Towards Enhancing Inter-Domain Routing Security with Visualization and Visual Analytics

Jingwei Tang, Guodao Sun, Jiahui Chen, Gefei Zhang, Qi Jiang, Yanbiao Li, Guangxing Zhang, Jian Liu, Haixia Wang and Ronghua Liang

***Abstract*—In the complex landscape of the Internet, inter-domain routing systems are essential for ensuring seamless connectivity and reachability across autonomous systems. However, the lack of dependable security validation mechanisms in these systems poses persistent challenges. Vulnerabilities such as prefix hijacking, path forgery, and route leakage not only compromise network operators and users, but also threaten the stability and accessibility of the Internet's core infrastructure. To address this, visualization and visual analytics techniques are adept at identifying and detecting security threats, offering network administrators effective methods to monitor and maintain network operations. This paper presents a comprehensive survey of the state-of-the-art research in visualization and visual analytics for inter-domain routing security. We delineate four scenarios for tasks analysis in network visualization: monitoring, detection, verification, and discovery. Each category is explored in detail, focusing on the employed data sources and visualization techniques. Several key findings are presented at the end of each category, aimed at providing researchers and practitioners with research inspiration. Furthermore, we examine the trends of academic interest observed in recent decades and propose potential directions for future research in visual analytics pertaining to Internet infrastructure security.**

***Index Terms*—Inter-domain Routing, Border Gateway Protocol, Anomaly Detection, Information Visualization, Visual Analytics**

I. Introduction

THE Inter-domain Routing Security (IDRS) has consistently garnered attention due to its inherent systemic criticality and security fragility. As a critical infrastructure of the Internet, the inter-domain routing system, which utilizes the Border Gateway Protocol (BGP), ensures the reliable and stable operation of the global Internet. It assumes the responsibility of maintaining and transferring routing reachability information among autonomous systems (ASes) embedded within the intricate fabric of the global Internet routing system. Despite its widespread deployment, the initial design of the BGP protocol lacked security features to ensure the authenticity of route announcements. A several of security challenges has emerged, encompassing issues like prefix hijacking [1], route leaks [2], misconfiguration [3] and other related factors [4]. Each year, a significant volume of attacks and anomalies within the inter-domain routing landscape present menacing challenges to the global internet infrastructure. Although security solutions such as BGPSec [5] and RPKI [6] have been introduced by the community to enhance the verification of route origin and path legitimacy.

In addition, monitoring and detecting anomalies in the inter-domain network poses a formidable challenge due to the rapid pace of BGP message updates, substantial message volume, and the blurred demarcation between anomalous and normal data instances. These anomalies encompass a spectrum of scenarios including frequent oscillations in updates, occurrences of routing loops, dissemination of false routes, and interruptions in BGP sessions. The presence of these deviations has the potential to engender instability within network routing, consequently exerting a cascading influence upon the seamless conveyance of data packets as well as the overall network availability. In the current intricate landscape of cyberspace, malicious incidents manifest in diverse forms and continue to evolve to elude detection. Despite the incorporation of automated AI algorithms and the integration of domain experts' expertise, the precise traceback of such malicious incidents remains a formidable challenge, primarily attributed to their mutable characteristics. As a result, the pursuit of effective anomaly detection confronts considerable hurdles. Visualization has the potential to address this issue by incorporating human knowledge into the information processing tasks. It intuitively presents security incidents and anomalous patterns to decision-makers, while involving human-machine interaction as they explore the real BGP route scenarios.

Previous research has indicated that the analysis of inter-domain routing and internet infrastructure analysis requires strong domain expertise [2]. Therefore, the users of BGP analysis tools are primarily targeted towards network administrators and resource owners such as AS admins, Internet service providers (ISPs), Internet exchange points (IXPs) managers, Prefix owners, and Internet regulators. Additionally, visual analytics can enhance the accessibility of network analysis by providing an intuitive understanding of network operation patterns. This can enable regular users and the media to better perceive network threats and gain insight into network operation modes. Furthermore, decision-makers can benefit from situational awareness of the network by leveraging visual analytics to gain insights into network operation patterns and identify potential threats.

Our survey aims to provide a comprehensive review of the state-of-the-art research in visual analytics of inter-domain security. The objective is to highlight current research trends and identify promising areas for future investigation, while also establishing systematic guidelines that can assist researchers and practitioners in identifying effective solutions for their

research in this field based on their specific application domains. Moreover, our work attempts to investigate the primary application domains that are of interest to the visualization research community, rather than providing a comprehensive or exclusive analysis given the significant overlap between data sources and visualization techniques.

In this survey, we contribute a taxonomy of visual analytics for inter-domain security. After conducting an extensive literature review and consulting with domain experts, we have compiled a comprehensive overview of potential security threats in the BGP system. Building upon this analysis, we have identified four primary task scenarios for inter-domain visual analytics: *Network Monitoring*, *Network Detection*, *Network Verification*, and *Network Discovery*. Following the visual analytics pipeline of cybersecurity, we then extract four common data sources including *Routing Message Updates*, *Routing Event Logging*, *Routing Table Topology* and *Routing Spatial Mapping*. Finally, we summarize four visualization techniques, including *Spatio-temporal based*, *Graph based*, *Hierarchical based*, and *Multivariate based*. We develop a web-based survey browser to help users understand taxonomy and relevant papers in this work (https://zjutvis.github.io/VOBGP). In summary, the contribution of this paper are as follows:

- We collect and summarize 94 typical papers that involve visualization and visual analysis techniques of inter-domain routing security to provide a review.
- We present a taxonomy categorizing target users, security threats, task scenarios, data sources, and visualization techniques for a detailed overview. Each task scenario includes a "*Key Findings*" section, highlighting challenges and future research opportunities.
- We develop a web-based survey browser to facilitate the exploration of our taxonomy and associated papers.

II. Related Surveys

Several research disciplines have shown interest in studying IDRS security, encompassing areas such as vulnerabilities [7], threats [8], defense mechanisms [9], security assessment [10], routing policies [11], and visualization techniques [12]. In order to identify the areas of interest addressed by these research studies within a given domain, we initially conducted a comparative analysis of relevant literature reviews, resulting in the identification of six distinct focus aspects. These aspects have informed our classification scheme for visual analytics tools, which we will be presenting.

