and experimental approach subtopics. Also, we can observe some efforts on other subtopics such as Wireless & mobile networks, configuration and performance management, and protocols. However, the number of publications in these subtopics is too small compared to the security field.

RQ2: What are the most employed information visualization techniques and tasks/interactions for network and service management?

Regarding information visualization techniques, we observe the prevalence of the standard 2D/3D displays subtopic, with 253 classified works. Icon-based displays also appear in a significant number of works (136). In terms of tasks/interactions, the most explored subtopics are Overview (154), Filter/Interactive Filtering (116), and Zoom/Interactive Zooming (105). We also highlight the small number of works that have addressed tasks/interactions such as history, extract, relate, linking and brushing, details-on-demand, and move/rotate.

RQ3: What related insights are revealed by the proposed classification? For example, what are the most widely used information visualization techniques for a given network and service management topic?

PREPRINT

We have correlated the subtopics of the employed network and service management and information visualization taxonomies covered by the 285 surveyed articles and papers. Amongst others, we have identified the predominance of standard 2D/3D visualization for security management. Moreover, we have also showed how each tasks/interactions subtopic is explored for each visualization technique.

RQ4: What are the future research directions identified from this survey?

We suggest five topics for future research directions as follows: (*i*) IoT; (*ii*) Big data; (*iii*) Cloud computing; (*iv*) SDN; and (*v*) Human-centered evaluation. These suggestions are also based on observations of the market and industry trends.

APPENDIX A
EXTRA INDICATORS

During the entire survey, we collected some additional information for each article. After analyzing such information, we decided to explain briefly the most cited articles/papers and the most visited venues (*i.e.*, journal, conferences, etc.).

Regarding the most cited articles/papers, we focused on the twenty most cited. The top five articles/papers in citations over the entire researched papers are: [2] (440 citations), [51] (222 citations), [55] (212 citations), [170] (210 citations), and [80] (204 citations). Among these five articles/papers, only the article [80] addresses security issues. This finding is explained because the top four articles/papers were published before 2001, *i.e.*, they are older works and before the raising of the VizSec forum. Moreover, the influence of the VizSec forum is also visible in the twenty most cited articles/papers: Eight publications among the twenty most cited were published in this venue (*i.e.*, 40%).

Table III summarizes the ten most popular venues where the analyzed articles/papers were published. We also added two columns concerning the target audience. These columns show if the venue intends to target the visualization community or the network community. In this aspect, we observed a balance by excluding the VizSec forum. In fact, this forum is the only one that fits both communities. Another relevant point is related to the presence of NOMS and IM symposiums in the list. These forums are specifically focused on network and service management, *i.e.*, it denotes that efforts addressing visualization are expected and well accepted by the network community.

APPENDIX B
NETWORK AND SERVICE MANAGEMENT CLASSIFICATION TABLES

Tables IV-X show the number of articles in each subtopic of the network and service management taxonomy, and the reference for each one of them. Rows in the table are ordered by the column "Total", which means the number of works classified in each subtopic.

APPENDIX C
INFORMATION VISUALIZATION CLASSIFICATION TABLES

Tables XI-XIII show the number of articles in each subtopic of the information visualization taxonomy, and the reference for each one of them. Rows in the table are ordered by the column "Total", which means the number of works classified in each subtopic.

REFERENCES

[1] D. Harrington, R. Presuhn, and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks," RFC 3411, STD 62, Dec. 2002.

[2] R. A. Becker, S. G. Eick, and A. R. Wilks, "Visualizing network data," *IEEE Transactions on Visualization and Computer Graphics*, vol. 1, no. 1, pp. 16–28, Mar. 1995. [Online]. Available: http://dx.doi.org/10.1109/2945.468391

[3] A. Pras, J. Schoenwaelder, M. Burgess, O. Festor, G. Martinez Perez, R. Stadler, and B. Stiller, "Key research challenges in network management," *IEEE Communications Magazine*, vol. 45, no. 10, pp. 104–110, October 2007. [Online]. Available: http://doc.utwente.nl/64389/

[4] VizSec. (2004) Visualization for cyber security. [Online]. Available: http://www.vizsec.org/

[5] H. Shiravi, A. Shiravi, and A. A. Ghorbani, "A survey of visualization systems for network security," *IEEE Transactions on Visualization and Computer Graphics*, vol. 18, no. 8, pp. 1313–1329, Aug. 2012. [Online]. Available: http://dx.doi.org/10.1109/TVCG.2011.144

[6] S. Keele, "Guidelines for performing systematic literature reviews in software engineering," Technical report, EBSE Technical Report EBSE-2007-01, Tech. Rep., 2007.

[7] "ISO 7498-4: Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 4: Management Framework," 1989.

[8] "ISO 10040: Information Processing Systems - Open Systems Interconnection - Systems Management Overview," 1992.

[9] A. Pras, "Network management architectures," Ph.D. dissertation, University of Twente, Enschede, The Netherlands, 1995.

[10] A. Clemm, *Network Management Fundamentals*, 1st ed. Indianapolis, IN 46240 USA: Cisco Press, 2006.

[11] B. Shneiderman, "The eyes have it: A task by data type taxonomy for information visualizations," in *Proceedings of the 1996 IEEE Symposium on Visual Languages*, ser. VL '96. Washington, DC, USA: IEEE Computer Society, 1996, pp. 336–. [Online]. Available: http://dl.acm.org/citation.cfm?id=832277.834354

[12] S. K. Card, J. Mackinlay, and B. Shneiderman, *Readings in Information Visualization: Using Vision to Think*, 1st ed. San Diego, CA, USA: Academic Press, 1999.

[13] M. Ward, G. Grinstein, and D. Keim, *Interactive Data Visualization: Foundations, Techniques, and Applications*. Natick, MA, USA: A. K. Peters, Ltd., 2010.

[14] M. Tory and T. Möller, "Rethinking visualization: A high-level taxonomy," in *Proceedings of the IEEE Symposium on Information Visualization*, ser. INFOVIS '04. Washington, DC, USA: IEEE Computer Society, 2004, pp. 151–158. [Online]. Available: http://dx.doi.org/10.1109/INFVIS.2004.59

[15] E. Corchado and A. Herrero, "Neural visualization of network traffic data for intrusion detection," *Appl. Soft Comput.*, vol. 11, no. 2, pp. 2042–2056, Mar. 2011. [Online]. Available: http://dx.doi.org/10.1016/j.asoc.2010.07.002

[16] B. Le Grand and M. Soto, "Information management–topic maps visualization," in *XML Europe*, vol. 2000. Citeseer, 2000.

[17] T. Itoh, H. Takakura, A. Sawada, and K. Koyamada, "Hierarchical visualization of network intrusion detection data," *Computer Graphics and Applications, IEEE*, vol. 26, no. 2, pp. 40–47, March 2006.

[18] K. G. Provan and P. Kenis, "Modes of network governance: Structure, management, and effectiveness," *Journal of public administration research and theory*, vol. 18, no. 2, pp. 229–252, 2008.

[19] H. Koike, K. Ohno, and K. Koizumi, "Visualizing cyber attacks using IP matrix," in *Visualization for Computer Security, 2005. (VizSEC 05). IEEE Workshop on*, Oct 2005, pp. 91–98.

[20] R. Veras, J. Thorpe, and C. Collins, "Visualizing semantics in passwords: The role of dates," in *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*, ser. VizSec '12. New York, NY, USA: ACM, 2012, pp. 88–95. [Online]. Available: http://doi.acm.org/10.1145/2379690.2379702

PREPRINT

Table III
THE TEN MOST POPULAR VENUES

Venues	Publications	Target audience	
		Visualization	Network
VizSec - Symposium on Visualization for Cyber Security	99	X	X
CGA - IEEE Computer Graphics and Applications	8	X	
NOMS - IEEE/IFIP Network Operations and Management Symposium	7		X
LISA - Large Installation System Administration Conference	6		X
IEEE Network	6		X
IM - IFIP/IEEE Symposium on Integrated Network and Service Management	5		X
IAW - IEEE Information Assurance Workshop	5		X
TVGC - IEEE Transactions on Visualization and Computer Graphics	5	X	
VAST - IEEE Symposium on Visual Analytics Science And Technology	4	X	
IV - International Conference on Information Visualisation	4	X	

Table IV
NETWORK AND SERVICE MANAGEMENT TAXONOMY - TOPIC: NETWORK MANAGEMENT

Total	Subtopic	References of articles/papers
243	IP networks	[171] [172] [173] [174] [175] [176] [177] [178] [125] [144] [143] [179] [180] [181] [182] [183] [184] [185] [126] [186] [187] [140] [188] [110] [189] [190] [145] [191] [111] [192] [135] [193] [194] [15] [142] [195] [196] [197] [198] [136] [199] [200] [201] [202] [203] [204] [205] [206] [207] [208] [209] [210] [109] [211] [212] [213] [214] [215] [216] [118] [121] [217] [218] [117] [219] [131] [134] [220] [122] [129] [119] [221] [222] [223] [224] [225] [226] [133] [227] [228] [137] [229] [230] [231] [232] [107] [233] [234] [235] [130] [236] [237] [108] [238] [91] [239] [240] [65] [241] [242] [93] [243] [244] [245] [64] [87] [246] [247] [60] [248] [249] [66] [95] [250] [251] [252] [253] [254] [92] [59] [255] [256] [257] [94] [258] [88] [101] [259] [17] [105] [260] [261] [67] [262] [263] [99] [264] [265] [266] [267] [268] [269] [270] [271] [272] [273] [274] [83] [275] [276] [277] [278] [279] [102] [280] [281] [282] [89] [283] [284] [285] [58] [104] [286] [100] [287] [288] [289] [290] [291] [292] [293] [103] [294] [295] [296] [297] [298] [299] [72] [300] [19] [81] [30] [301] [302] [303] [304] [305] [57] [306] [90] [54] [80] [53] [307] [51] [49] [98] [308] [309] [310] [48] [311] [312] [79] [71] [73] [313] [61] [63] [82] [170] [314] [70] [69] [315] [39] [41] [316] [50] [317] [37] [2] [47] [46] [44] [318] [319] [320] [147] [321] [55] [322] [323] [43] [29] [324] [325] [326] [327] [31] [138]
18	Wireless & mobile networks	[328] [113] [115] [329] [330] [139] [331] [332] [333] [334] [68] [335] [106] [336] [337] [69] [26] [114]
9	LANs	[338] [201] [207] [255] [88] [79] [61] [69] [34]
4	Sensor Networks	[113] [112] [329] [330]
3	Data Center Networks	[128] [338] [339]
3	Ad-hoc networks	[329] [26] [340]
1	Virtual Networks	[124]
1	Software Defined and Programmable Networks	[341]
1	Smart Grids	[342]
1	Optical Networks	[343]
0	Overlay Networks	—

PREPRINT

Table V
NETWORK AND SERVICE MANAGEMENT TAXONOMY - TOPIC: SERVICE MANAGEMENT

Total	Subtopic	References of articles/papers
19	Data services (e.g., email, web)	[173] [175] [176] [181] [184] [187] [140] [199] [255] [262] [263] [277] [282] [302] [48] [73] [317] [318] [320]
3	QoE-centric management	[125] [183] [31]
3	Multimedia services (e.g., voice, video)	[125] [318] [320]
2	Service discovery, migration and orchestration	[188] [201]
2	Resource provisioning and management	[124] [123]
2	Hosting (virtual machines)	[341] [255]
2	Cloud services	[126] [339]
0	Grids	—

Table VI
NETWORK AND SERVICE MANAGEMENT TAXONOMY - TOPIC: BUSINESS MANAGEMENT

Total	Subtopic	References of articles/papers
2	Process management	[123] [119]
2	Legal & ethical issues	[177] [207]

Table VII
NETWORK AND SERVICE MANAGEMENT TAXONOMY - TOPIC: FUNCTIONAL AREAS

Total	Subtopic	References of articles/papers
203	Security management	[171] [172] [328] [173] [174] [342] [175] [146] [176] [177] [344] [330] [178] [144] [179] [180] [181] [143] [182] [184] [345] [185] [186] [187] [140] [188] [189] [190] [145] [341] [191] [192] [135] [194] [15] [142] [195] [196] [197] [139] [338] [136] [200] [199] [202] [203] [205] [206] [331] [208] [207] [209] [210] [211] [212] [213] [214] [215] [216] [121] [217] [218] [131] [134] [334] [220] [129] [221] [224] [225] [226] [133] [227] [228] [137] [230] [231] [232] [233] [234] [235] [130] [236] [237] [238] [91] [239] [240] [241] [242] [93] [243] [244] [245] [87] [246] [247] [248] [249] [95] [250] [335] [251] [252] [253] [254] [92] [106] [255] [256] [94] [257] [258] [88] [101] [259] [105] [17] [260] [261] [262] [263] [99] [264] [265] [266] [267] [268] [269] [270] [271] [272] [273] [274] [83] [275] [276] [277] [278] [279] [102] [280] [281] [282] [336] [89] [283] [284] [285] [286] [287] [100] [288] [289] [290] [291] [292] [293] [103] [294] [295] [296] [297] [298] [299] [300] [19] [81] [301] [302] [303] [304] [305] [306] [90] [54] [80] [53] [307] [98] [308] [309] [310] [311] [312] [79] [73] [313] [82] [170] [314] [315] [346] [97] [96] [147] [347] [321] [29] [324] [325] [326] [327]
34	Performance management	[125] [179] [183] [126] [115] [189] [205] [68] [60] [339] [250] [59] [257] [285] [104] [48] [71] [61] [63] [343] [170] [70] [50] [37] [2] [34] [26] [114] [318] [319] [320] [325] [31] [138]
27	Fault management	[115] [179] [189] [197] [205] [333] [220] [339] [255] [265] [71] [63] [343] [170] [50] [2] [44] [34] [114] [127] [318] [97] [96] [55] [29] [324] [325]
18	Configuration management	[128] [179] [111] [205] [109] [68] [339] [299] [30] [49] [71] [63] [343] [316] [318] [319] [320] [31]
11	Event management	[205] [49] [343] [82] [47] [346] [97] [96] [347] [55] [324]
4	Accounting management	[205] [60] [170] [34]
2	SLA management	[205] [138]

Table VIII
NETWORK AND SERVICE MANAGEMENT TAXONOMY - TOPIC: MANAGEMENT APPROACHES

Total	Subtopic	References of articles/papers
10	Policy-based management	[185] [341] [192] [109] [95] [94] [300] [170] [320] [323]
2	Centralized management	[193] [67]
2	Autonomic and self management	[124] [332]
1	Pro-active management	[137]
1	Federated network management	[332]
1	Distributed management	[115]
0	Energy-aware network management	—

PREPRINT

Table IX
NETWORK AND SERVICE MANAGEMENT TAXONOMY - TOPIC: TECHNOLOGIES

Total	Subtopic	References of articles/papers
48	Human Machine interaction	[172] [173] [174] [175] [146] [329] [176] [143] [187] [140] [188] [189] [190] [145] [135] [142] [197] [198] [123] [202] [331] [333] [109] [212] [225] [228] [230] [243] [249] [254] [94] [258] [269] [270] [275] [283] [284] [287] [290] [293] [294] [295] [297] [306] [90] [98] [147] [31]
30	Protocols	[171] [110] [111] [194] [201] [205] [210] [109] [122] [231] [108] [240] [65] [241] [64] [66] [252] [278] [279] [284] [58] [104] [300] [30] [305] [57] [69] [42] [29] [327]
22	Data, information, and semantic modeling	[185] [196] [197] [136] [203] [204] [333] [229] [244] [60] [248] [59] [88] [17] [261] [99] [269] [51] [42] [34] [32] [147]
3	Cloud computing	[126] [185] [338]
2	P2P	[195] [276]
1	Grid	[338]
0	Operations and Business Support Systems (OSS/BSS)	—
0	Mobile agents	—
0	Middleware	—
0	Internet of Things	—

[21] A.-V. Dinh-Duc, T.-H. Dang-Ha, and N.-A. Lam, "Nviz - a general purpose visualization tool for wireless sensor networks," in *Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2012 9th International Conference on*, May 2012, pp. 1–4.