Based on the different aspects the selected surveys focused on, we have established six categories: *BGP Theory and Practice (BTP), Target Users Groups (TUG), Security Threats Assessment (STA), Tasks Scenarios Investigation (TSI), Data Mining and Characterization (DMC), and Visual Encoding Discussion (VED).* In Table. I, enumerates identified survey papers, with each entry marked by a check to indicate its focus among the six delineated areas.

Reviews on BGP security threats and anomalies. Like other routing protocols, BGP is vulnerable to security threats, primarily due to the lack of message authentication and integrity protection, absence of authoritative validation for network announcements, and insufficient authentication verification for AS paths and path attributes [13], [14]. These issues may result in BGP messages being spoofed, deleted, modified, or relayed, leading to incorrect routing information and security vulnerabilities. To address these concerns, various measures and best practices have been proposed, such as Secure BGP (S-BGP) and Resource Public Key Infrastructure (RPKI) [15], to enhance BGP security and mitigate these threats. Certain studies focus on the introduction of security concerns, including threat types [8] and attack methods [10] related to the BGP system, as well as the evaluation and analysis of available BGP security extensions and detection-recovery systems [16]. Other works have specifically addressed BGP prefix hijacking and interception issues, proposing corresponding solutions [17]. Additionally, routing address information management issues [18] and IRR data consistency problems concerning [19] have also been introduced. Furthermore, there are also several works that discuss the research and classification of BGP anomaly detection technology and non-visual forms of anomaly event detection, such as algorithmic or pattern matching methods [20].

TABLE I
COMPARISON OF RELATED SURVEYS.

Publications	Year	BGP Theory	Target Users	Sercurity Threats	Tasks Scenarios	Data Mining	Visual Encoding
Butler et al. [9]	2010	■	□	■	▣	□	□
Huston et al. [12]	2011	■	▣	■	■	□	□
Biersack et al. [23]	2012	▣	□	□	■	▣	■
Siddiquia et al. [15]	2015	■	□	■	▣	□	□
Al-Musawi et al. [19]	2017	■	□	■	▣	■	□
Ulmer et al. [28]	2017	□	■	▣	■	■	■
Mitseva et al. [8]	2018	■	□	■	▣	▣	□
Raynor et al.[11]	2022	▣	■	■	▣	■	■
Kowalski et al.[84]	2023	■	□	■	■	▣	□
Our paper	2023	□	■	■	■	■	■

■ Aspects of primary focus
▣ Aspects not emphasized
□ Aspects insufficiently discussed

Reviews on BGP visual analytics and monitoring. Visual analytics techniques not only provide a beautiful and attractive representations of datasets, but also assist users in effectively monitoring network patterns, accurately identifying anomalous features, rapidly detecting network anomalies, and comprehensively understanding network evolution patterns [21]–[23]. Several works focus on the visualization acquisition of routing information and geospatial network information to help users better understand and protect Internet routing, and to further identify, analyze, and understand routing configuration errors and vulnerabilities [24]–[26]. Other works focus on introducing network visualization tools and conduct detailed investigations and visual classifications of visualization tools related to BGP anomaly monitoring to better understand the corresponding network attacks and capture the visualization techniques used in this field [12]. In addition, visual analytics for network security also involves various network visualization methods, such as semantic layers, graphical rendering, and visual analysis, with the aim of aiding users in better understanding and analyzing network data, as well as guiding

the development of new network visualization methods and techniques [27]–[29].

III. Problem Characterization

In the realm of the Internet, it comprises tens of thousands of autonomous systems (ASes), each operating as a distinct network entity. These autonomous systems encompass a variety of organizations, including *Internet Service Providers (ISPs)*, *Internet Content Providers (ICPs)*, *Content Delivery Networks (CDNs)*, *Cloud Service Providers (CSPs)*, *Educational Institutions* and *Independently Operated Networks*. In the context of network infrastructure, these autonomous systems establish connections with each other through border networks, employing the Border Gateway Protocol (BGP) grounded in a trust-based model for communication, thereby ensuring the holistic interconnectivity of the Internet. Considering the trust-based networking mechanism in place, inter-domain routing systems continue to exhibit various security risks, including prefix hijacking, route leakage and source address spoofing. With the evolution of the internet, the proliferation of diverse demands has become increasingly apparent. This section provides a detailed exposition of the current security threats and varied demands for visualization and visual analysis concerning inter-domain routing security issues from different user levels.

TABLE II
A comparison across four dimensions (Domain Expertise, Primary Responsibilities, Visualization Requirement, and Potential Roles), highlights the distinctions among three user groups with different knowledge backgrounds(Network Administrators, Research Analysts, and General Audiences).

Characteristics / User Groups	Domain Expertise	Primary Responsibilities	Visualization Requirement	Potential Roles
Network Administrators	Strong technical expertise	Ensuring system reliability, avoiding route flapping; Monitoring system operation, identifying routing anomalies.	Detailed real-time data; Overview and drill-down capabilities; Efficient monitoring supports quick decision-making.	AS, ISP, IXP Admins; Prefix Owners; Security Operation Centers.
Research Analysts	Expertise in their specific research field	Analyzing business opportunities, Optimizing strategic decisions; Evaluating network performance, Enhancing system robustness; Tracking spot irregularities, improving network regulation.	Overview of the system, ability to drill down to detailed data; Focusing on anomalies for researchers; Avoiding information overload for business analysts.	Business Analysts; Academic Researchers; Internet Regulators; Law Enforcement Officers.
General Audiences	Limited technical expertise	Optimizing user experience; Understanding and disseminating the impact of security incidents.	Providing a timeline of network incidents; Showing the occurrence, duration, and impact scope; Avoiding complex information that could lead to information overload.	Policy makers; Journalists; General Internet Users.

A. Target Users Groups

This section we describe the user groups who might derive advantages from inter-domain routing security visualization and visual analytics. Several studies have explored the classification of user groups, revealing a need for visualization tools not just for experts but also for users with varying levels of domain experience, encompassing diverse analytical interests. ProBGP [2] integrates domain knowledge to position AS administrators and prefix owners as the primary users. It utilizes visual analytics to provide deep insights into routing data, while also accommodating AS, ISP, IXP Managers, and regulators for comprehensive network analysis interests. Ulmer et al. [29] introduce two new user groups in their subsequent research, including business analysts and researchers who are interested in achieving higher effectiveness in discovering new insights from data. Raynor et al. [12] emphasize the importance of visual analytics for the general public in their latest review. Despite the limited domain background of ordinary internet users, network anomalies significantly impact user experience. Thus, visual analytics tools should also cater to ordinary users, journalists, and policymakers to understand potential network risks.

Based on the previous research, we categorize users into three non-mutually exclusive groups based on user expertise: Administrators, Analysts, and Audiences. As shown in table. II, we summarize the comparison of users with different knowledge backgrounds in terms of their primary responsibilities, visualization requirements, and potential roles. It should be noted that many of the visual analytics works discussed may cater to more than one group. For instance, both analysts and non-domain experts require an overview to reinforce their own intuition for how BGP works.

1) Network Administrators: The first groups of users engaging with IDRS visualization consist of network and resource administrators who are responsible for managing network routing, monitoring system operations, and promptly troubleshooting issues. These administrators and operators, whether researchers or engineers possess a profound understanding of inter-domain routing architecture and showcase extensive network in operation experience. Their expertise accelerates critical decision-making in IDRS, particularly in identifying anomalies or misconfigurations that result in reduced traffic speed or packet loss.

Experts from large ISPs and organizations have extensive experience in configuring and monitoring routing strategies. This tool leverages expert insights derived from real-world instances, such as Berkeley root routing cause analysis and ISP-Anon's routing flapping. It addresses issues such as unbalanced load balancing, backdoor routes, BGP community tagging, route leakage among peers, and continuous route flapping.

2) Research Analysts: The second group of individuals who may derive benefits from IDRS visualization comprises analysts and researchers. These users may possess relevant technical or business background but are novices in BGP network operations. This category encompasses users such as business analysts, prefix owners, internet regulators, and law enforcement agencies (LEAs). They integrate their specific business requirements with the use of visualization tools to analyze trends in BGP route changes, identify potential issues and optimization opportunities, support decision-making and strategic planning, and engage in relationship analysis. This group of users may not possess extensive domain expertise but require the integration of BGP data for analysis, where visualization can effectively support these users in their tasks.

3) General Audiences: The third group of users who can benefit from visualization consists of non-experts in inter-domain routing security. These individuals typically have no prior knowledge of BGP system and may not possess a technical background. Research efforts targeting this group primarily aim to simplify comprehension and enhance the dissemination of information. They rely on the reports and dashboards provided by visual analytics tools to access summarized in-

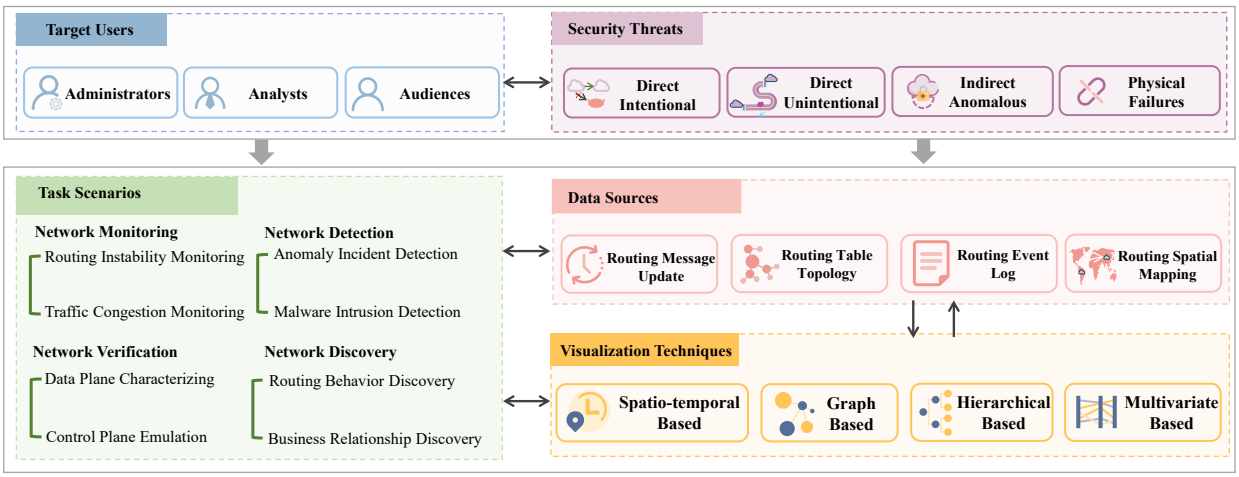

Fig. 1. The taxonomy of this survey outlines four task scenarios, associated with relevant data sources and visualization techniques, all within the context of inter-domain routing security threats and targeting user groups.

formation on network performance, connectivity status, and to stay informed about significant security incidents.

These group also includes people who are beginners in IDRS. They may gain inspiration from visual analysis tools to better understand the workings of the BGP routing network, aiding them in gradually developing skills in network management and route configuration. The system has been used to analyze the dynamics of AS-level topology and diagnose issues in internet routing.

B. Security Threats Landscape

To comprehensively analyze inter-domain routing security, it typically requires the concurrent examination of both the data plane and the control plane. The control plane of inter-domain routing systems primarily involves managing routing information exchange, determining optimal route paths, and controlling routing policies.

The data plane is responsible for the fundamental-level packet transmission and processing. This includes forwarding data packets based on routing decisions, implementing traffic classification, enforcing quality of service, and applying firewall filtering. In network environments, typical malicious activities such as DDoS attacks, worm viruses, and botnets may cause anomalies in data plane traffic. The challenges of data plane threats are differentiating legitimate from attack traffic within the routing system [24]. When attack traffic substantially increases, it may overwhelm the network's processing capacity, leading to disruptions or delays in normal traffic flow. Extended periods of link congestion or connection disruptions may cause resets of BGP sessions potentially leading to interruptions or service halts in inter-domain routing systems [30].