[22] J. Goodall, "Visualization is better! A comparative evaluation," in *Visualization for Cyber Security, 2009. VizSec 2009. 6th International Workshop on*, Oct 2009, pp. 57–68.

[23] A. Koyama, S. Sato, L. Barolli, and M. Takizawa, "An implementation of visualization system for visualizing network topology and packet flow in mobile ad hoc networks," in *Network-Based Information Systems (NBiS), 2012 15th International Conference on*, Sept 2012, pp. 148–155.

[24] A. Koyama, K. Kamakura, and L. Barolli, "MANET-viewer: A visualization system for mobile ad-hoc networks," in *Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia*, ser. MoMM '09. New York, NY, USA: ACM, 2009, pp. 452–457. [Online]. Available: http://doi.acm.org/10.1145/1821748.1821834

[25] S. Sato, A. Koyama, and L. Barolli, "MANET-Viewer II: A visualization system for visualizing packet flow in mobile ad-hoc networks," in *Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference on*, March 2011, pp. 549–554.

[26] A. Inoue, Y. Takahashi, and A. Koyama, "MANET Viewer III: 3d visualization system for mobile ad hoc networks," in *Network-Based Information Systems (NBiS), 2013 16th International Conference on*, Sept 2013, pp. 178–185.

[27] W. Fang, B. P. Miller, and J. A. Kupsch, "Automated tracing and visualization of software security structure and properties," in *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*, ser. VizSec '12. New York, NY, USA: ACM, 2012, pp. 9–16. [Online]. Available: http://doi.acm.org/10.1145/2379690.2379692

[28] H. Burch and B. Cheswick, "Mapping the internet," *Computer*, vol. 32, no. 4, pp. 97–98, 102, Apr 1999.

[29] S. T. Teoh, K. liu Ma, S. F. Wu, and K. Words, "A visual technique for internet anomaly detection," in *IASTED International Conference on Computer Graphics and Imaging (CGIM '02), IASTED*. ACTA Press, 2002.

[30] L. Colitti, G. D. Battista, F. Mariani, M. Patrignani, and M. Pizzonia, "Visualizing interdomain routing with BGPlay," in *JOURNAL ON GRAPH ALGORITHMS AND APPLICATIONS*, 2005, pp. 2004–2005.

[31] J. Yang, W. K. Edwards, and D. Haslem, "Eden: Supporting home network management through interactive visual tools," in *Proceedings of the 23Nd Annual ACM Symposium on User Interface Software and Technology*, ser. UIST '10. New York, NY, USA: ACM, 2010, pp. 109–118. [Online]. Available: http://doi.acm.org/10.1145/1866029.1866049

[32] R. S. Gilbert and W. B. Kleinöoder, "CNMGRAF – graphic presentation services for network management," *SIGCOMM Comput. Commun. Rev.*, vol. 15, no. 4, pp. 199–206, Sep. 1985. [Online]. Available: http://doi.acm.org/10.1145/318951.319049

[33] G. Kar, B. Madden, and R. Gilbert, "Heuristic layout algorithms for network management presentation services," *Network, IEEE*, vol. 2, no. 6, pp. 29–36, Nov 1988.

[34] B. Anderson and R. Linebarger, "A graphical representation for network management," in *Local Computer Networks, 1989., Proceedings 14th Conference on*, Oct 1989, pp. 106–124.

[35] R. Becker, S. Eick, E. Miller, and A. Wilks, "Dynamic graphics for network visualization," in *Visualization, 1990. Visualization '90., Proceedings of the First IEEE Conference on*, Oct 1990, pp. 93–96, 467.

[36] R. Becker, S. Eick, and A. Wilks, "Graphical methods to analyze network data," in *Communications, 1993. ICC 93 Geneva. Technical Program, Conference Record, IEEE International Conference on*, vol. 2, May 1993, pp. 946–951 vol.2.

[37] K. Cox and S. Eick, "Case study: 3d displays of internet traffic," in *Information Visualization, 1995. Proceedings.*, Oct 1995, pp. 129–131.

[38] S. Eick, "Aspects of network visualization," *Computer Graphics and Applications, IEEE*, vol. 16, no. 2, pp. 69–72, Mar 1996.

[39] J. Abello, E. R. Gansner, and S. C. North, "Large-scale network visualization," *ACM Computer Graphics*, 1999.

[40] E. Koutsofios, S. North, R. Truscott, and D. Keim, "Visualizing large-scale telecommunication networks and services," in *Visualization 99. Proceedings*, Oct 1999, pp. 457–461.

[41] E. Koutsofios, S. North, and D. Keim, "Visualizing large telecommunication data sets," *Computer Graphics and Applications, IEEE*, vol. 19, no. 3, pp. 16–19, May 1999.

[42] J. A. Zinky and F. M. White, "Visualizing packet traces," *SIGCOMM Comput. Commun. Rev.*, vol. 22, no. 4, pp. 293–304, Oct. 1992. [Online]. Available: http://doi.acm.org/10.1145/144191.144303

[43] M. P. Consens, M. Z. Hasan, and A. O. Mendelzon, "Using Hy+ for network management and distributed debugging," in *Proceedings of the 1993 Conference of the Centre for Advanced Studies on Collaborative Research: Software Engineering - Volume 1*, ser. CASCON 93. IBM Press, 1993, pp. 450–471. [Online]. Available: http://dl.acm.org/citation.cfm?id=962289.962326

[44] M. P. Consens and M. Z. Hasan, "Supporting network management through declaratively specified data visualizations," in *Proceedings of the IEEE/IFIP Third International Symposium on Integrated Network Management, III*. Elsevier North, 1993, pp. 725–738.

[45] L. Crutcher, A. Lazar, S. K. Feiner, and M. Zhou, "Management of broadband networks using 3d virtual world," in *High Performance Distributed Computing, 1993., Proceedings the 2nd International Symposium on*, Jul 1993, pp. 306–315.

[46] S. Feiner, M. Zhou, L. Crutcher, and A. Lazar, "A virtual world

PREPRINT

Table X
NETWORK AND SERVICE MANAGEMENT TAXONOMY - TOPIC: METHODS

Total	Subtopic	References of articles/papers
263	Experimental approach	[328] [173] [174] [342] [175] [146] [329] [176] [177] [344] [330] [125] [178] [128] [144] [179] [180] [181] [143] [182] [183] [184] [345] [126] [185] [186] [187] [140] [110] [188] [115] [189] [124] [341] [145] [190] [191] [111] [192] [193] [135] [194] [142] [15] [195] [196] [197] [338] [139] [198] [136] [200] [123] [201] [199] [203] [202] [204] [205] [206] [208] [332] [333] [210] [109] [211] [212] [213] [214] [215] [216] [118] [121] [217] [218] [117] [219] [131] [134] [334] [122] [119] [221] [222] [223] [224] [225] [226] [133] [227] [137] [229] [228] [230] [207] [107] [233] [235] [130] [234] [236] [108] [238] [91] [239] [240] [65] [241] [242] [93] [244] [245] [243] [64] [87] [68] [246] [60] [247] [248] [249] [66] [339] [95] [250] [335] [251] [252] [253] [254] [92] [106] [59] [255] [256] [94] [257] [258] [88] [101] [259] [105] [17] [260] [261] [67] [262] [263] [99] [264] [265] [266] [268] [269] [270] [271] [272] [274] [83] [275] [276] [277] [278] [102] [279] [280] [281] [282] [336] [283] [89] [284] [285] [58] [286] [287] [100] [288] [290] [289] [291] [292] [103] [295] [294] [296] [297] [298] [299] [72] [300] [19] [30] [81] [301] [302] [303] [304] [305] [57] [306] [90] [54] [348] [80] [53] [52] [307] [51] [49] [98] [309] [310] [311] [48] [312] [79] [337] [71] [73] [313] [61] [63] [343] [82] [170] [314] [70] [315] [39] [41] [316] [50] [317] [2] [47] [46] [44] [42] [34] [33] [32] [346] [26] [114] [127] [318] [319] [320] [147] [347] [321] [55] [322] [323] [43] [29] [324] [325] [326] [327] [31] [138]
261	Design	[328] [173] [174] [342] [146] [329] [177] [176] [344] [330] [128] [125] [144] [179] [181] [143] [182] [183] [184] [345] [126] [185] [187] [140] [110] [188] [115] [189] [124] [341] [145] [190] [111] [191] [192] [193] [135] [194] [142] [15] [195] [196] [197] [338] [139] [198] [136] [200] [123] [201] [199] [203] [202] [204] [205] [331] [208] [332] [333] [209] [210] [109] [211] [212] [213] [214] [215] [216] [118] [121] [217] [218] [117] [219] [131] [134] [334] [122] [129] [119] [221] [222] [223] [224] [225] [226] [133] [227] [137] [229] [228] [230] [207] [231] [232] [107] [233] [130] [235] [234] [236] [237] [108] [238] [91] [239] [240] [65] [241] [242] [93] [244] [245] [243] [87] [64] [68] [246] [60] [247] [248] [249] [66] [339] [250] [335] [251] [252] [253] [254] [92] [106] [59] [255] [256] [94] [257] [258] [88] [101] [259] [105] [17] [260] [261] [67] [262] [263] [99] [264] [265] [267] [268] [269] [270] [271] [272] [273] [274] [83] [275] [276] [277] [278] [102] [279] [280] [281] [336] [283] [89] [284] [58] [285] [104] [100] [288] [290] [291] [292] [103] [295] [294] [296] [297] [298] [299] [72] [300] [19] [30] [81] [301] [302] [303] [304] [305] [57] [306] [90] [54] [348] [80] [53] [307] [52] [51] [49] [98] [308] [309] [310] [311] [48] [312] [79] [337] [71] [73] [313] [61] [63] [343] [82] [314] [170] [70] [69] [315] [39] [41] [316] [50] [317] [37] [2] [47] [46] [44] [42] [34] [33] [32] [346] [26] [114] [127] [318] [319] [320] [97] [96] [347] [323] [29] [324] [325] [326] [327] [31] [138]
94	Monitoring & Measurements	[112] [349] [175] [329] [344] [125] [182] [184] [186] [126] [115] [341] [194] [195] [136] [201] [331] [332] [210] [211] [217] [219] [131] [134] [119] [226] [227] [137] [229] [230] [207] [107] [233] [130] [108] [87] [60] [248] [250] [253] [252] [106] [59] [257] [88] [259] [105] [262] [264] [265] [267] [268] [269] [273] [83] [279] [283] [285] [286] [288] [291] [292] [103] [298] [297] [19] [301] [302] [303] [304] [80] [307] [52] [51] [309] [73] [63] [343] [82] [170] [70] [315] [39] [47] [114] [319] [97] [321] [55] [322] [29] [324] [325] [138]
22	Simulation	[112] [330] [128] [144] [180] [187] [111] [139] [123] [214] [334] [220] [231] [232] [106] [102] [104] [308] [69] [46] [340] [326]
22	Data mining and (big) data analytics	[179] [182] [110] [15] [195] [136] [209] [121] [117] [219] [119] [234] [105] [265] [269] [303] [305] [309] [48] [44] [147] [324]
11	Machine learning and genetic algorithms	[176] [210] [129] [119] [225] [226] [133] [235] [249] [267] [53]
10	Probabilistic, stochastic processes, queuing theory	[171] [328] [177] [180] [186] [139] [203] [133] [286] [292]
2	Optimization theories	[183] [140]
1	Control theories	[175]
0	Logics	—
0	Economic theories	—

PREPRINT

Table XI
INFORMATION VISUALIZATION TAXONOMY - TOPIC: DATASET TYPES

Total	Subtopic	References of articles/papers
216	Tables	[172] [345] [349] [245] [282] [283] [286] [287] [290] [294] [297] [299] [19] [301] [302] [303] [304] [305] [57] [306] [90] [80] [49] [316] [50] [37] [182] [140] [135] [174] [192] [194] [143] [190] [15] [139] [136] [202] [204] [47] [317] [320] [203] [188] [195] [206] [208] [333] [55] [31] [214] [218] [221] [223] [225] [226] [133] [227] [137] [332] [210] [212] [213] [117] [131] [134] [220] [145] [224] [170] [228] [231] [232] [107] [48] [236] [237] [108] [238] [91] [239] [327] [244] [65] [242] [60] [66] [87] [248] [253] [249] [243] [335] [92] [138] [235] [106] [255] [240] [256] [44] [52] [247] [105] [263] [336] [254] [59] [257] [258] [101] [259] [17] [99] [264] [325] [267] [268] [270] [271] [272] [273] [274] [275] [277] [102] [280] [58] [292] [103] [295] [296] [334] [83] [276] [281] [324] [285] [104] [100] [288] [289] [291] [293] [310] [307] [98] [308] [309] [311] [337] [79] [71] [63] [82] [29] [73] [81] [313] [61] [260] [69] [315] [54] [39] [347] [51] [119] [34] [32] [97] [96] [326] [72] [251] [93] [129] [33] [322] [147] [319] [201] [191] [64] [265] [312] [42] [2] [94] [122] [144] [339] [250] [230] [207] [53] [41] [89] [70] [298] [266] [314] [88] [234] [269] [130] [261] [284] [146] [43] [343] [209] [95] [178] [233] [262]
178	Static file	[172] [173] [176] [180] [128] [183] [182] [179] [181] [318] [177] [111] [194] [142] [197] [338] [198] [200] [320] [203] [188] [124] [190] [195] [136] [199] [204] [206] [208] [55] [214] [216] [215] [109] [185] [218] [219] [221] [222] [223] [225] [226] [133] [137] [212] [213] [217] [117] [131] [134] [220] [145] [224] [228] [231] [232] [108] [238] [91] [65] [327] [241] [242] [244] [87] [68] [246] [60] [249] [243] [66] [321] [92] [112] [235] [106] [255] [175] [44] [52] [247] [105] [336] [252] [254] [59] [259] [17] [264] [325] [267] [268] [270] [271] [272] [275] [277] [278] [102] [280] [282] [58] [287] [292] [295] [296] [334] [83] [276] [281] [324] [104] [289] [291] [297] [19] [301] [304] [305] [57] [306] [90] [307] [309] [310] [337] [79] [71] [196] [29] [73] [313] [69] [54] [39] [348] [50] [347] [37] [47] [46] [119] [34] [32] [97] [96] [72] [251] [33] [64] [265] [312] [42] [122] [328] [144] [331] [339] [207] [146] [317] [53] [41] [89] [70] [30] [314] [88] [234] [269] [130] [284] [43] [209] [95] [233] [121] [178]
86	Link/Node	[346] [342] [173] [114] [127] [180] [344] [330] [128] [183] [179] [184] [140] [177] [125] [135] [126] [110] [189] [341] [171] [111] [194] [198] [200] [188] [124] [195] [139] [136] [199] [204] [205] [333] [55] [211] [31] [214] [216] [215] [118] [113] [221] [222] [223] [225] [227] [213] [217] [228] [108] [91] [65] [241] [244] [66] [92] [112] [235] [252] [67] [278] [280] [282] [334] [300] [196] [315] [347] [340] [46] [119] [123] [326] [33] [193] [279] [323] [122] [328] [331] [317] [53] [30] [130] [121]
85	Dynamic stream	[349] [346] [342] [344] [186] [184] [140] [329] [125] [143] [135] [110] [189] [341] [174] [115] [171] [202] [205] [333] [31] [118] [113] [227] [332] [210] [170] [26] [107] [187] [239] [335] [253] [138] [240] [256] [263] [257] [101] [67] [325] [273] [274] [283] [286] [290] [103] [285] [100] [288] [293] [294] [299] [302] [303] [80] [98] [308] [311] [63] [82] [81] [61] [260] [315] [51] [49] [316] [326] [129] [322] [147] [319] [201] [279] [2] [94] [250] [230] [298] [266] [261] [343] [262] [229]
12	Trees	[346] [184] [192] [142] [185] [91] [65] [66] [321] [252] [57] [348]
0	Multidimensional tables	—
0	Geometry	—
0	Fields	—

PREPRINT

for network management," in *Virtual Reality Annual International Symposium, 1993., 1993 IEEE*, Sep 1993, pp. 55–61.

[47] H. Fuji, S. Nakai, H. Matoba, and H. Takano, "Real-time bifocal network-visualization," in *Network Operations and Management Symposium, 1994. Symposium Record., 1994 IEEE*, vol. 3, Feb 1994, pp. 867–876.

[48] S. E. Lamm, D. A. Reed, and W. H. Scullin, "Real-time geographic visualization of world wide web traffic," *Comput. Netw. ISDN Syst.*, vol. 28, no. 7-11, pp. 1457–1468, May 1996. [Online]. Available: http://dx.doi.org/10.1016/0169-7552(96)00055-4

[49] G. Parulkar, D. Schmidt, E. Kraemer, J. Turner, and A. Kantawala, "An architecture for monitoring, visualization, and control of gigabit networks," *Network, IEEE*, vol. 11, no. 5, pp. 34–43, Sep 1997.

[50] T. Munzner, E. Hoffman, K. Claffy, and B. Fenner, "Visualizing the global topology of the MBone," in *Information Visualization 96, Proceedings IEEE Symposium on*, Oct 1996, pp. 85–92, 129.

[51] T. Oetiker, "MRTG: The multi router traffic grapher," in *LISA*. USENIX, 1998, pp. 141–148. [Online]. Available: http://dblp.uni-trier.de/db/conf/lisa/lisa1998.html#Oetiker98

[52] E. Swing, "Flodar: flow visualization of network traffic," *Computer Graphics and Applications, IEEE*, vol. 18, no. 5, pp. 6–8, Sep 1998.

[53] L. Girardin and D. Brodbeck, "A visual approach for monitoring logs," in *Proceedings of the Twelfth Systems Administration Conference (LISA 98)*. Massachusetts, MA, USA: USENIX Association, 1998, pp. 299–308.

[54] L. Girardin, "An eye on network intruder-administrator shootouts," in *Proceedings of the Workshop on Intrusion Detection and Network Monitoring*. Berkeley, CA, USA: USENIX Association, 1999, pp. 19–28. [Online]. Available: http://dl.acm.org/citation.cfm?id=647593.728890

[55] B. Cheswick, H. Burch, and S. Branigan, "Mapping and visualizing the internet," in *In Proceedings of the 2000 USENIX Annual Technical Conference*, 2000, pp. 1–12.

[56] S. T. Teoh, K.-L. Ma, S. Wu, and X. Zhao, "Case study: Interactive visualization for internet security," in *Visualization, 2002. VIS 2002. IEEE*, Nov 2002, pp. 505–508.

[57] S. C. Au, C. Leckie, A. Parhar, and G. Wong, "Efficient visualization of large routing topologies," *Int. J. Netw. Manag.*, vol. 14, no. 2, pp. 105–118, Mar. 2004. [Online]. Available: http://dx.doi.org/10.1002/nem.511

[58] M. Lad, D. Massey, and L. Zhang, "Visualizing internet routing changes," *IEEE Transactions on Visualization and Computer Graphics*, vol. 12, no. 6, pp. 1450–1460, Nov. 2006. [Online]. Available: http://dx.doi.org/10.1109/TVCG.2006.108

[59] L. Xiao, J. Gerth, and P. Hanrahan, "Enhancing visual analysis of network traffic using a knowledge representation," in *IEEE SYMPOSIUM ONVISUAL ANALYTICS SCIENCE AND TECHNOLOGY*, 2006.

[60] P. Minarik and T. Dymacek, "NetFlow data visualization based on graphs," in *Proceedings of the 5th International Workshop on Visualization for Computer Security*, ser. VizSec '08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 144–151.

[61] A. Gubin, W. Yurcik, and L. Brumbaugh, "PingTV: A case study in visual network monitoring," in *Proceedings of the Conference on Visualization '01*, ser. VIS '01. Washington, DC, USA: IEEE Computer Society, 2001, pp. 421–424. [Online]. Available: http://dl.acm.org/citation.cfm?id=601671.601738

[62] ——, "Network management visualization with PingTV," in *Local Computer Networks, 2001. Proceedings. LCN 2001. 26th Annual IEEE Conference on*, 2001, pp. 62–63.

[63] L. Dimopoulou, E. Nikolouzou, P. Sampatakos, and I. Venieris, "QMTool: an XML-based management platform for QoS-aware IP networks," *Network, IEEE*, vol. 17, no. 3, pp. 8–14, May 2003.

Table XII
INFORMATION VISUALIZATION TAXONOMY - TOPIC: VISUALIZATION TECHNIQUE

Total	Subtopic	References of articles/papers
253	Standard 2D/3D displays	[172] [349] [346] [342] [173] [114] [127] [176] [180] [344] [330] [128] [183] [182] [179] [181] [184] [345] [318] [140] [329] [177] [125] [143] [135] [126] [110] [189] [341] [174] [115] [171] [111] [192] [194] [142] [198] [200] [320] [203] [188] [124] [190] [15] [195] [139] [136] [199] [204] [205] [208] [333] [211] [55] [31] [214] [216] [215] [118] [185] [219] [113] [221] [222] [223] [225] [133] [227] [137] [332] [212] [213] [217] [117] [134] [145] [224] [170] [228] [26] [231] [232] [107] [187] [48] [236] [108] [238] [91] [239] [65] [327] [241] [244] [245] [68] [246] [60] [248] [249] [66] [243] [321] [335] [92] [138] [235] [106] [255] [112] [240] [256] [175] [44] [52] [247] [105] [263] [336] [252] [59] [257] [101] [17] [67] [99] [264] [325] [267] [268] [270] [271] [272] [273] [274] [275] [277] [278] [102] [280] [282] [58] [287] [290] [292] [103] [295] [296] [334] [83] [276] [281] [324] [285] [104] [100] [288] [291] [293] [294] [299] [300] [19] [301] [302] [303] [304] [305] [57] [306] [90] [80] [98] [308] [309] [310] [311] [337] [71] [63] [82] [196] [29] [73] [81] [313] [61] [260] [69] [315] [54] [39] [348] [51] [49] [316] [50] [347] [37] [340] [47] [46] [119] [34] [32] [97] [96] [326] [72] [33] [322] [147] [319] [193] [201] [191] [64] [265] [279] [312] [323] [42] [122] [328] [144] [2] [94] [331] [339] [250] [230] [207] [146] [317] [53] [41] [89] [70] [298] [266] [30] [88] [234] [269] [130] [284] [43] [343] [95] [233] [262] [229] [121]
136	Icon-based displays	[172] [346] [344] [184] [318] [143] [135] [126] [110] [341] [115] [194] [197] [200] [320] [188] [124] [190] [15] [195] [136] [199] [204] [205] [208] [333] [211] [31] [214] [216] [215] [118] [109] [113] [223] [225] [137] [213] [117] [220] [224] [228] [26] [232] [237] [108] [91] [65] [244] [68] [248] [249] [66] [243] [335] [235] [256] [44] [247] [263] [254] [257] [17] [99] [272] [273] [274] [275] [102] [280] [283] [58] [287] [290] [292] [103] [296] [83] [276] [324] [104] [100] [293] [294] [299] [303] [305] [57] [90] [80] [311] [71] [63] [29] [73] [81] [313] [61] [260] [69] [54] [348] [49] [340] [47] [46] [119] [34] [32] [97] [326] [322] [201] [265] [122] [328] [2] [94] [331] [339] [250] [230] [123] [317] [53] [89] [30] [88] [284] [343] [95] [233] [262] [43] [229] [121]
62	Dense pixel displays	[125] [111] [194] [135] [15] [139] [136] [226] [137] [332] [210] [134] [237] [242] [243] [253] [235] [247] [263] [252] [254] [101] [99] [267] [272] [273] [277] [283] [286] [290] [292] [334] [83] [281] [285] [100] [289] [293] [297] [299] [19] [305] [306] [80] [307] [98] [308] [309] [310] [82] [29] [39] [340] [326] [251] [129] [2] [41] [298] [284] [95] [233]
36	Geometrically transformed displays	[172] [349] [176] [186] [135] [171] [338] [202] [206] [218] [131] [232] [238] [239] [254] [258] [101] [271] [283] [100] [288] [289] [293] [299] [307] [79] [82] [260] [347] [33] [144] [53] [314] [209] [233] [178]
21	Stacked displays	[172] [349] [184] [221] [213] [145] [228] [231] [87] [92] [105] [259] [264] [325] [93] [147] [250] [130] [261] [284] [262]

[64] J. Schönwälder, A. Pras, M. Harvan, J. Schippers, and R. van de Meent, "SNMP traffic analysis: Approaches, tools, and first results," in *Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on*, May 2007, pp. 323–332.

[65] E. Salvador and L. Granville, "An investigation of visualization techniques for SNMP traffic traces," in *Network Operations and Management Symposium, 2008. NOMS 2008. IEEE*, April 2008, pp. 887–890.

[66] ——, "Using visualization techniques for SNMP traffic analyses," in *Computers and Communications, 2008. ISCC 2008. IEEE Symposium on*, July 2008, pp. 806–811.

[67] A. Douitsis and D. Kalogeras, "Interactive network management visualization with SVG and AJAX," in *Proceedings of the 20th Conference on Large Installation System Administration*, ser. LISA '06. Berkeley, CA, USA: USENIX Association, 2006, pp. 19–19. [Online]. Available: http://dl.acm.org/citation.cfm?id=1267793.1267812

[68] R. De T.Valle, D. Passos, C. Albuquerque, and D. C. M. Saade, "Mesh Topology Viewer (MTV): an SVG-based interactive mesh network topology visualization tool," in *Computers and Communications, 2008. ISCC 2008. IEEE Symposium on*, July 2008, pp. 292–297.

[69] D. Estrin, M. Handley, J. Heidemann, S. McCanne, Y. Xu, and H. Yu, "Network visualization with nam, the VINT network animator," *Computer*, vol. 33, no. 11, pp. 63–68, Nov. 2000. [Online]. Available: http://dx.doi.org/10.1109/2.881696

[70] J. Brown, A. McGregor, and H.-W. Braun, "Network performance visualization: Insight through animation," 2000.

[71] C. M. Burns, J. Kuo, and S. Ng, "Ecological interface design: A new approach for visualizing network management," *Comput. Netw.*, vol. 43, no. 3, pp. 369–388, Oct. 2003. [Online]. Available: http://dx.doi.org/10.1016/S1389-1286(03)00287-1

[72] B. Yip, S. Goyette, and C. Madden, "Visualising internet traffic data with three-dimensional spherical display," in *Proceedings of the 2005 Asia-Pacific Symposium on Information Visualisation - Volume 45*, ser. APVis '05. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2005, pp. 153–158. [Online]. Available: http://dl.acm.org/citation.cfm?id=1082315.1082337

[73] R. Erbacher, K. Walker, and D. Frincke, "Intrusion and misuse detection in large-scale systems," *Computer Graphics and Applications, IEEE*, vol. 22, no. 1, pp. 38–47, Jan 2002.

[74] R. Erbacher, "Intrusion behavior detection through visualization," in *Systems, Man and Cybernetics, 2003. IEEE International Conference on*, vol. 3, Oct 2003, pp. 2507–2513 vol.3.

[75] R. F. Erbacher, "Glyph-based generic network visualization," in *Proc. SPIE Conference on Visualization and Data Analysis*, 2002, pp. 228–237.

[76] ——, "Visual behavior characterization for intrusion detection in large scale systems," 2001.

[77] ——, "Visual traffic monitoring and evaluation," in *in Proceedings of the Conference on Internet Performance and Control of Network Systems II*, 2001, pp. 153–160.

[78] R. Erbacher and D. Frincke, "Visualization in detection of intrusions and misuse in large scale networks," in *Information Visualization, 2000. Proceedings. IEEE International Conference on*, 2000, pp. 294–299.

[79] X. Yin, W. Yurcik, M. Treaster, Y. Li, and K. Lakkaraju, "VisFlowConnect: Netflow visualizations of link relationships for security situational awareness," in *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, ser. VizSEC/DMSEC '04. New York, NY, USA: ACM, 2004, pp. 26–34. [Online]. Available: http://doi.acm.org/10.1145/1029208.1029214

[80] K. Lakkaraju, W. Yurcik, and A. J. Lee, "NVisionIP: Netflow visualizations of system state for security situational awareness," in *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, ser. VizSEC/DMSEC '04. New York, NY, USA: ACM, 2004, pp. 65–72. [Online]. Available: http://doi.acm.org/10.1145/1029208.1029219

[81] K. Nyarko, T. Capers, C. Scott, and K. Ladeji-Osias, "Network intrusion visualization with NIVA, an intrusion detection visual analyzer with haptic integration," in *Haptic Interfaces for Virtual Environment and Teleoperator Systems, 2002. HAPTICS 2002. Proceedings. 10th Symposium on*, 2002, pp. 277–284.