The control plane is responsible for routing control and management within a network, ensuring that data is transmitted along the correct paths in the network. Its main tasks include maintaining routing tables, running routing protocols, defining routing policies, and detecting and recovering from faults. The challenges of control plane arise from the fundamental trust-based architecture of the Border Gateway Protocol (BGP) [31]. In practice, autonomous systems typically accept routing announcements from neighbors without conditional validation. Therefore, the control plane is vulnerable to various threats such as prefix hijacking, source path spoofing, and route termination. These threats often result in anomalies or manipulation of routing tables, subsequently impacting routing reachability across the entire network.

Drawing upon academic expertise in networking and an extensive review of pertinent literature, security threats to inter-domain routing systems are conventionally classified into four distinct categories: *direct intentional*, *direct unintentional*, *indirect anomalous*, and *physical failures*.

1) Direct intentional: threats refer to malicious attack operations targeting inter-domain routing systems within the cyberspace. Malicious intrusion such as BGP prefix hijacking, BGP message spoofing and BGP path manipulation can lead to issues like abnormal data transmission, security vulnerabilities, information leakage, or network interruptions. Strengthening inter-domain routing security can involve the use of BGP route policy filtering, BGP monitoring, RPKI (Resource Public Key Infrastructure) signing, and other measures. Monitoring, detecting, and mitigating these anomalies are crucial steps in enhancing network security.

2) Direct unintentional: threats typically result from inadvertent configuration errors operational mistakes by network administrators, or software failures in devices, leading to adverse effects on routing and data transmission. These incidents can result in BGP route leakage and BGP route blackholing, and similar issues, which can lead to the erroneous propagation of routing information, affecting regional or even global internet services [32].

3) Indirect anomalous: threats refer to anomalies that are not directly caused by BGP routing protocols or router configurations but rather result from complex interactions due to external factors and network activities within the internet space, such as DDoS attacks [33], Botnet [34] and worm viruses [30]. These anomalies typically manifest as abnormalities in data plane traffic, link congestion, subsequently influencing routing policy decisions, and may even lead to the complete paralysis of certain BGP networks. Despite researchers proposing various solutions for mitigating route flapping, and some network operators prioritizing BGP traffic, these incidents still necessitate more advanced monitoring and

analysis at higher levels to recognize and address them.

4) Physical failures: threats refer to issues caused by problems with the physical components or elements of network infrastructure, resulting in network interruptions or abnormal routing behavior. These problems are typically triggered by natural factors, equipment malfunctions, or physical damage. When a backbone network link experiences a failure, whether due to reasons like undersea fiber optic cable breaks, equipment malfunctions, natural disasters, or human interference, the operational effectiveness of BGP routers, particularly in terms of acquiring and transmitting route information, can be compromised. Such incidents have the potential to lead to disruptions in the accessibility and performance of inter-domain routing, thereby affecting internet services across multiple regions worldwide [35].

As described above, *Direct intentional* and *Direct unintentional* threats fall under the category of control plane failures. In contrast, *Indirect anomalous* and *Physical failures* typically exert an indirect influence on the data plane, they both have adverse effects on inter-domain routing communications.

IV. Methodology and Taxonomy

This section presents our methodology for selecting papers related to the survey topic, along with a taxonomy of inter-domain routing security task scenarios that consider common data sources and visualization techniques (see Fig.1). We also delve into how visualizations can effectively address specific challenges, tailored to meet diverse user requirements in the context of IDRS.

A. Methodology

This study primarily focuses on visual analytics methodologies aimed at enhancing the accessibility of inter-domain network monitoring, detection, verification and discovery for both novice users and domain experts. To provide a comprehensive survey of visualization and visual analytics techniques in the context of inter-domain routing security, a keyword search was conducted to gather papers published in visualization and computer network conferences, venues, and journals spanning the past two decades (2003-2023).

Our literature search primarily focused on notable publications within the field, such as *ACM Special Interest Group on Data Communication (SIGCOMM)*, *IEEE Transactions on Network and Service Management (TNSM)*, *IEEE Transactions on Visualization and Computer Graphics (TVCG)*, *IEEE Visualization (IEEE VIS)*, *Eurographics Conference on Visualization (EuroVis)*, and *IEEE Symposium on Visualization for Cyber Security (VizSec)*. We utilized a range of cybersecurity related search queries (e.g., *"inter-domain routing", "BGP", "security", "anomaly", "hijacking"*) and visualization-related keywords (e.g. "visualization", "visual analytics", "diagrams", "charts", "monitoring"). To identify additional publications collected in our study, we then employ a citation-based search strategy that involves the reference lists of each relevant paper and also searching for later incoming citations using Google Scholar. After such a round of paper selection and filtering, we obtained 363 papers.

We then carefully reviewed the 363 selected papers, following the subsequent criteria for evaluation. Firstly, as this survey aims to investigate how visualization and visual analytics could enhance the security of inter-domain routing, we focused on papers that contribute novel forms of visualization or interactive analysis tools. Subsequently, we excluded articles focused on network optimization, physical network infrastructure development, network performance testing, and similar topics. Although these areas are related to networks, they do not directly involve visual analytics.

All the papers were reviewed by two visualization researchers to confirm their relevance the concept of BGP security. Specifically, we screened the titles of collected papers to identify candidate papers. Then, we reviewed the abstracts of the candidate papers to further determine whether they concerned visual analytics techniques for BGP security. If the title and abstract did not provide sufficient information, we reviewed the full text of the candidate papers to make a final determination. After collecting the literature and consulting with domain experts, we conducted a thorough review to ensure that no important articles were missed. Through an exhaustive examination, our final corpus included 94 relevant papers.

B. Taxonomy

In this section, we conduct a comprehensive analysis of the collected visual analytics work to systematically understand the major research trends concerning visual analytics of BGP security. Within the realm of security threat analysis, we have classified four task scenarios for BGP security visual analytics task: network monitoring, feature mining, anomaly detection, and pattern evolution. For each category, we identify common data sources and visualization techniques.

*1) **Task Scenarios**:* Visual analysis about IDRS can provide users with a situational awareness and support to ensure the security and reliability of BGP networks. To categorize task scenarios relevant to IDRS Visualization, we initially consulted prior research in the field of cybersecurity visualization. Komadina et al [21] conducted an analysis of 17 review papers pertaining to cybersecurity visualization, synthesizing from these a set of 14 overarching security tasks identified in VizSec papers, which include situational awareness, threat analysis, user behavior, and incident handling, among others. In the realm of network and service management [25], operators must consider a multitude of managerial aspects, including business relationships, temporal synchronization, configuration management, fault handling and performance optimization. Furthermore, it is essential to devise management approaches such as automation, semi-automation, or policy-based methods, and implement them using applicable technologies. Incorporating the principles of *from overview to detail.* and *Focus + Context.* from visual analytics [36], we develop an analytical framework that progresses from monitoring to response, analysis to optimization, and global to local to guide our task scenario categorization. This framework encompasses inter-domain routing network functions, ranging from monitoring and detection to verification and discovery.

Network monitoring plays a fundamental role in Inter-domain routing visual analysis. Network monitoring primarily entails real-time monitoring of network device status and

TABLE III
OVERVIEW OF TYPICAL WORKS IN VISUALIZATION AND VISUAL ANALYTICS OF INTER-DOMAIN ROUTING SECURITY. EACH ROW IS ONE WORK; WORKS ARE SORTED CHRONOLOGICALLY BY THE PUBLICATION TIME. EACH COLUMN CORRESPONDS TO DIFFERENT FOCUS AREAS WITHIN THE PAPERS. A WORK'S RELEVANT AREAS IS INDICATED BY A COLORED CELL.

Publication	year	Security Threats				Task Scenarios				Data Sources				Visualization			
		Direct Intended	Direct Unintended	Indirect Anomalies	Physical Failures	Network Monitoring	Network Detection	Network Verification	Network Discovery	Time Series	Network Topology	Cybersecurity Report	Geospatial	Spatial-temporal	Graph Based	Hierarchical Based	Multivariate Based
Schufrin et al. [64]	2022	■				■	■			■		■					■
Peng et al. [70]	2022			■				■			■						■
Danneman et al. [35]	2022				■		■			■			■	■			
Ulmer et al. [2]	2021	■	■			■	■			■	■		■	■	■		
Candela et al. [79]	2020	■	■		■		■		■	■	■			■	■		
Syamkumar et al. [3]	2020		■		■	■	■			■			■	■			
Yan et al. [92]	2020	■		■			■			■	■			■	■		
Goodall et al. [61]	2019			■		■				■		■		■	■		
Kalwar et al. [59]	2019			■		■				■	■			■	■		
Candela et al. [63]	2018		■			■			■	■	■			■	■	■	
Yan et al. [92]	2018	■		■			■	■		■	■			■	■		■
Ceneda et al. [80]	2016		■			■			■	■	■		■	■	■		
Papadopoulos et al. [74]	2016	■	■				■	■		■	■				■	■	
Syamkumar et al. [39]	2016	■	■				■		■		■		■	■	■		
Angelini et al. [93]	2015	■					■				■				■		
Gray et al. [4]	2015			■	■		■		■	■	■			■	■		
Chen et al. [33]	2014			■			■		■		■					■	■
Shrestha et al. [101]	2014			■					■	■					■		
Papadopoulos et al. [32]	2013		■		■	■	■			■	■		■	■	■		
Papadopoulos et al. [75]	2013	■				■	■	■		■	■		■	■			■
Zhao et al. [91]	2013			■		■	■			■				■		■	
Papadopoulos et al. [73]	2012		■					■		■	■				■	■	
Boschetti et al. [95]	2011	■					■		■				■	■	■		
Yan et al. [77]	2009	■				■	■			■							
Chi et al. [78]	2008	■	■	■		■	■			■	■				■		
Cittadini et al. [41]	2008				■		■		■	■						■	
Deng et al. [52]	2008		■			■		■		■	■				■		
Mansmann et al. [62]	2007	■				■	■			■				■		■	
Cortese et al. [90]	2006	■						■	■	■	■		■	■	■	■	
Lad et al. [71]	2006	■					■	■		■	■			■	■		
Oberheide et al. [42]	2006	■	■				■			■	■				■		
Teoh et al. [54]	2006	■		■		■	■			■	■			■	■		
Colitti et al. [57]	2005	■	■			■	■			■	■			■	■		
Wong et al. [69]	2005	■	■				■		■		■				■		
Lad et al. [44]	2004		■				■	■			■	■		■			
Teoh et al. [58]	2004	■				■	■			■	■			■		■	■

traffic to ensure network security and reachability, thereby ensuring the normal operation of the network [37]. It requires collecting and storing multi-dimensional routing communication data, extracting critical information, and expedite its visualization for user consumption. This task not only provides real-time snapshots of network operational status for network administrators but also facilitates a deeper understanding of the stability and performance of routers and links. Additionally, it serves as an interface for beginners to gain insight into network anomalies.

Network detection refers to the detection of possible anomalies by identifying behavior or events that deviate from expected patterns. After obtaining a global understanding of network operation status, specific algorithms or interactive visual analytics are required to further investigate and confirm security threats such as Anomaly incident or malicious intrusions within the cyberspace domain. Anomaly detection can assist administrators in identifying security threats, such as malicious hijacking [1], unauthorized announcements [38], configuration errors [39], and link failures [40], and prompt detection and resolution of such issues.

Network verification employs feature extraction modeling methodologies and interactive visual analytics techniques to deliver validation support for both the data plane and control plane of routing networks. This approach ensures that network intentions are properly executed while concurrently offering emulation techniques capable of identifying prospective implementation mistakes in networking equipment in advance. Network verification entails deeper investigation of cybersecurity incidents. It has the ability to identify critical characteristics in BGP network data, such as BGP update summary [31], route path inspection [41], and AS topology analysis [42], in order to facilitate more in-depth analysis and utilization [43].