[82] M. Stolze, R. Pawlitzek, and A. Wespi, "Visual problem-solving

IEEE PROOF

Table XIII
INFORMATION VISUALIZATION TAXONOMY - TOPIC: TASKS

Total	Subtopic	References of articles/papers
154	Overview	[172] [349] [346] [342] [173] [127] [176] [330] [128] [181] [184] [345] [140] [329] [125] [143] [126] [110] [189] [341] [174] [171] [194] [142] [135] [188] [124] [190] [15] [195] [136] [199] [202] [55] [214] [118] [218] [221] [222] [223] [225] [227] [137] [332] [212] [213] [134] [224] [145] [228] [26] [231] [232] [107] [108] [238] [91] [65] [60] [249] [243] [335] [92] [138] [106] [255] [112] [256] [175] [44] [247] [105] [336] [254] [257] [258] [101] [259] [67] [99] [264] [325] [268] [272] [278] [102] [280] [282] [283] [290] [292] [103] [296] [334] [83] [276] [100] [288] [293] [294] [297] [19] [301] [80] [98] [79] [196] [260] [69] [39] [348] [50] [340] [119] [34] [32] [97] [326] [72] [251] [322] [147] [323] [122] [328] [144] [2] [94] [331] [250] [123] [207] [146] [317] [53] [41] [89] [70] [298] [30] [88] [269] [130] [261] [284] [343] [209] [95] [233] [262] [43] [229] [121] [178]
116	Filter/Interactive Filtering	[172] [349] [346] [342] [173] [176] [330] [140] [143] [189] [171] [135] [203] [188] [124] [136] [199] [202] [214] [118] [218] [221] [137] [332] [212] [217] [228] [231] [187] [91] [327] [241] [48] [60] [249] [243] [335] [92] [138] [255] [112] [175] [247] [105] [240] [175] [44] [52] [254] [257] [257] [258] [101] [259] [99] [325] [272] [278] [102] [280] [290] [83] [100] [293] [297] [98] [79] [196] [260] [50] [340] [347] [340] [119] [97] [322] [147] [122] [328] [144] [94] [331] [250] [230] [146] [53] [41] [89] [30] [88] [130] [261] [146] [185] [317] [53] [41] [89] [70] [298] [266] [30] [314] [88] [234] [269] [130] [261] [343] [209] [95] [233] [262] [43] [229] [121]
105	Zoom/Interactive Zooming	[172] [346] [342] [127] [181] [184] [345] [329] [125] [126] [110] [194] [142] [135] [188] [190] [118] [222] [223] [225] [227] [137] [212] [213] [134] [224] [145] [231] [232] [107] [108] [238] [91] [245] [243] [138] [106] [112] [256] [44] [247] [105] [336] [254] [257] [101] [259] [67] [99] [264] [268] [278] [280] [282] [283] [290] [292] [103] [296] [334] [83] [276] [100] [288] [293] [297] [19] [301] [80] [79] [196] [260] [69] [39] [348] [50] [340] [34] [32] [326] [72] [251] [147] [323] [122] [144] [2] [94] [331] [250] [230] [123] [207] [146] [41] [89] [70] [88] [269] [261] [209] [95] [233] [43] [121]
33	Moving/Rotate	[172] [26] [48] [176] [176] [144] [143] [50] [98] [290] [324] [19] [134] [270] [106] [94] [257] [271] [278] [255] [72] [291] [137] [175] [334] [260] [340] [323] [123] [70] [284] [43] [178]
32	Details-on-demand	[346] [342] [174] [203] [135] [222] [223] [107] [60] [138] [292] [83] [281] [100] [288] [293] [294] [98] [260] [340] [32] [119] [323] [2] [250] [123] [53] [41] [88] [284] [233] [262]
18	Linking and Brushing	[171] [135] [145] [243] [340] [122] [328] [144] [2] [94] [339] [250] [230] [317] [298] [88] [209] [233]
14	Relate	[172] [342] [171] [199] [243] [336] [334] [196] [340] [119] [331] [43] [121] [178]
1	History	[240]
1	Extract	[209]

support for new event triage in centralized network security monitoring: Challenges, tools and benefits," in *IMF*, ser. LNI, J. Nedon, S. Frings, and O. Göbel, Eds., vol. 39. GI, 2003, pp. 0–. [Online]. Available: http://dblp.uni-trier.de/db/conf/sidar/sidar2003.html#StolzePW03

[83] K. Abdullah, C. Lee, G. Conti, J. Copeland, and J. Stasko, "IDS RainStorm: visualizing IDS alarms," in *Visualization for Computer Security, 2005. (VizSEC 05). IEEE Workshop on*, Oct 2005, pp. 1–10.

[84] W. Yurcik, J. Barlow, K. Lakkaraju, and M. Haberman, "Two visual computer network security monitoring tools incorporating operator interface requirements," in *In ACM CHI Workshop on Human-Computer Interaction and Security Systems (HCISEC*, 2003.

[85] R. Bearavolu, K. Lakkaraju, W. Yurcik, and H. Raje, "A visualization tool for situational awareness of tactical and strategic security events on large and complex computer networks," in *Military Communications Conference, 2003. MILCOM '03. 2003 IEEE*, vol. 2, Oct 2003, pp. 850–855 Vol.2.

[86] W. Yurcik, K. Lakkaraju, J. Barlow, and J. Rosendale, "A prototype tool for visual data mining of network traffic for intrusion detection," in *In Proceedings of the ICDM Workshop on Data Mining for Computer Security (DMSEC?03*, 2003.

[87] F. Fischer, F. Mansmann, D. A. Keim, S. Pietzko, and M. Waldvogel, "Large-scale network monitoring for visual analysis of attacks," in *Proceedings of the 5th International Workshop on Visualization for Computer Security*, ser. VizSec '08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 111–118.

[88] D. Phan, J. Gerth, M. Lee, A. Paepcke, and T. Winograd, "Visual analysis of network flow data with timelines and event plots," in *VizSEC*, ser. Mathematics and Visualization, J. R. Goodall, G. J. Conti, and K.-L. Ma, Eds. Springer, 2007, pp. 85–99. [Online]. Available: http://dblp.uni-trier.de/db/conf/vizsec/vizsec2007.html#PhanGLPW07

[89] S. Noel, M. Jacobs, P. Kalapa, and S. Jajodia, "Multiple coordinated views for network attack graphs," in *Visualization for Computer Security, 2005. (VizSEC 05). IEEE Workshop on*, Oct 2005, pp. 99–106.

[90] S. Noel and S. Jajodia, "Managing attack graph complexity through visual hierarchical aggregation," in *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, ser. VizSEC/DMSEC '04. New York, NY, USA: ACM, 2004, pp. 109–118. [Online]. Available: http://doi.acm.org/10.1145/1029208.1029225

[91] S. O'Hare, S. Noel, and K. Prole, "A graph-theoretic visualization approach to network risk analysis," in *VizSEC*, 2008, pp. 60–67.

[92] L. Williams, R. Lippmann, and K. Ingols, "An interactive attack graph cascade and reachability display," in *VizSEC*, 2007, pp. 221–236.

[93] ——, "GARNET: A graphical attack graph and reachability network evaluation tool," in *VizSEC*, ser. Lecture Notes in Computer Science, J. R. Goodall, G. J. Conti, and K.-L. Ma, Eds., vol. 5210. Springer, 2008, pp. 44–59. [Online]. Available: http://dblp.uni-trier.de/db/conf/vizsec/vizsec2008.html#WilliamsLI08

[94] E. Bertini, P. Hertzog, and D. Lalanne, "SpiralView: Towards security policies assessment through visual correlation of network resources with evolution of alarms," in *Visual Analytics Science and Technology, 2007. VAST 2007. IEEE Symposium on*, Oct 2007, pp. 139–146.

[95] W. Xu, M. Shehab, and G.-J. Ahn, "Visualization based policy analysis: Case study in SELinux," in *Proceedings of the 13th ACM Symposium on Access Control Models and Technologies*, ser. SACMAT '08. New York, NY, USA: ACM, 2008, pp. 165–174. [Online]. Available: http://doi.acm.org/10.1145/1377836.1377863

[96] "MieLog: A highly interactive visual log browser using information visualization and statistical analysis," in *Proceedings of the 16th USENIX Conference on System Administration*, ser. LISA '02. Berkeley, CA, USA: USENIX Association, 2002, pp. 133–144. [Online]. Available: http://dl.acm.org/citation.cfm?id=1050517.1050532

[97] T. Takada and H. Koike, "Tudumi: information visualization system for monitoring and auditing computer logs," in *Information Visualisation, 2002. Proceedings. Sixth International Conference on*, 2002, pp. 570–576.

[98] J. McPherson, K.-L. Ma, P. Krystosk, T. Bartoletti, and M. Christensen, "PortVis: A tool for port-based detection of security events," in *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, ser. VizSEC/DMSEC '04. New York, NY, USA: ACM, 2004, pp. 73–81. [Online]. Available: http://doi.acm.org/10.1145/1029208.1029220

[99] C. Muelder, K.-L. Ma, and T. Bartoletti, "Interactive visualization

PREPRINT

for network and port scan detection," in *Proceedings of the 8th International Conference on Recent Advances in Intrusion Detection*, ser. RAID'05. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 265–283.

[100] J. Goodall, W. Lutters, P. Rheingans, and A. Komlodi, "Preserving the big picture: visual network traffic analysis with TNV," in *Visualization for Computer Security, 2005. (VizSEC 05). IEEE Workshop on*, Oct 2005, pp. 47–54.

[101] ——, "Focusing on context in network traffic analysis," *Computer Graphics and Applications, IEEE*, vol. 26, no. 2, pp. 72–80, March 2006.

[102] S. Foresti, J. Agutter, Y. Livnat, S. Moon, and R. Erbacher, "Visual correlation of network alerts," *Computer Graphics and Applications, IEEE*, vol. 26, no. 2, pp. 48–59, March 2006.

[103] Y. Livnat, J. Agutter, S. Moon, R. Erbacher, and S. Foresti, "A visualization paradigm for network intrusion detection," in *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC*, June 2005, pp. 92–99.

[104] T. Arvanitis, C. Constantinou, A. Stepanenko, Y. Sun, B. Liu, and K. Baughan, "Network visualisation and analysis tool based on logical network abridgment," in *Military Communications Conference, 2005. MILCOM 2005. IEEE*, Oct 2005, pp. 106–112 Vol. 1.

[105] F. Mansmann, D. Keim, S. North, B. Rexroad, and D. Sheleheda, "Visual analysis of network traffic for resource planning, interactive monitoring, and interpretation of security threats," *Visualization and Computer Graphics, IEEE Transactions on*, vol. 13, no. 6, pp. 1105–1112, Nov 2007.

[106] W. Wang and A. Lu, "Interactive wormhole detection and evaluation," *Information Visualization*, vol. 6, no. 1, pp. 3–17, Mar. 2007. [Online]. Available: http://dx.doi.org/10.1057/palgrave.ivs.9500144

[107] R. Hofstede and T. Fioreze, "SURFmap: A network monitoring tool based on the Google Maps API," in *Integrated Network Management, 2009. IM '09. IFIP/IEEE International Symposium on*, June 2009, pp. 676–690.

[108] P. Dobrev, S. Stancu-Mara, and J. Schönwälder, "Visualization of node interaction dynamics in network traces," in *AIMS*, 2009, pp. 147–160.

[109] S. Lee and H. Kim, "Correlation, visualization, and usability analysis of routing policy configurations," *Network and Service Management, IEEE Transactions on*, vol. 7, no. 1, pp. 28–41, March 2010.

[110] S. Papadopoulos, K. Moustakas, and D. Tzovaras, "Hierarchical visualization of BGP routing changes using entropy measures," in *ISVC (2)*, ser. Lecture Notes in Computer Science, G. Bebis, R. Boyle, B. Parvin, D. Koracin, C. Fowlkes, S. Wang, M.-H. Choi, S. Mantler, J. P. Schulze, D. Acevedo, K. Mueller, and M. E. Papka, Eds., vol. 7432. Springer, 2012, pp. 696–705. [Online]. Available: http://dblp.uni-trier.de/db/conf/isvc/isvc2012-2.html#PapadopoulosMT12

[111] V. Ramachandran and D. Street, "Pathsift: A library for separating the effects of topology, policy, and protocols on IP routing," in *Proceedings of the 5th International ICST Conference on Simulation Tools and Techniques*, ser. SIMUTOOLS '12. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012, pp. 65–74. [Online]. Available: http://dl.acm.org/citation.cfm?id=2263019.2263028

[112] Z. Bi, "An integrated environment for visualization of distributed wireless sensor networks," in *Control and Automation (ICCA), 2013 10th IEEE International Conference on*, June 2013, pp. 312–317.

[113] L. Ma, L. Wang, L. Shu, J. Zhao, S. Li, Z. Yuan, and N. Ding, "NetViewer: A universal visualization tool for wireless sensor networks," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, Dec 2010, pp. 1–5.

[114] Y. Kumata and A. Koyama, "Mesh Net Viewer: A visualization system for wireless mesh networks," in *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2013 Eighth International Conference on*, Oct 2013, pp. 80–87.

[115] R. Riggio, M. Gerola, A. Francescon, A. Zanardi, T. Rasheed, and F. Jan, "Network topology visualization and monitoring for multi-hop wireless networks," *Broadband Communications, Networks, and Systems*, vol. 66, pp. 435–449, 2012.

[116] ——, "Network topology visualization and monitoring for multi-hop wireless networks," in *Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on*, May 2011, pp. 856–870.

[117] T. Qiu, Z. Ge, D. Pei, J. Wang, and J. Xu, "What happened in my network: Mining network events from router syslogs," in *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*, ser. IMC '10. New York, NY, USA: ACM, 2010, pp. 472–484. [Online]. Available: http://doi.acm.org/10.1145/1879141.1879202

[118] H. Wang, "From a mess to graphic maps: Visualization of large-scale heterogeneous networks," in *Computer Modeling and Simulation, 2010. ICCMS '10. Second International Conference on*, vol. 1, Jan 2010, pp. 531–535.

[119] Q. Liao, A. Blaich, D. VanBruggen, and A. Striegel, "Managing networks through context: Graph visualization and exploration," *Comput. Netw.*, vol. 54, no. 16, pp. 2809–2824, Nov. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.07.015

[120] Q. Liao, A. Blaich, A. Striegel, and D. Thain, "ENAVis: Enterprise network activities visualization," in *LISA*, M. Obejas, Ed. USENIX Association, 2008, pp. 59–74. [Online]. Available: http://dblp.uni-trier.de/db/conf/lisa/lisa2008.html#LiaoBST08

[121] Q. Liao, A. Striegel, and N. Chawla, "Visualizing graph dynamics and similarity for enterprise network security and management," in *Proceedings of the Seventh International Symposium on Visualization for Cyber Security*, ser. VizSec '10. New York, NY, USA: ACM, 2010, pp. 34–45. [Online]. Available: http://doi.acm.org/10.1145/1850795.1850799

[122] P. Barbosa and L. Granville, "Interactive SNMP traffic analysis through information visualization," in *Network Operations and Management Symposium (NOMS), 2010 IEEE*, April 2010, pp. 73–79.

[123] C. Bartolini, C. Stefanelli, D. Targa, and M. Tortonesi, "A web-based what-if scenario analysis tool for performance improvement of IT support organizations," in *Network and Service Management (CNSM), 2011 7th International Conference on*, Oct 2011, pp. 1–5.

[124] S. Kamamura, Y. Koizumi, T. Miyamura, S. Arakawa, K. Shiomoto, and M. Murata, "Control and visualization system for managed self-organization network," in *Network and Service Management (CNSM), 2011 7th International Conference on*, Oct 2011, pp. 1–4.

[125] U. Sedlar, M. Volk, J. Sterle, A. Kos, and R. Sernec, "Contextualized monitoring and root cause discovery in IPTV systems using data visualization," *Network, IEEE*, vol. 26, no. 6, pp. 40–46, November 2012.

[126] D. S. Kim, M. Ito, S. Komorita, Y. Kitatsuji, and H. Yokota, "Design and implementation of a network management system for service oriented network," in *World Telecommunications Congress (WTC), 2012*, March 2012, pp. 1–6.

[127] N. Tateishi, M. Tahara, N. Tanji, and H. Seshake, "Method for visualizing information from large-scale carrier networks," in *Network Operations and Management Symposium (APNOMS), 2013 15th Asia-Pacific*, Sept 2013, pp. 1–6.

[128] Y. Himura and Y. Yasuda, "Static validation of network device configurations in virtualized multi-tenant datacenters," in *Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on*, May 2013, pp. 160–168.

[129] l. Herrero, E. Corchado, M. A. Pellicer, and A. Abraham, "MOVIH-IDS: A mobile-visualization hybrid intrusion detection system," *Neurocomputing*, vol. 72, no. 13-15, pp. 2775–2784, 2009. [Online]. Available: http://dblp.uni-trier.de/db/journals/ijon/ijon72.html#HerreroCPA09

[130] F. Mansmann, F. Fischer, D. A. Keim, and S. C. North, "Visual support for analyzing network traffic and intrusion detection events using treemap and graph representations," in *Proceedings of the Symposium on Computer Human Interaction for the Management of Information Technology*, ser. CHiMiT '09. New York, NY, USA: ACM, 2009, pp. 3:19–3:28. [Online]. Available: http://doi.acm.org/10.1145/1641587.1641590

[131] H. Choi, H. Lee, and H. Kim, "Fast detection and visualization of network attacks on parallel coordinates," *Computers & Security*, vol. 28, no. 5, pp. 276–288, 2009.

[132] H. Choi and H. Lee, "PCAV: Internet attack visualization on parallel coordinates," in *Proceedings of the 7th International Conference on Information and Communications Security*, ser. ICICS'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 454–466.

[133] M. Celenk, T. Conley, J. Willis, and J. Graham, "Predictive network anomaly detection and visualization," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 2, pp. 288–299, June 2010.

[134] T. Taylor, D. Paterson, J. Glanfield, C. Gates, S. Brooks, and J. McHugh, "FloVis: Flow visualization system," in *Conference For Homeland Security, 2009. CATCH '09. Cybersecurity Applications Technology*, March 2009, pp. 186–198.

[135] C. Kintzel, J. Fuchs, and F. Mansmann, "Monitoring large IP spaces with ClockView," in *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, ser. VizSec '11. New York, NY, USA: ACM, 2011, pp. 2:1–2:10. [Online]. Available: http://doi.acm.org/10.1145/2016904.2016906

PREPRINT

[136] A. Boschetti, L. Salgarelli, C. Muelder, and K.-L. Ma, "TVi: A visual querying system for network monitoring and anomaly detection," in *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, ser. VizSec '11. New York, NY, USA: ACM, 2011, pp. 1:1–1:10. [Online]. Available: http://doi.acm.org/10.1145/2016904.2016905

[137] D. M. Best, S. Bohn, D. Love, A. Wynne, and W. A. Pike, "Real-time visualization of network behaviors for situational awareness," in *Proceedings of the Seventh International Symposium on Visualization for Cyber Security*, ser. VizSec '10. New York, NY, USA: ACM, 2010, pp. 79–90. [Online]. Available: http://doi.acm.org/10.1145/1850795.1850805

[138] P. McLachlan, T. Munzner, E. Koutsofios, and S. North, "LiveRAC: Interactive visual exploration of system management time-series data," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '08. New York, NY, USA: ACM, 2008, pp. 1483–1492. [Online]. Available: http://doi.acm.org/10.1145/1357054.1357286

[139] A. Lu, W. Wang, A. Dnyate, and X. Hu, "Sybil attack detection through global topology pattern visualization," *Information Visualization*, vol. 10, no. 1, pp. 32–46, Jan. 2011. [Online]. Available: http://dx.doi.org/10.1057/ivs.2010.1

[140] Y. Zhao, F. Zhou, and X. Fan, "A real-time visualization framework for IDS alerts," in *Proceedings of the 5th International Symposium on Visual Information Communication and Interaction*, ser. VINCI '12. New York, NY, USA: ACM, 2012, pp. 11–17. [Online]. Available: http://doi.acm.org/10.1145/2397696.2397698

[141] Y. Zhao, F. Zhou, X. Fan, X. Liang, and Y. Liu, "IDSRadar: a real-time visualization framework for IDS alerts," *Science China Information Sciences*, vol. 56, no. 8, pp. 1–12, 2013.

[142] F. Mansmann, T. Göbel, and W. Cheswick, "Visual analysis of complex firewall configurations," in *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*, ser. VizSec '12. New York, NY, USA: ACM, 2012, pp. 1–8. [Online]. Available: http://doi.acm.org/10.1145/2379690.2379691

[143] D. Inoue, M. Eto, K. Suzuki, M. Suzuki, and K. Nakao, "DAEDALUS-VIZ: Novel real-time 3d visualization for darknet monitoring-based alert system," in *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*, ser. VizSec '12. New York, NY, USA: ACM, 2012, pp. 72–79. [Online]. Available: http://doi.acm.org/10.1145/2379690.2379700

[144] T. Nunnally, P. Chi, K. Abdullah, A. Uluagac, J. Copeland, and R. Beyah, "P3D: A parallel 3d coordinate visualization for advanced network scans," in *Communications (ICC), 2013 IEEE International Conference on*, June 2013, pp. 2052–2057.

[145] L. Harrison, R. Spahn, M. Iannacone, E. Downing, and J. R. Goodall, "NV: Nessus vulnerability visualization for the web," in *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*, ser. VizSec '12. New York, NY, USA: ACM, 2012, pp. 25–32. [Online]. Available: http://doi.acm.org/10.1145/2379690.2379694

[146] L. Hao, C. G. Healey, and S. E. Hutchinson, "Flexible web visualization for alert-based network security analytics," in *Proceedings of the Tenth Workshop on Visualization for Cyber Security*, ser. VizSec '13. New York, NY, USA: ACM, 2013, pp. 33–40. [Online]. Available: http://doi.acm.org/10.1145/2517957.2517962

[147] F. Fischer, J. Fuchs, F. Mansmann, and D. A. Keim, "BANKSAFE: Visual analytics for big data in large-scale computer networks," *Information Visualization*, 2013.

[148] ——, "BANKSAFE: A visual situational awareness tool for large-scale computer networks," in *Proceedings of the 2012 IEEE Conference on Visual Analytics Science and Technology (VAST)*, ser. VAST '12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 257–258. [Online]. Available: http://dx.doi.org/10.1109/VAST.2012.6400528

[149] A. Gort and J. Gort, "Survey of Network Visualization Tools," Defence R&D Canada-DRDC - CONTRACT REPORT, Dec. 2007.

[150] R. Marty, *Applied Security Visualization*, 1st ed. Addison-Wesley Professional, 2008.

[151] D. A. Keim, A. Pras, J. Schönwälder, P. C. Wong, and F. Mansmann, "Report on the Dagstuhl seminar on visualization and monitoring of network traffic," *J. Netw. Syst. Manage.*, vol. 18, no. 2, pp. 232–236, Jun. 2010.

[152] "Network and Services Management Taxonomy," Dec. 2013. [Online]. Available: http://sites.ieee.org/tc-cnom/resources/taxonomy/

[153] B. A. Price, R. Baecker, and I. S. Small, "A principled taxonomy of software visualization," *J. Vis. Lang. Comput.*, vol. 4, no. 3, pp. 211–266, 1993. [Online]. Available: http://dblp.uni-trier.de/db/journals/vlc/vlc4.html#PriceBS93

[154] B. Lee, C. Plaisant, C. S. Parr, J.-D. Fekete, and N. Henry, "Task taxonomy for graph visualization," in *Proceedings of the 2006 AVI Workshop on BEyond Time and Errors: Novel Evaluation Methods for Information Visualization*, ser. BELIV '06. New York, NY, USA: ACM, 2006, pp. 1–5. [Online]. Available: http://doi.acm.org/10.1145/1168149.1168168

[155] E. H. Chi, "A taxonomy of visualization techniques using the data state reference model," in *Information Visualization, 2000. InfoVis 2000. IEEE Symposium on*, 2000, pp. 69–75.

[156] D. A. Keim, "Information visualization and visual data mining," *IEEE Transactions on Visualization and Computer Graphics*, vol. 8, no. 1, pp. 1–8, Jan. 2002. [Online]. Available: http://dx.doi.org/10.1109/2945.981847

[157] T. Munzner, *Visualization Analysis and Design*, ser. AK Peters Visualization Series. CRC Press, 2014.

[158] G. Inc., "Gartner's hype cycle special report for 2014," 2014. [Online]. Available: http://www.gartner.com/technology/research/hype-cycles/

[159] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the Internet of Things: A survey," *Communications Surveys Tutorials, IEEE*, vol. 16, no. 1, pp. 414–454, First 2014.

[160] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013. [Online]. Available: http://dx.doi.org/10.1016/j.future.2013.01.010

[161] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.05.010

[162] H. Hu, Y. Wen, T.-S. Chua, and X. Li, "Toward scalable systems for big data analytics: A technology tutorial," *Access, IEEE*, vol. 2, pp. 652–687, 2014.

[163] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Gener. Comput. Syst.*, vol. 25, no. 6, pp. 599–616, Jun. 2009.

[164] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *J. Internet Services and Applications*, vol. 1, no. 1, pp. 7–18, 2010. [Online]. Available: http://dblp.uni-trier.de/db/journals/jisa/jisa1.html#ZhangCB10

[165] B. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks," *Communications Surveys Tutorials, IEEE*, vol. 16, no. 3, pp. 1617–1634, Third 2014.

[166] O. N. Foundation. (2014) Software-defined networking (SDN) definition. [Online]. Available: https://www.opennetworking.org/

[167] C. Freitas, M. Pimenta, and D. Scapin, "User-centered evaluation of information visualization techniques: Making the HCI-InfoVis connection explicit," in *Handbook of Human Centric Visualization*, W. Huang, Ed. Springer New York, 2014, pp. 315–336.

[168] S. Foresti and J. Agutter, "VisAlert: From idea to product," in *VizSEC*, ser. Mathematics and Visualization, J. R. Goodall, G. J. Conti, and K.-L. Ma, Eds. Springer, 2007, pp. 159–174. [Online]. Available: http://dblp.uni-trier.de/db/conf/vizsec/vizsec2007.html#ForestiA07

[169] J. Stoll, D. McColgin, M. Gregory, V. Crow, and W. K. Edwards, "Adapting personas for use in security visualization design," in *VizSEC*, ser. Mathematics and Visualization, J. R. Goodall, G. J. Conti, and K.-L. Ma, Eds. Springer, 2007, pp. 39–52. [Online]. Available: http://dblp.uni-trier.de/db/conf/vizsec/vizsec2007.html#StollMGCE07

[170] D. Plonka, "FlowScan: A network traffic flow reporting and visualization tool," in *Proceedings of the 14th USENIX Conference on System Administration*, ser. LISA '00. Berkeley, CA, USA: USENIX Association, 2000, pp. 305–318. [Online]. Available: http://dl.acm.org/citation.cfm?id=1045502.1045522

[171] S. Papadopoulos, G. Theodoridis, and D. Tzovaras, "BGPfuse: Using visual feature fusion for the detection and attribution of BGP anomalies," in *Proceedings of the Tenth Workshop on Visualization for Cyber Security*, ser. VizSec '13. New York, NY, USA: ACM, 2013, pp. 57–64. [Online]. Available: http://doi.acm.org/10.1145/2517957.2517965

[172] T. R. Leschke and C. Nicholas, "Change-link 2.0: A digital forensic tool for visualizing changes to shadow volume data," in *Proceedings of the Tenth Workshop on Visualization for Cyber Security*, ser. VizSec '13. New York, NY, USA: ACM, 2013, pp. 17–24. [Online]. Available: http://doi.acm.org/10.1145/2517957.2517960

[173] C. Humphries, N. Prigent, C. Bidan, and F. Majorczyk, "ELVIS: Extensible Log VISualization," in *Proceedings of the Tenth Workshop on Visualization for Cyber Security*, ser. VizSec '13. New

PREPRINT

York, NY, USA: ACM, 2013, pp. 9–16. [Online]. Available: http://doi.acm.org/10.1145/2517957.2517959

[174] W. Zhuo and Y. Nadji, "MalwareVis: entity-based visualization of malware network traces," in *VizSEC*, 2012, pp. 41–47.

[175] F. Stoffel, F. Fischer, and D. A. Keim, "Finding anomalies in time-series using visual correlation for interactive root cause analysis," in *Proceedings of the Tenth Workshop on Visualization for Cyber Security*, ser. VizSec '13. New York, NY, USA: ACM, 2013, pp. 65–72. [Online]. Available: http://doi.acm.org/10.1145/2517957.2517966

[176] T. Nunnally, K. Abdullah, A. S. Uluagac, J. A. Copeland, and R. Beyah, "NAVSEC: A recommender system for 3d network security visualizations," in *Proceedings of the Tenth Workshop on Visualization for Cyber Security*, ser. VizSec '13. New York, NY, USA: ACM, 2013, pp. 41–48. [Online]. Available: http://doi.acm.org/10.1145/2517957.2517963

[177] O. Tsigkas and D. Tzovaras, "Analysis of rogue anti-virus campaigns using hidden structures in k-partite graphs," in *Cryptology and Network Security*, ser. Lecture Notes in Computer Science, J. Pieprzyk, A.-R. Sadeghi, and M. Manulis, Eds. Springer Berlin Heidelberg, 2012, vol. 7712, pp. 114–125.

[178] Y. Okada, "Network data visualization using parallel coordinates version of time-tunnel with 2Dto2D visualization for intrusion detection," in *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on*, March 2013, pp. 1088–1093.

[179] E. Glatz, S. Mavromatidis, B. Ager, and X. Dimitropoulos, "Visualizing big network traffic data using frequent pattern mining and hypergraphs," *Computing*, vol. 96, no. 1, pp. 27–38, Jan. 2014.

[180] J. Chen, "Real-time network security situation visualization and threat assessment based on semi-Markov process," vol. 8784, 2013, pp. 87 840A–87 840A–9. [Online]. Available: http://dx.doi.org/10.1117/12.2013675

[181] A. Muallem, S. Shetty, and S. Hargrove, "Visualizing geolocation of spam email," in *Computing, Communications and IT Applications Conference (ComComAp), 2013*, April 2013, pp. 63–68.

[182] R. Sánchez, l. Herrero, and E. Corchado, "Visualization and clustering for SNMP intrusion detection," *Cybern. Syst.*, vol. 44, no. 6-7, pp. 505–532, Oct. 2013. [Online]. Available: http://dx.doi.org/10.1080/01969722.2013.803903

[183] M. Hruby, M. Olsovsky, and M. Kotocova, "Traffic flow optimization and visualization in MPLS networks," in *Proceedings of the World Congress on Engineering*, vol. 2, 2013.

[184] M. Alsaleh, A. Alqahtani, A. Alarifi, and A. Al-Salman, "Visualizing PHPIDS log files for better understanding of web server attacks," in *Proceedings of the Tenth Workshop on Visualization for Cyber Security*, ser. VizSec '13. New York, NY, USA: ACM, 2013, pp. 1–8. [Online]. Available: http://doi.acm.org/10.1145/2517957.2517958

[185] P. Li, L. Ning, and Z. Xiaochao, "Visualization framework for inter-domain access control policy integration," *Communications, China*, vol. 10, no. 3, pp. 67–75, March 2013.

[186] J. Cho, H. Lee, K. Choi, S. Nam, and J. Moon, "Visualization of abnormal behavior detection using parallel coordinate and correspondence analysis," *International Journal of Information*, vol. 15, no. 2, pp. 2741–1749, 2012.

[187] T. T. Dang and T. K. Dang, "Visualization of web form submissions for security analysis," *IJWIS*, vol. 9, no. 2, pp. 165–180, 2013. [Online]. Available: http://dblp.uni-trier.de/db/journals/ijwis/ijwis9.html#DangD13a

[188] F. Roveta, G. Caviglia, L. Di Mario, S. Zanero, F. Maggi, and P. Ciuccarelli, "BURN: Baring Unknown Rogue Networks," in *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, ser. VizSec '11. New York, NY, USA: ACM, 2011, pp. 6:1–6:10. [Online]. Available: http://doi.acm.org/10.1145/2016904.2016910

[189] Q. Liao and A. Striegel, "Intelligent network management using graph differential anomaly visualization," in *Network Operations and Management Symposium (NOMS), 2012 IEEE*, April 2012, pp. 1008–1014.