Network discovery leverages visual analytics to expose the evolution and implicit patterns of interdomain routing system networks. Research into the evolution of routing patterns in routing networks can assist administrators in elucidating trajectories of change pertaining to network traffic and routing relationships, in order to forecast future network conditions and identify potential latent issues. Moreover, elucidating commercial relationships within cybernetworks can also facilitate more efficacious deployment of routing apparatuses and enhancement of regional routing load capacity. Network discovery enables users to gain insights into the evolving trends of network topology [44] and routing performance [45], and to discover AS business relationships, regional routing load capabilities, and other relevant factors. This facilitates valuable decision-making support for network resource planning.

*2) **Data sources**:* Network security analysts are primarily concerned with what data is available and what information can be extracted from it. Once this is established, it is crucial to focus on the design of visual structures that accurately represent the data and the subsequent mapping of the data to these structures. After analyzing research papers and technical communities, we have identified and categorized 24 different types of data sources used in various studies. These data sources include BGP routing update data, IP prefix allocation, and AS-relationship, among others. Two researchers in the field of visual analytics, one working towards a master's degree and the other a doctorate, independently generalized and summarized the data based on common analysis tasks in visual analytics [46]–[49]. The results were then discussed with researchers in the field of BGP data mining. Through the analysis of multiple data attributes, four common data sources have been identified, which include time series data, network topology data, cybersecurity reports data, and geospatial data. A brief description of each data source is provided as follows. *Routing Message Update* data is a set of data and arranged in chronological order [50], which can be used to describe BGP network traffic, routing path features [31], AS topology changes over time. *Routing Event Log* data refer to a collection of unstructured text data or records of anomalous events on the Internet [51]. *Routing Table Topology* data describes the structure and connectivity relationships of network elements such as routers, AS relationships, as well as hierarchical data such as IP address allocation and RPKI authorization chains. *Routing Spatial Mapping* data such as GeoIP and AS-IP

data [2], contains information about longitude and latitude, and typically describes the physical location and connectivity relationships of network devices, as well as the geographical distribution of network traffic. This can aid administrators in conducting geographical analysis and visualization related to network infrastructure.

*3) **Visualization Techniques**:* Existing Visualization techniques utilize a range of visual representations to demonstrate BGP network patterns and convey meaningful insights. The selection of visual representations has an impact on how anomalous events and cybersecurity data are organized and aggregated. We identified four categories of visual representation for displaying BGP security data. *Spatio-temporal based* visualizations refer to the utilization of the time axis to facilitate improved network traffic monitoring, tracking the timing of network events, and exploring other relevant temporal aspects. By incorporating geospatial data, the visualization technique provides insights into the geographical distribution of BGP networks. This includes identifying the geographic location of IP addresses and visualizing the spatial patterns of network traffic. *Graph based* visualizations refers to node-link representation, which help users better understand the topology and routing relationships of BGP networks. When combined with temporal analysis, they can also be used to uncover patterns of network evolution. *Hierarchical based* visualizations employ a hierarchical structure to help users better understand the relationships and interactions between different levels in the BGP network, such as the business relationships between ASes and the hierarchical relationship of RPKI authorization. *Multivariate based* visualizations leverage multi-dimensional data to integrate and analyze different types of data, such as multi-dimensional features extracted from BGP updates.

Overall, based on a comprehensive review of existing BGP security threats, we have identified and categorized four types of BGP security task scenarios, including Network monitoring, Feature mining, Anomaly detection and Pattern evolution. For each task, we provide a detailed breakdown of common data source and visualization techniques. We believe that these categories can provide guidance for researchers and practitioners by linking visual analytical tasks and BGP security. The example papers are shown in Table.III.

V. Visual analytics on Network Monitoring

Network monitoring is a critical process that involves analyzing diverse operational data and presenting network status, traffic, and other essential metrics in an interactive visual format to gain comprehensive insights into network operations. Network monitoring serves as the basis for other network analysis tasks, and by integrating it with advanced visual analytics techniques, security analysts can swiftly comprehend the network's operation status, detect potential security threats or anomalies, and take preemptive measures to mitigate these risks, thereby ensuring the stability and security of the system. The main purpose of visualization in this category is to present the current state of the network by displaying fundamental statistics such as system load, entropy, overall throughput, and the number of users that reflect the network's condition [25]. Visualization facilitates the prompt detection of significant changes in these statistics, allowing users to identify state changes and potential anomalies in the network.

1) Routing Instability Monitoring: In the realm of network management, routing updates materialize subsequent to various events such as configuration adjustments, network failures, and dynamic traffic engineering. These updates are a direct consequence of alterations in routing decisions [56]. BGPlay [57] allows Internet Service Providers to monitor the reachability of a specified prefix by utilizing a graph metaphor. Teoh et al. [58] developed a real-time data collection and interactive visual analysis client, which facilitates user-interaction to monitor metrics such as BGP updates and differences in the frequency of AS path occurrences.

2) Traffic Congestion Monitoring: Real-time monitoring and analysis of data traffic in BGP networks is essential for network administrators to understand the distribution and trends of network traffic, as well as to detect anomalous traffic patterns, such as sudden increases in route announcement volume or a large number of withdrawn announcements. Visualizations in this category describe the traffic flows between different nodes in the network. TVis [59] models network traffic as an undirected graph and computes Heron triangles based on the correlations of each vertex within a 5-second time window, enabling real-time monitoring of both low-rate and high-rate traffic attacks and triggering alerts. As shown in Fig.2(d), BGPEye [54] provides multi-granularity views to assist administrators in monitoring the number of network traffic anomalies caused by route interruptions. It presents a dual-perspective visualization tool for real-time and scalable root-cause analysis of BGP updates events, providing both Internet-Centric and Home-Centric perspectives to improve network monitoring.