[190] W. Urbanski, M. Dunlop, R. Marchany, and J. Tront, "Cover-VT: Converged security visualization tool," in *Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on*, May 2011, pp. 714–717.

[191] A. E.-D. Riad, I. Elhenawy, A. Hassan, and N. Awadallah, "Data visualization technique framework for intrusion detection," *International Journal of Computer Science Issues (IJCSI)*, vol. 8, no. 5, 2011.

[192] U.-H. Kim, J.-M. Kang, J.-S. Lee, H.-S. Kim, and S.-Y. Jung, "Practical firewall policy inspection using anomaly detection and its visualization," *Multimedia Tools Appl.*, vol. 71, no. 2, pp. 627–641, Jul. 2014.

[193] H. Yan, "The study on network topology discovery algorithm based on SNMP protocol and ICMP protocol," in *Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on*, June 2012, pp. 665–668.

[194] F. Fischer, J. Fuchs, P.-A. Vervier, F. Mansmann, and O. Thonnard, "VisTracer: A visual analytics tool to investigate routing anomalies in traceroutes," in *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*, ser. VizSec '12. New York, NY, USA: ACM, 2012, pp. 80–87. [Online]. Available: http://doi.acm.org/10.1145/2379690.2379701

[195] S. Togawa, K. Kanenishi, and Y. Yano, "Peer-to-peer file sharing communication detection using spherical SOM visualization for network management," in *Proceedings of the 2011 International Conference on Human Interface and the Management of Information - Volume Part I*, ser. HI'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 259–267. [Online]. Available: http://dl.acm.org/citation.cfm?id=2027916.2027949

[196] O. Tsigkas, O. Thonnard, and D. Tzovaras, "Visual spam campaigns analysis using abstract graphs representation," in *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*, ser. VizSec '12. New York, NY, USA: ACM, 2012, pp. 64–71. [Online]. Available: http://doi.acm.org/10.1145/2379690.2379699

[197] R. F. Erbacher, "Visualization design for immediate high-level situational assessment," in *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*, ser. VizSec '12. New York, NY, USA: ACM, 2012, pp. 17–24. [Online]. Available: http://doi.acm.org/10.1145/2379690.2379693

[198] Y. Guozheng, L. Yuliang, and C. Huixian, "A new network topology visualization algorithm," in *Instrumentation, Measurement, Computer, Communication and Control, 2011 First International Conference on*, Oct 2011, pp. 369–372.

[199] M. L. Huang, J. Zhang, Q. V. Nguyen, and J. Wang, "Visual clustering of spam emails for DDoS analysis," in *Information Visualisation (IV), 2011 15th International Conference on*, July 2011, pp. 65–72.

[200] C.-S. Chao and S. J.-H. Yang, "A novel three-tiered visualization approach for firewall rule validation," *J. Vis. Lang. Comput.*, vol. 22, no. 6, pp. 401–414, Dec. 2011. [Online]. Available: http://dx.doi.org/10.1016/j.jvlc.2011.07.002

[201] Y. Tsukahara, T. Tomine, and K. Sugiura, "Acquisition and visualization of hosts connected to the network," in *Applications and the Internet (SAINT), 2011 IEEE/IPSJ 11th International Symposium on*, July 2011, pp. 421–426.

[202] S. Tricaud, K. Nance, and P. Saadé, "Visualizing network activity using parallel coordinates," in *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, Jan 2011, pp. 1–8.

[203] D. Best, R. Hafen, B. Olsen, and W. Pike, "Atypical behavior identification in large-scale network traffic," in *Large Data Analysis and Visualization (LDAV), 2011 IEEE Symposium on*, Oct 2011, pp. 15–22.

[204] J. Joseph and A. Ghorbani, "VisVerND: Visual verification of network traffic dataset," in *Communication Networks and Services Research Conference (CNSR), 2011 Ninth Annual*, May 2011, pp. 56–62.

[205] C. So-In, C. Netphakdee, K. Wijitsopon, C. Panichayanubal, and P. Seresangtakul, "Web-based automatic network discovery/Map Systems," in *Computer Applications and Industrial Electronics (ICCAIE), 2011 IEEE International Conference on*, Dec 2011, pp. 416–421.

[206] L. Fu Lu, J. Wan Zhang, M. Lin Huang, and L. Fu, "A new concentric-circle visualization of multi-dimensional data and its application in network security," *J. Vis. Lang. Comput.*, vol. 21, no. 4, pp. 194–208, Aug. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.jvlc.2010.05.002

[207] S. Mukosaka and H. Koike, "Integrated visualization system for monitoring security in large-scale local area network," in *Visualization, 2007. APVIS '07. 2007 6th International Asia-Pacific Symposium on*, Feb 2007, pp. 41–44.

[208] L. Yang, W. Gasior, R. Katipally, and X. Cui, "Alerts analysis and visualization in network-based intrusion detection systems," in *Social Computing (SocialCom), 2010 IEEE Second International Conference on*, Aug 2010, pp. 785–790.

[209] S. Tricaud and P. Saadé, "Applied parallel coordinates for logs and network traffic attack analysis," *Journal in Computer Virology*, vol. 6, no. 1, pp. 1–29, 2010.

[210] W. Lian, F. Monrose, and J. McHugh, "Traffic classification using visual motifs: An empirical evaluation," in *Proceedings of the Seventh International Symposium on Visualization for Cyber Security*, ser.

PREPRINT

VizSec '10. New York, NY, USA: ACM, 2010, pp. 70–78. [Online]. Available: http://doi.acm.org/10.1145/1850795.1850804

[211] L. Briesemeister, S. Cheung, U. Lindqvist, and A. Valdes, "Detection, correlation, and visualization of attacks against critical infrastructure systems," in *PST*. IEEE, 2010, pp. 15–22. [Online]. Available: http://dblp.uni-trier.de/db/conf/pst/pst2010.html#BriesemeisterCLV10

[212] D. Shelly, M. Dunlop, R. C. Marchany, and P. Sforza, "Using geographic information systems for enhanced network security visualization," in *COM.Geo*, ser. ACM International Conference Proceeding Series, L. Liao, Ed. ACM, 2010. [Online]. Available: http://dblp.uni-trier.de/db/conf/comgeo/comgeo2010.html#ShellyDMS10

[213] M. Chu, K. Ingols, R. Lippmann, S. Webster, and S. Boyer, "Visualizing attack graphs, reachability, and trust relationships with NAVIGATOR," in *Proceedings of the Seventh International Symposium on Visualization for Cyber Security*, ser. VizSec '10. New York, NY, USA: ACM, 2010, pp. 22–33. [Online]. Available: http://doi.acm.org/10.1145/1850795.1850798

[214] T. Yu, R. Lippmann, J. Riordan, and S. Boyer, "EMBER: A global perspective on extreme malicious behavior," in *Proceedings of the Seventh International Symposium on Visualization for Cyber Security*, ser. VizSec '10. New York, NY, USA: ACM, 2010, pp. 1–12. [Online]. Available: http://doi.acm.org/10.1145/1850795.1850796

[215] D.-T. Wong, K.-S. Chai, S. Ramadass, and N. Vavasseur, "Expert-aware approach towards network security visualization tool services," in *Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on*, Sept 2010, pp. 213–217.

[216] ——, "Expert-aware approach: A new approach to improve network security visualization tool," in *Computational Intelligence, Communication Systems and Networks (CICSyN), 2010 Second International Conference on*, July 2010, pp. 227–231.

[217] E. Glatz, "Visualizing host traffic through graphs," in *Proceedings of the Seventh International Symposium on Visualization for Cyber Security*, ser. VizSec '10. New York, NY, USA: ACM, 2010, pp. 58–63. [Online]. Available: http://doi.acm.org/10.1145/1850795.1850802

[218] H. Shiravi, A. Shiravi, and A. A. Ghorbani, "IDS alert visualization and monitoring through heuristic host selection," in *Proceedings of the 12th International Conference on Information and Communications Security*, ser. ICICS'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 445–458. [Online]. Available: http://dl.acm.org/citation.cfm?id=1948352.1948393

[219] D.-T. Wong and S. Manickam, "Intelligent expertise classification approach: An innovative artificial intelligence approach to accelerate network data visualization," in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, vol. 6, Aug 2010, pp. V6–437–V6–440.

[220] Y. Cai and R. M. Franco, "Interactive visualization of network anomalous events," in *Proceedings of the 9th International Conference on Computational Science: Part I*, ser. ICCS '09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 450–459.

[221] Z. Kan, C. Hu, Z. Wang, G. Wang, and X. Huang, "NetVis: A network security management visualization tool based on treemap," in *Advanced Computer Control (ICACC), 2010 2nd International Conference on*, vol. 4, March 2010, pp. 18–21.

[222] H. Wang and Y. Chen, "Network topology description and visualization," in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, vol. 6, Aug 2010, pp. V6–52–V6–56.

[223] H. Wang, "NevML: A markup language for network topology visualization," in *Future Networks, 2010. ICFN '10. Second International Conference on*, Jan 2010, pp. 119–123.

[224] Z. Jiawan, Y. Peng, L. Liangfu, and C. Lei, "NetViewer: A visualization tool for network security events," in *Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC '09. International Conference on*, vol. 1, April 2009, pp. 434–437.

[225] J. Rasmussen, K. Ehrlich, S. Ross, S. Kirk, D. Gruen, and J. Patterson, "Nimble cybersecurity incident management through visualization and defensible recommendations," in *Proceedings of the Seventh International Symposium on Visualization for Cyber Security*, ser. VizSec '10. New York, NY, USA: ACM, 2010, pp. 102–113. [Online]. Available: http://doi.acm.org/10.1145/1850795.1850807

[226] C. Wagner, G. Wagener, R. State, A. Dulaunoy, and T. Engel, "PeekKernelFlows: Peeking into IP flows," in *Proceedings of the Seventh International Symposium on Visualization for Cyber Security*, ser. VizSec '10. New York, NY, USA: ACM, 2010, pp. 52–57. [Online]. Available: http://doi.acm.org/10.1145/1850795.1850801

[227] J. Guenther, F. Volk, and M. Shaneck, "Proposing a multi-touch interface for intrusion detection environments," in *Proceedings of the Seventh International Symposium on Visualization for Cyber Security*, ser. VizSec '10. New York, NY, USA: ACM, 2010, pp. 13–21. [Online]. Available: http://doi.acm.org/10.1145/1850795.1850797

[228] J. Glanfield, S. Brooks, T. Taylor, D. Paterson, C. Smith, C. Gates, and J. McHugh, "Over flow: An overview visualization for network analysis," in *Visualization for Cyber Security, 2009. VizSec 2009. 6th International Workshop on*. IEEE, 2009, pp. 11–19.

[229] M. Dayarathna, Y. Tsukahara, and K. Sugiura, "TelescopeVisualizer: A real-time internet information visualizer with a flexible user interface," in *Proceedings of the Sixth Asian Internet Engineering Conference*, ser. AINTEC '10. New York, NY, USA: ACM, 2010, pp. 16–23. [Online]. Available: http://doi.acm.org/10.1145/1930286.1930289

[230] J. P. S. Medeiros and S. R. dos Santos, "RadialNet: An interactive network topology visualization tool with visual auditing support," in *CRITIS*, ser. Lecture Notes in Computer Science, R. Setola and S. Geretshuber, Eds., vol. 5508. Springer, 2008, pp. 168–179. [Online]. Available: http://dblp.uni-trier.de/db/conf/critis/critis2008.html#MedeirosS08

[231] D. Barrera and P. Van Oorschot, "Security visualization tools and IPv6 addresses," in *Visualization for Cyber Security, 2009. VizSec 2009. 6th International Workshop on*, Oct 2009, pp. 21–26.

[232] G. R. Abuaitah and B. Wang, "Secvizer: A security visualization tool for qualnet-generated traffic traces," *VisSec poster*, 2009.

[233] J. Goodall and M. Sowul, "VIAssist: Visual analytics for cyber defense," in *Technologies for Homeland Security, 2009. HST '09. IEEE Conference on*, May 2009, pp. 143–150.

[234] K. Stockinger, E. W. Bethel, S. Campbell, E. Dart, and K. Wu, "Detecting distributed scans using high-performance query-driven visualization," in *Proceedings of the 2006 ACM/IEEE Conference on Supercomputing*, ser. SC '06. New York, NY, USA: ACM, 2006. [Online]. Available: http://doi.acm.org/10.1145/1188455.1188542

[235] C. Muelder, L. Chen, R. Thomason, K.-L. Ma, and T. Bartoletti, "Intelligent classification and visualization of network scans," in *VizSEC*, ser. Mathematics and Visualization, J. R. Goodall, G. J. Conti, and K.-L. Ma, Eds. Springer, 2007, pp. 237–253. [Online]. Available: http://dblp.uni-trier.de/db/conf/vizsec/vizsec2007.html#MuelderCTMB07

[236] A. Yelizarov and D. Gamayunov, "Visualization of complex attacks and state of attacked network," in *Visualization for Cyber Security, 2009. VizSec 2009. 6th International Workshop on*, Oct 2009, pp. 1–9.

[237] C. Langin, D. Che, M. Wainer, and S. Rahimi, "Visualization of network security traffic using hexagonal self-organizing maps," in *The 22nd International Conference on Computers and Their Applications in Industry and Engineering (CAINE-2009)*, 2009, pp. 1–6.

[238] S. Morrissey and G. Grinstein, "Visualizing firewall configurations using created voids," in *Visualization for Cyber Security, 2009. VizSec 2009. 6th International Workshop on*, Oct 2009, pp. 75–79.

[239] Z. Jiawan, L. Liang, L. Liangfu, and Z. Ning, "A novel visualization approach for efficient network scans detection," in *Security Technology, 2008. SECTECH '08. International Conference on*, Dec 2008, pp. 23–26.

[240] H. Yu, X. Dai, T. Baxley, and J. Xu, "A real -time interactive visualization system for DNS amplification attack challenges," in *Computer and Information Science, 2008. ICIS 08. Seventh IEEE/ACIS International Conference on*, May 2008, pp. 55–60.

[241] J. Shearer, K.-L. Ma, and T. Kohlenberg, "BGPeep: An IP-space centered view for internet routing data," in *VizSEC*, ser. Lecture Notes in Computer Science, J. R. Goodall, G. J. Conti, and K.-L. Ma, Eds., vol. 5210. Springer, 2008, pp. 95–110. [Online]. Available: http://dblp.uni-trier.de/db/conf/vizsec/vizsec2008.html#ShearerMK08

[242] J. Janies, "Existence plots: A low-resolution time series for port behavior analysis," in *VizSEC*, ser. Lecture Notes in Computer Science, J. R. Goodall, G. J. Conti, and K.-L. Ma, Eds., vol. 5210. Springer, 2008, pp. 161–168. [Online]. Available: http://dblp.uni-trier.de/db/conf/vizsec/vizsec2008.html#Janies08

[243] D. Phan, A. Paepcke, and T. Winograd, "Progressive multiples for communication-minded visualization," in *Proceedings of Graphics Interface 2007*, ser. GI '07. New York, NY, USA: ACM, 2007, pp. 225–232. [Online]. Available: http://doi.acm.org/10.1145/1268517.1268554

[244] J. Homer, A. Varikuti, X. Ou, and M. A. Mcqueen, "Improving attack graph visualization through data reduction and attack grouping," in *Proceedings of the 5th International Workshop on Visualization for Computer Security*, ser. VizSec '08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 68–79.