A. Data Sources

Routing Message Update data is essential to capturing the dynamic nature of BGP state and traffic. It encompasses crucial components including timestamps, durations, and temporal relationships, providing a comprehensive understanding of the temporal variations within the BGP network. It also has the capability to incorporate real-time variations in link conditions. The data is obtained from historical BGP update records or IP traceroute traffic data retrieved from diverse RIS organizations or institutions, such as RIPE NCC, RouteViews, and CAIDA. As shown in Fig.2(c) various institutions deploy observation points globally to gather sequentially updated routing data [29]. Visual representations with temporal relationships, such as timeline [60], line charts [61], is commonly employed to monitor network status and traffic. These visual mappings facilitate the detection of notable deviations in system load patterns, thus aiding in the identification of changes in network state or potential anomalies [62].

Routing Table Topology data typically describes the connectivity relationships between networks, such as AS-relationships, which depict the interconnections between ASes. In inter-domain routing systems, topology data is commonly extracted from multi-hop paths recorded in BGP routing tables. Obtaining a comprehensive understanding of the Internet's

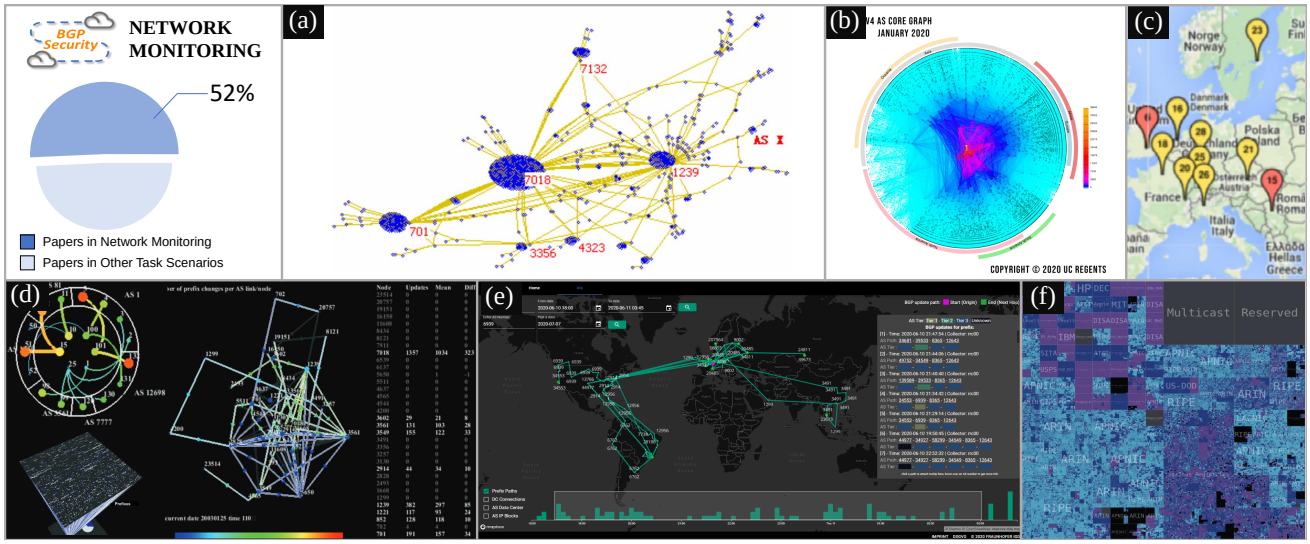

Fig. 2. Visualization of network monitoring. (a) ROUSSEAU [52] employs a spring-magnetic layout algorithm for monitoring internet providers and national networks. (b) AS Core Graph [53] shows AS connectivity and evolution by converting IP connections into AS links. (c) BGP Monitoring Points [29] mark Routeviews in red and RIPE NCC points in yellow, aiding global internet routing analysis. (d) BGPEye [54] offers a real-time BGP updates analysis tool with Internet-Centric and Home-Centric views. (e) ProBGP [2] introduces a progressive visual analytics application to represent global routing network monitoring. (f) IPCensus [55] utilizes a Hilbert map for detailed visualization of global IP space allocation.

topology at a global scale presents significant challenges. As shown in Fig. 2(a), ROUSSEAU [52] present an enhanced graph layout algorithm, combined with a force layout model, to mitigate network node overlap and minimize edge crossings. This approach facilitates a in-depth understanding of routing anomalies, such as the announcement of private IP blocks and inconsistent IP-AS mappings.

Over the past two decades, CAIDA has been devoted to the measurement of global Macroscopic Topology. They have made the AS Rank dataset openly accessible, thereby fostering further in-depth exploration by researchers into the attributes, dynamic behavior, and evolution of critical infrastructure within the Internet. As shown in Fig. 2(b), AS Core Graph [53] captures the connectivity attributes between ASes, converting IP connections into AS links. By leveraging geographic mappings, it represents global AS connectivity relationships, effectively addressing the challenges of large-scale topologies in the global Internet. Global topological data are represented through a chord plot, facilitating the observation and analysis of interconnectivity among Autonomous System (AS) resources at multiple hierarchical levels. In addition, the traceroute command serves as a simple tool capable of offering localized AS topology information, aiding in the preliminary analysis of routing behavior for individual devices [63].

Routing Event Log data is commonly used for data analysis and summarization in network monitoring to reveal the most significant entities and event sequences. The cybersecurity reports data primarily comprises log data from network monitoring systems and text-based security reports manually curated by experts [35]. Cybersecurity incident reports can assist decision-makers in quickly understanding the development of network security situations and provide valuable insights and information to support decision-making and the formulation of risk management measures [64]. Customizable user summarization and narrative visualization for network security reports can aid security analysts in rapidly comprehending complex temporal relationships within textual data, enabling them to more quickly identify underlying patterns in network anomaly events [51].

Routing Spatial Mapping data establishes a connection between geographic coordinates and topology, providing analysts with a spatial perspective for analysis. These approaches commonly rely on typical data sources like GeoIP and AS-IP data [2]. The geospatial data includes longitude and latitude information, which commonly represent the physical coordinates and connectivity associations among network devices, along with the geographic dispersion of network traffic [65]. The combination of traceroute data and geospatial data facilitates the analysis of BGP update's spatial propagation paths in the real world, enabling insights into potential business relationships [26]. Furthermore, by incorporating temporal information, it is possible to further explore the spatiotemporal correlations of abnormal events in the BGP system [3].