[245] M. Alsaleh, D. Barrera, and P. van Oorschot, "Improving security visualization with exposure map filtering," in *Computer Security Appli-*

DRAFT

cations Conference, 2008. ACSAC 2008. Annual, Dec 2008, pp. 205–214.

[246] J. Wang, Z. guang Qin, L. Ye, and J. Jin, "Modeling of network situation awareness," in *Communications, Circuits and Systems, 2008. ICCCAS 2008. International Conference on*, May 2008, pp. 461–465.

[247] B. Irwin and J.-P. van Riel, "Using InetVis to evaluate Snort and Bro scan detection on a network telescope," in *VizSEC*, ser. Mathematics and Visualization, J. R. Goodall, G. J. Conti, and K.-L. Ma, Eds. Springer, 2007, pp. 255–273. [Online]. Available: http://dblp.uni-trier.de/db/conf/vizsec/vizsec2007.html#IrwinR07

[248] G. Vandenberghe, "Network traffic exploration application: A tool to assess, visualize, and analyze network security events," in *Proceedings of the 5th International Workshop on Visualization for Computer Security*, ser. VizSec '08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 181–196.

[249] S. Musa and D. J. Parish, "Using time series 3d AlertGraph and false alert classification to analyse Snort alerts," in *Proceedings of the 5th International Workshop on Visualization for Computer Security*, ser. VizSec '08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 169–180.

[250] R. Blue, C. Dunne, A. Fuchs, K. King, and A. Schulman, "Visualizing real-time network resource usage," in *Proceedings of the 5th International Workshop on Visualization for Computer Security*, ser. VizSec '08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 119–135.

[251] B. Irwin and N. Pilkington, "High level internet scale traffic visualization using Hilbert curve mapping," in *VizSEC*, ser. Mathematics and Visualization, J. R. Goodall, G. J. Conti, and K.-L. Ma, Eds. Springer, 2007, pp. 147–158. [Online]. Available: http://dblp.uni-trier.de/db/conf/vizsec/vizsec2007.html#IrwinP07

[252] S. T. Teoh, S. Ranjan, A. Nucci, and C.-N. Chuah, "BGP Eye: A new visualization tool for real-time detection and analysis of BGP anomalies," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security*, ser. VizSEC '06. New York, NY, USA: ACM, 2006, pp. 81–90. [Online]. Available: http://doi.acm.org/10.1145/1179576.1179593

[253] T. Samak, A. El-Atawy, E. Al-Shaer, and M. Ismail, "A novel visualization approach for efficient network-wide traffic monitoring," in *End-to-End Monitoring Techniques and Services, 2007. E2EMON '07. Workshop on*, Yearly 2007, pp. 1–7.

[254] G. Conti, K. Abdullah, J. Grizzard, J. Stasko, J. A. Copeland, M. Ahamad, H. L. Owen, and C. Lee, "Countering security information overload through alert and packet visualization," *IEEE Comput. Graph. Appl.*, vol. 26, no. 2, pp. 60–70, Mar. 2006. [Online]. Available: http://dx.doi.org/10.1109/MCG.2006.30

[255] T. Taylor, S. Brooks, and J. McHugh, "NetBytes Viewer: An entity-based NetFlow visualization utility for identifying intrusive behavior," in *VizSEC*, ser. Mathematics and Visualization, J. R. Goodall, G. J. Conti, and K.-L. Ma, Eds. Springer, 2007, pp. 101–114. [Online]. Available: http://dblp.uni-trier.de/db/conf/vizsec/vizsec2007.html#TaylorBM07

[256] W. A. Pike, C. Scherrer, and S. Zabriskie, "Putting security in context: Visual correlation of network activity with real-world information," in *VizSEC*, ser. Mathematics and Visualization, J. R. Goodall, G. J. Conti, and K.-L. Ma, Eds. Springer, 2007, pp. 203–220. [Online]. Available: http://dblp.uni-trier.de/db/conf/vizsec/vizsec2007.html#PikeSZ07

[257] J. Oberheide, M. Goff, and M. Karir, "Flamingo: Visualizing internet traffic," in *Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP*, April 2006, pp. 150–161.

[258] C. P. Lee and J. A. Copeland, "Flowtag: A collaborative attack-analysis, reporting, and sharing tool for security researchers," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security*, ser. VizSEC '06. New York, NY, USA: ACM, 2006, pp. 103–108. [Online]. Available: http://doi.acm.org/10.1145/1179576.1179597

[259] E. Le Malecot, M. Kohara, Y. Hori, and K. Sakurai, "Grid based network address space browsing for network traffic visualization," in *Information Assurance Workshop, 2006 IEEE*, June 2006, pp. 261–267.

[260] S. Musa and D. Parish, "Visualising communication network security attacks," in *Information Visualization, 2007. IV '07. 11th International Conference*, July 2007, pp. 726–733.

[261] F. Mansmann and S. Vinnik, "Interactive exploration of data traffic with hierarchical network maps," *IEEE Transactions on Visualization and Computer Graphics*, vol. 12, no. 6, pp. 1440–1449, Nov. 2006. [Online]. Available: http://dx.doi.org/10.1109/TVCG.2006.98

[262] F. Mansman, L. Meier, and D. Keim, "Visualization of host behavior for network security," in *VizSEC 2007*, ser. Mathematics and Visualization, J. Goodall, G. Conti, and K.-L. Ma, Eds. Springer Berlin Heidelberg, 2008, pp. 187–202.

[263] J. Pearlman and P. Rheingans, "Visualizing network security events using compound glyphs from a service-oriented perspective," in *VizSEC*, ser. Mathematics and Visualization, J. R. Goodall, G. J. Conti, and K.-L. Ma, Eds. Springer, 2007, pp. 131–146. [Online]. Available: http://dblp.uni-trier.de/db/conf/vizsec/vizsec2007.html#PearlmanR07

[264] E. Le Malécot, M. Kohara, Y. Hori, and K. Sakurai, "Interactively combining 2d and 3d visualization for network traffic monitoring," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security*, ser. VizSEC '06. New York, NY, USA: ACM, 2006, pp. 123–127. [Online]. Available: http://doi.acm.org/10.1145/1179576.1179600

[265] K. Yoshida, Y. Shomura, and Y. Watanabe, "Visualizing network status," in *Machine Learning and Cybernetics, 2007 International Conference on*, vol. 4, Aug 2007, pp. 2094–2099.

[266] E. Bethel, S. Campbell, E. Dart, K. Stockinger, and K. Wu, "Accelerating network traffic analytics using query-driven visualization," in *Visual Analytics Science And Technology, 2006 IEEE Symposium On*, Oct 2006, pp. 115–122.

[267] A. Herrero, E. Corchado, and J. M. Sáiz, "MOVICAB-IDS: Visual analysis of network traffic data streams for intrusion detection," in *Proceedings of the 7th International Conference on Intelligent Data Engineering and Automated Learning*, ser. IDEAL'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 1424–1433.

[268] K. Abdullah, C. Lee, G. Conti, and J. Copeland, "Processing data to construct practical visualizations for network security," *Information Assurance Newsletter*, vol. 9, pp. 3–7, 2006.

[269] A. Shabtai, D. Klimov, Y. Shahar, and Y. Elovici, "An intelligent, interactive tool for exploration and visualization of time-oriented security data," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security*, ser. VizSEC '06. New York, NY, USA: ACM, 2006, pp. 15–22. [Online]. Available: http://doi.acm.org/10.1145/1179576.1179580

[270] W. Harrop and G. Armitage, "Real-time collaborative network monitoring and control using 3d game engines for representation and interaction," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security*, ser. VizSEC '06. New York, NY, USA: ACM, 2006, pp. 31–40. [Online]. Available: http://doi.acm.org/10.1145/1179576.1179583

[271] Y. Hideshima and H. Koike, "STARMINE: A visualization system for cyber attacks," in *Proceedings of the 2006 Asia-Pacific Symposium on Information Visualisation - Volume 60*, ser. APVis '06. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2006, pp. 131–138. [Online]. Available: http://dl.acm.org/citation.cfm?id=1151903.1151923

[272] K. Abdullah and J. A. Copeland, "Tool update: High alarm count issues in IDS Rainstorm," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security*, ser. VizSEC '06. New York, NY, USA: ACM, 2006, pp. 61–62. [Online]. Available: http://doi.acm.org/10.1145/1179576.1179587

[273] W. Yurcik, "Tool update: NVisionIP improvements (difference view, sparklines, and shapes)," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security*, ser. VizSEC '06. New York, NY, USA: ACM, 2006, pp. 65–66. [Online]. Available: http://doi.acm.org/10.1145/1179576.1179589

[274] S. Mathew, R. Giomundo, S. Upadhyaya, M. Sudit, and A. Stotz, "Understanding multistage attacks by attack-track based visualization of heterogeneous event streams," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security*, ser. VizSEC '06. New York, NY, USA: ACM, 2006, pp. 1–6. [Online]. Available: http://doi.acm.org/10.1145/1179576.1179578

[275] A. L. Stephano and D. P. Groth, "USEable security: Interface design strategies for improving security," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security*, ser. VizSEC '06. New York, NY, USA: ACM, 2006, pp. 109–116. [Online]. Available: http://doi.acm.org/10.1145/1179576.1179598

[276] R. de Paula, X. Ding, P. Dourish, K. Nies, B. Pillet, D. F. Redmiles, J. Ren, J. A. Rode, and R. S. Filho, "In the eye of the beholder: A visualization-based approach to information system security," *Int. J. Hum.-Comput. Stud.*, vol. 63, no. 1-2, pp. 5–24, Jul. 2005. [Online]. Available: http://dx.doi.org/10.1016/j.ijhcs.2005.04.021

[277] C. V. Wright, F. Monrose, and G. M. Masson, "Using visual motifs to classify encrypted traffic," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security*, ser. VizSEC '06. New York, NY, USA: ACM, 2006, pp. 41–50. [Online]. Available: http://doi.acm.org/10.1145/1179576.1179584

[278] J. Oberheide, M. Karir, and D. Blazakis, "VAST: Visualizing Autonomous System Topology," in *Proceedings of the 3rd International*

PREPRINT

Workshop on Visualization for Computer Security, ser. VizSEC '06. New York, NY, USA: ACM, 2006, pp. 71–80. [Online]. Available: http://doi.acm.org/10.1145/1179576.1179592

[279] T. Wong, V. Jacobson, and C. Alaettinoglu, "Internet routing anomaly detection and visualization," in *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on*, June 2005, pp. 172–181.

[280] L. Li, P. Liu, and G. Kesidis, "Visual toolkit for network security experiment specification and data analysis," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security*, ser. VizSEC '06. New York, NY, USA: ACM, 2006, pp. 7–14. [Online]. Available: http://doi.acm.org/10.1145/1179576.1179579

[281] K. Ohno, H. Koike, and K. Koizumi, "IPMatrix: an effective visualization framework for cyber threat monitoring," in *Information Visualisation, 2005. Proceedings. Ninth International Conference on*, July 2005, pp. 678–685.

[282] S. Axelsson, "Visualising intrusions: Watching the webserver," in *SEC*, 2004, pp. 259–274.

[283] P. Hertzog, "Visualizations to improve reactivity towards security incidents inside corporate networks," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security*, ser. VizSEC '06. New York, NY, USA: ACM, 2006, pp. 95–102. [Online]. Available: http://doi.acm.org/10.1145/1179576.1179596

[284] P. Ren, J. Kristoff, and B. Gooch, "Visualizing DNS traffic," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security*, ser. VizSEC '06. New York, NY, USA: ACM, 2006, pp. 23–30. [Online]. Available: http://doi.acm.org/10.1145/1179576.1179582

[285] S. S. Kim and A. L. N. Reddy, "NetViewer: A network traffic visualization and analysis tool," in *Proceedings of the 19th Conference on Large Installation System Administration Conference - Volume 19*, ser. LISA '05. Berkeley, CA, USA: USENIX Association, 2005, pp. 18–18. [Online]. Available: http://dl.acm.org/citation.cfm?id=1251150.1251168

[286] ——, "A study of analyzing network traffic as images in real-time," in *INFOCOM*. IEEE, 2005, pp. 2056–2067. [Online]. Available: http://dblp.uni-trier.de/db/conf/infocom/infocom2005.html#KimR05

[287] J. R. Goodall, A. A. Ozok, W. G. Lutters, P. Rheingans, and A. Komlodi, "A user-centered approach to visualizing network traffic for intrusion detection," in *CHI '05 Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA '05. New York, NY, USA: ACM, 2005, pp. 1403–1406. [Online]. Available: http://doi.acm.org/10.1145/1056808.1056927

[288] S. Krasser, G. Conti, J. Grizzard, J. Gribschaw, and H. Owen, "Real-time and forensic network data analysis using animated and coordinated visualization," in *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC*, June 2005, pp. 42–49.

[289] G. Fink and C. North, "Root polar layout of internet address data for security administration," in *Visualization for Computer Security, 2005. (VizSEC 05). IEEE Workshop on*, Oct 2005, pp. 55–64.

[290] A. Komlodi, P. Rheingans, U. Ayachit, J. Goodall, and A. Joshi, "A user-centered look at glyph-based security visualization," in *Visualization for Computer Security, 2005. (VizSEC 05). IEEE Workshop on*, Oct 2005, pp. 21–28.

[291] I.-V. Onut, B. Zhu, and A. A. Ghorbani, "SVision: A network host-centered anomaly visualization technique," in *ISC*, ser. Lecture Notes in Computer Science, J. Zhou, J. Lopez, R. H. Deng, and F. Bao, Eds., vol. 3650. Springer, 2005, pp. 16–28. [Online]. Available: http://dblp.uni-trier.de/db/conf/isw/isc2005.html#OnutZG05

[292] C. Muelder, K.-L. Ma, and T. Bartoletti, "A visualization methodology for characterization of network scans," in *Visualization for Computer Security, 2005. (VizSEC 05). IEEE Workshop on*, Oct 2005, pp. 29–38.

[293] J. Goodall, "User requirements and design of a visualization for intrusion detection analysis," in *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC*, June 2005, pp. 394–401.

[294] G. Fink, P. Muessig, and C. North, "Visual correlation of host processes and network traffic," in *Visualization for Computer Security, 2005. (VizSEC 05). IEEE Workshop on*, Oct 2005, pp. 11–19.

[295] R. F. Erbacher, K. Christensen, and A. Sundberg, "Designing visualization capabilities for IDS challenges," in *Proceedings of the IEEE Workshops on Visualization for Computer Security*, ser. VIZSEC '05. Washington, DC, USA: IEEE Computer Society, 2005, pp. 15–. [Online]. Available: http://dx.doi.org/10.1109/VIZSEC.2005.1532074

[296] A. Oline and D. Reiners, "Exploring three-dimensional visualization for intrusion detection," in *Visualization for Computer Security, 2005. (VizSEC 05). IEEE Workshop on*, Oct 2005, pp. 113–120.

[297] G. Conti, J. Grizzard, M. Ahamad, and H. Owen, "Visual exploration of malicious network objects using semantic zoom, interactive encoding and dynamic queries," in *Visualization for Computer Security, 2005. (VizSEC 05). IEEE Workshop on*, Oct 2005, pp. 83–90.

[298] P. Ren, Y. Gao, Z. Li, Y. Chen, and B. Watson, "IDGraphs: Intrusion detection and analysis using histographs," in *VizSEC*, K.-L. Ma, S. C. North, and W. Yurcik, Eds. IEEE Computer Society, 2005, p. 5. [Online]. Available: http://dblp.uni-trier.de/db/conf/vizsec/vizsec2005.html#RenGLCW05

[299] C. Lee, J. Trost, N. Gibbs, R. Beyah, and J. Copeland, "Visual firewall: real-time network security monitor," in *Visualization for Computer Security, 2005. (VizSEC 05). IEEE Workshop on*, Oct 2005, pp. 129–136.

[300] D. Yao, M. Shin, R. Tamassia, and W. Winsborough, "Visualization of automated trust negotiation," in *Visualization for Computer Security, 2005. (VizSEC 05). IEEE Workshop on*, Oct 2005, pp. 65–74.

[301] K. Abdullah, C. Lee, G. Conti, and J. Copeland, "Visualizing network data for intrusion detection," in *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC*, June 2005, pp. 100–108.

[302] I.-V. Onut, B. Zhu, and A. A. Ghorbani, "A novel visualization technique for network anomaly detection," in *PST*, 2004, pp. 167–174. [Online]. Available: http://dblp.uni-trier.de/db/conf/pst/pst2004.html#OnutZG04

[303] S. T. Teoh, K. Zhang, S.-M. Tseng, K.-L. Ma, and S. F. Wu, "Combining visual and automated data mining for near-real-time anomaly detection and analysis in BGP," in *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, ser. VizSEC/DMSEC '04. New York, NY, USA: ACM, 2004, pp. 35–44. [Online]. Available: http://doi.acm.org/10.1145/1029208.1029215

[304] C. Papadopoulos, C. Kyriakakis, A. Sawchuk, and X. He, "CyberSeer: 3d audio-visual immersion for network security and management," in *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, ser. VizSEC/DMSEC '04. New York, NY, USA: ACM, 2004, pp. 90–98. [Online]. Available: http://doi.acm.org/10.1145/1029208.1029223

[305] S. T. Teoh, K.-L. Ma, S. Wu, and T. J. Jankun-Kelly, "Detecting flaws and intruders with visual data analysis," *Computer Graphics and Applications, IEEE*, vol. 24, no. 5, pp. 27–35, Sept 2004.

[306] R. Ball, G. A. Fink, and C. North, "Home-centric visualization of network traffic for security administration," in *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, ser. VizSEC/DMSEC '04. New York, NY, USA: ACM, 2004, pp. 55–64. [Online]. Available: http://doi.acm.org/10.1145/1029208.1029217

[307] G. Conti and K. Abdullah, "Passive visual fingerprinting of network attack tools," in *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, ser. VizSEC/DMSEC '04. New York, NY, USA: ACM, 2004, pp. 45–54. [Online]. Available: http://doi.acm.org/10.1145/1029208.1029216

[308] H. Kim, I. Kang, and S. Bahk, "Real-time visualization of network attacks on high-speed links," *Network, IEEE*, vol. 18, no. 5, pp. 30–39, Sept 2004.

[309] A. Valdes and M. Fong, "Scalable visualization of propagating internet phenomena," in *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, ser. VizSEC/DMSEC '04. New York, NY, USA: ACM, 2004, pp. 124–127. [Online]. Available: http://doi.acm.org/10.1145/1029208.1029228

[310] T. Goldring, "Scatter (and other) plots for visualizing user profiling data and network traffic," in *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, ser. VizSEC/DMSEC '04. New York, NY, USA: ACM, 2004, pp. 119–123. [Online]. Available: http://doi.acm.org/10.1145/1029208.1029227

[311] H. Koike and K. Ohno, "SnortView: Visualization system of snort logs," in *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, ser. VizSEC/DMSEC '04. New York, NY, USA: ACM, 2004, pp. 143–147. [Online]. Available: http://doi.acm.org/10.1145/1029208.1029232

[312] S. Lau, "The spinning cube of potential doom," *Commun. ACM*, vol. 47, no. 6, pp. 25–26, Jun. 2004. [Online]. Available: http://doi.acm.org/10.1145/990680.990699

[313] T. Atkison, K. Pensy, C. Nicholas, D. Ebert, R. Atkison, and C. Morris, "Case study: Visualization and information retrieval techniques for network intrusion detection," in *Proceedings of*

PREPRINT

the 3rd Joint Eurographics - IEEE TCVG Conference on Visualization, ser. EGVISSYM'01. Aire-la-Ville, Switzerland, Switzerland: Eurographics Association, 2001, pp. 283–290. [Online]. Available: http://dx.doi.org/10.2312/VisSym/VisSym01/283-290

[314] S. Axelsson, "Visualisation for intrusion detection - hooking the worm," in *In The proceedings of the 8th European Symposium on Research in Computer Security (ESORICS 2003), volume 2808 of LNCS*. Springer Verlag, 2003.

[315] J. Tolle and O. Niggemann, "Supporting intrusion detection by graph clustering and graph drawing," in *Proc. of Third International Workshop on Recent Advances in Intrusion Detection (RAID 2000)*. Springer, 2000.

[316] G. Mansfield, M. Ouchi, K. Jayanthi, Y. Kimura, K. Ohta, and Y. Nemoto, "Techniques for automated network map generation using SNMP," in *INFOCOM '96. Fifteenth Annual Joint Conference of the IEEE Computer Societies. Networking the Next Generation. Proceedings IEEE*, vol. 2, Mar 1996, pp. 473–480 vol.2.

[317] A. O. Mendelzon, "Visualizing the World Wide Web," in *AVI*, T. Catarci, M. F. Costabile, S. Levialdi, and G. Santucci, Eds. ACM Press, 1996, pp. 13–19. [Online]. Available: http://dblp.uni-trier.de/db/conf/avi/avi1996.html#Mendelzon96

[318] Y. Song, J. Keeney, and O. Conlan, "A framework to leverage domain expertise to support novice users in the visual exploration of home area networks," in *Network Operations and Management Symposium (NOMS), 2012 IEEE*, April 2012, pp. 550–553.

[319] A. Oslebo, "Share and visualize your data using the perfSONAR NC framework," in *Network Operations and Management Symposium (NOMS), 2012 IEEE*, April 2012, pp. 838–852.

[320] J. Sventek, A. Koliousis, O. Sharma, N. Dulay, D. Pediaditakis, M. Sloman, T. Rodden, T. Lodge, B. Bedwell, K. Glover, and R. Mortier, "An information plane architecture supporting home network management," in *Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on*, May 2011, pp. 1–8.

[321] Y. Xia, K. Fairbanks, and H. Owen, "Visual analysis of program flow data with data propagation," in *Proceedings of the 5th International Workshop on Visualization for Computer Security*, ser. VizSec '08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 26–35.

[322] P. Abel, P. Gros, C. Russo Dos Santos, D. Loisel, and J.-P. Paris, "Automatic construction of dynamic 3d metaphoric worlds: an application to network management," vol. 3960, 2000, pp. 312–323. [Online]. Available: http://dx.doi.org/10.1117/12.378908

[323] G. Melissargos and P. Pu, "Conceptualizing bandwidth allocation in network management," in *Proceedings of the 1999 Workshop on New Paradigms in Information Visualization and Manipulation in Conjunction with the Eighth ACM Internation Conference on Information and Knowledge Management*, ser. NPIVM 99. New York, NY, USA: ACM, 1999, pp. 62–69. [Online]. Available: http://doi.acm.org/10.1145/331770.331787

[324] N. Patwari, A. O. Hero, III, and A. Pacholski, "Manifold learning visualization of network traffic data," in *Proceedings of the 2005 ACM SIGCOMM Workshop on Mining Network Data*, ser. MineNet '05. New York, NY, USA: ACM, 2005, pp. 191–196. [Online]. Available: http://doi.acm.org/10.1145/1080173.1080182

[325] D. Keim, F. Mansmann, J. Schneidewind, and T. Schreck, "Monitoring network traffic with Radial Traffic Analyzer," in *Visual Analytics Science And Technology, 2006 IEEE Symposium On*, Oct 2006, pp. 123–128.

[326] T. Yu, B. Fuller, J. Bannick, L. Rossey, and R. Cunningham, "Integrated environment management for information operations testbeds," in *VizSEC 2007*, ser. Mathematics and Visualization, J. Goodall, G. Conti, and K.-L. Ma, Eds. Springer Berlin Heidelberg, 2008, pp. 67–83.

[327] S. Bratus, A. Hansen, F. Pellacini, and A. Shubina, "Backhoe, a packet trace and log browser," in *Proceedings of the 5th International Workshop on Visualization for Computer Security*, ser. VizSec '08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 152–160.

[328] S. Papadopoulos and D. Tzovaras, "Towards visualizing mobile network data," in *ISCIS*, ser. Lecture Notes in Electrical Engineering, E. Gelenbe and R. Lent, Eds., vol. 264. Springer, 2013, pp. 379–387. [Online]. Available: http://dblp.uni-trier.de/db/conf/iscis/iscis2013.html#0002T13

[329] A. Panangadan, S. Monacos, S. Burleigh, J. Joswig, M. James, E. Chow, A. Talukder, and K.-D. Chu, "A system to provide real-time collaborative situational awareness by web enabling a distributed sensor network," in *Proceedings of the First ACM SIGSPATIAL Workshop on Sensor Web Enablement*, ser. SWE '12. New York, NY, USA: ACM, 2012, pp. 24–31. [Online]. Available: http://doi.acm.org/10.1145/2451716.2451720

[330] E. Karapistoli, P. Sarigiannidis, and A. A. Economides, "SRNET: A real-time, cross-based anomaly detection and visualization system for wireless sensor networks," in *Proceedings of the Tenth Workshop on Visualization for Cyber Security*, ser. VizSec '13. New York, NY, USA: ACM, 2013, pp. 49–56. [Online]. Available: http://doi.acm.org/10.1145/2517957.2517964

[331] S. A. Catanese and G. Fiumara, "A visual tool for forensic analysis of mobile phone traffic," in *Proceedings of the 2Nd ACM Workshop on Multimedia in Forensics, Security and Intelligence*, ser. MiFor '10. New York, NY, USA: ACM, 2010, pp. 71–76. [Online]. Available: http://doi.acm.org/10.1145/1877972.1877992

[332] O. Conlan, J. Keeney, C. Hampson, and F. Williams, "Towards non-expert users monitoring networks and services through semantically enhanced visualizations," in *Network and Service Management (CNSM), 2010 International Conference on*, Oct 2010, pp. 406–409.

[333] Y. Song, J. Keeney, O. Conlan, P. Perry, and A. Hava, "An ontology-driven approach to support wireless network monitoring for home area networks," in *Network and Service Management (CNSM), 2011 7th International Conference on*, Oct 2011, pp. 1–7.

[334] L. Harrison, X. Hu, X. Ying, A. Lu, W. Wang, and X. Wu, "Interactive detection of network anomalies via coordinated multiple views," in *Proceedings of the Seventh International Symposium on Visualization for Cyber Security*, ser. VizSec '10. New York, NY, USA: ACM, 2010, pp. 91–101. [Online]. Available: http://doi.acm.org/10.1145/1850795.1850806

[335] K. Prole, J. R. Goodall, A. D. D'Amico, and J. K. Kopylec, "Wireless cyber assets discovery visualization," in *Proceedings of the 5th International Workshop on Visualization for Computer Security*, ser. VizSec '08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 136–143.

[336] W. Wang and A. Lu, "Visualization assisted detection of sybil attacks in wireless networks," in *Proceedings of the 3rd International Workshop on Visualization for Computer Security*, ser. VizSEC '06. New York, NY, USA: ACM, 2006, pp. 51–60. [Online]. Available: http://doi.acm.org/10.1145/1179576.1179585

[337] J. Ishmael and N. Race, "Visawin: visualising a wireless network," in *Vehicular Technology Conference, 2004. VTC 2004-Spring. 2004 IEEE 59th*, vol. 5, May 2004, pp. 2623–2626 Vol.5.

[338] S. Engle and S. Whalen, "Visualizing distributed memory computations with hive plots," in *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*, ser. VizSec '12. New York, NY, USA: ACM, 2012, pp. 56–63. [Online]. Available: http://doi.acm.org/10.1145/2379690.2379698

[339] *Using Visualization to Support Network and Application Management in a Data Center*, October 2008. [Online]. Available: http://research.microsoft.com/apps/pubs/default.aspx?id=79267

[340] M. Sedlmair, A. Frank, T. Munzner, and A. Butz, "RelEx: Visualization for actively changing overlay network specifications," *Visualization and Computer Graphics, IEEE Transactions on*, vol. 18, no. 12, pp. 2729–2738, Dec 2012.

[341] K. Wang, Y. Qi, B. Yang, Y. Xue, and J. Li, "LiveSec: Towards effective security management in large-scale production networks," in *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on*, June 2012, pp. 451–460.

[342] W. J. Matuszak, L. DiPippo, and Y. L. Sun, "CyberSAVe: Situational awareness visualization for cyber security of smart grid systems," in *Proceedings of the Tenth Workshop on Visualization for Cyber Security*, ser. VizSec '13. New York, NY, USA: ACM, 2013, pp. 25–32. [Online]. Available: http://doi.acm.org/10.1145/2517957.2517961

[343] K. Liu, B. Wilson, and J. Wei, "A management and visualization framework for reconfigurable WDM optical networks," *Network, IEEE*, vol. 14, no. 6, pp. 8–15, Nov 2000.

[344] T. Takahashi, K. Emura, A. Kanaoka, S. Matsuo, and T. Minowa, "Risk visualization and alerting system: Architecture and proof-of-concept implementation," in *Proceedings of the First International Workshop on Security in Embedded Systems and Smartphones*, ser. SESP '13. New York, NY, USA: ACM, 2013, pp. 3–10. [Online]. Available: http://doi.acm.org/10.1145/2484417.2484421

[345] T. Nunnally, A. S. Uluagac, J. A. Copeland, and R. A. Beyah, "3DSVAT: A 3d stereoscopic vulnerability assessment tool for network security," in *LCN*. IEEE, 2012, pp. 111–118. [Online]. Available: http://dblp.uni-trier.de/db/conf/lcn/lcn2012.html#NunnallyUCB12

[346] E. Novikova and I. Kotenko, "Analytical visualization techniques for security information and event management," in *Parallel, Distributed and Network-Based Processing (PDP), 2013 21st Euromicro International Conference on*, Feb 2013, pp. 519–525.

[347] C. Horn and A. D'Amico, "Visual analysis of goal-directed network defense decisions," in *Proceedings of the 8th International*

PREPRINT

Symposium on Visualization for Cyber Security, ser. VizSec '11. New York, NY, USA: ACM, 2011, pp. 5:1–5:6. [Online]. Available: http://doi.acm.org/10.1145/2016904.2016909

[348] B. Le Grand and M. Soto, "Navigation in huge information hierarchies application to network management," in *Proceedings of the 1999 Workshop on New Paradigms in Information Visualization and Manipulation in Conjunction with the Eighth ACM Internation Conference on Information and Knowledge Management*, ser. NPIVM '99. New York, NY, USA: ACM, 1999, pp. 56–61. [Online]. Available: http://doi.acm.org/10.1145/331770.331785

[349] "An online visualization system for streaming log data of computing clusters," *Tsinghua Science and Technology*, vol. 18, no. 2, pp. 196–205, April 2013.

PREPRINT