B. Visualization Techniques

The utilization of visualization techniques enables the transformation of diverse and heterogeneous network state and traffic data into intuitive and visually appealing graphical representations. This empowers network administrators and security analysts to gain comprehensive insights into monitoring behaviors, identify network anomalies, and make precise decisions for network optimization and security enhancement.

Spatial-temporal based visualization combines the dimensions of time and space, encompassing a variety of time-based visual representations. It enables users to monitor route propagation on maps and facilitates a comprehensive understanding of dynamic network behavior. As shown in Fig. 2(e), ProBGP [2] is utilized for BGP update queries and geographic visualization, with its primary visualization being a map overlaid with query input fields. Users can enter an AS number and a date to obtain the geographic approximation of the AS data centers. Situ [61] introduces a streaming analysis

tool that incorporates the event search page to assist analysts in acquiring situational awareness, detecting suspicious behavior, and comprehending the contextual information associated with the behavior.

Graph based visualization techniques are commonly employed to depict the connectivity relationships at both the IP-level and AS-level of interdomain routing. The AS graph demonstrates a densely connected structure at its core, with prominent nodes forming extensive interconnections among themselves. Conversely, the majority of leaf ASes exhibit connections to a comparatively limited number of ASes [53]. TPlay [66] presents a radial layered drawings for displaying traceroutes. This technique represents graphs with vertices placed on concentric circles and targets in the center, which is effective for visualizing sparse hierarchical graphs. The probes originating the traceroutes are in the periphery of the drawing, and this approach is effective in displaying topological distances.

Hierarchical based visualization hierarchically presents the business relationships among ASes, enabling users to explore and access detailed information about the AS path from various perspectives. The AS path and other attributes are represented as hierarchical dimensions, with instances organized into higher-level categories at multiple levels, forming a tree structure. This visualization design preserves the geographic position, proximity, and size of network nodes while presenting the hierarchical relationships, facilitating the comparison of different nodes in the network. Hierarchical Network Map [67] organizes the display area as a map with a zoomable rectangle area for each network, using the associated IP addresses for computing the node's coordinates. Fischer et al. [68] employs treemap visualization technique in conjunction with a multi-criteria clustering algorithm to monitor potential patterns and characteristics of attack activities in a network.

To monitor the allocation and utilization of global network resources, Ipcensus [55] employs a Hilbert map (see Fig. 2(f)) to enhance network monitoring by systematically depicting the allocation of global IP space in a detailed and accessible manner. Additionally, treemap representations also find applications in both network traffic exploration in security domains and providing overviews in file systems forensics, as well as in malware analysis [62].

TABLE IV
THE PRIMARY ANALYSIS PERSPECTIVES OF NETWORK MONITORING AND THE ASSOCIATED DATA SOURCES, VISUALIZATIONS AND TOOLS.

Data & Tools / Analysis perspectives	Data Sources	Visualization Techniques	Typical Works
Topology Dynamics	Multi-hop Routing Data, Real-time BGP Updates, AS Rank Dataset	Force Layout Graphs, Enhanced Graph Layout Algorithms, Chord Plots	ROUSSEAU [52], BGPlay [57], AS Core Graph [53]
Traffic Insights	Real-time BGP Traffic Data, Historical BGP Update Records, IP Traceroute Data	Spatial-temporal Visualizations, Graphs with Correlations, Timeline and Line Charts	Tvis [59], BGPEye [54]
Geo-Intelligence	GeoIP Data, AS-IP Mappings, Traceroute Data with Geographic Coordinates, IP	Geographic Visualization on Maps, Hilbert Map for Spatial Distribution	ProBGP [2], IPCensus [55]

C. Key Findings

Visual analytics for network monitoring facilitate the dissemination of real-time information regarding network status and traffic by graphically illustrating critical statistical data, including system load, entropy, total throughput, and user count, thereby enabling network administrators to promptly discern notable fluctuations within these metrics. As shown in Table. IV, by integrating and employing time-series data alongside network topology data, the spectrum of network monitoring is expanded, allowing for a more precise pinpointing and scrutiny of potential red flags in network operations, such as identifying suspicious prefixes, analyzing propagation paths, and scrutinizing routing updates. Under the guidance of multi-view correlated visual analysis techniques, the integration and joint analysis of different data perspectives become possible, providing administrators with a more comprehensive view of network operations and enhanced precision and speed in threat detection. Simultaneously, this multidimensional, multi-angled data fusion and analysis bring forth new challenges, such as ensuring data integrity and accuracy, balancing real-time dynamic monitoring with historical data analysis, and providing a user-friendly experience while retaining depth in data analysis.

Current visual analytics for network monitoring primarily focuses on BGP route update data provided by institutions like RIPE NCC, RouteView, and CAIDA. Additionally, as the data is sourced from limited observation points, it poses challenges in accurately identifying localized network issues and is often employed for post-event analysis. In future research directions, on one hand, there is an emphasis on integrating and aligning multiple data sources, including network traffic data, security logs, and geographical data, to enhance the monitoring and detection capabilities within the BGP system. On the other hand, there's an emphasis on merging local routing dynamics with global routing information to strengthen real-time network monitoring capabilities. This approach benefits a more comprehensive, accurate, and detailed understanding of network status and security intelligence This necessitates an effective integration and amalgamation of diverse visualization techniques in the design realm, aiming to offer a more comprehensive analysis of BGP characteristics.

VI. VISUAL ANALYTICS ON NETWORK DETECTION

Network detection refers to identifying potential anomalies by detecting events or behaviors that do not conform to expected patterns. This scenario helps network administrators to detect abnormal traffic [69], anomalous routers [52], and other potential security threats [76]. By employing this approach, administrators can promptly detect and address network malfunctions and security threats. Anomalies encompass a broad spectrum of network security issues, such as abrupt fluctuations in traffic, device failures, unauthorized resource access, and suspicious host behavior. This work focuses on the application of visual analytics methods to common anomalies in the BGP routing system, such as sudden changes in route announcement traffic, prefix hijacking and network faults caused by operational mistakes. The complexity of the BGP

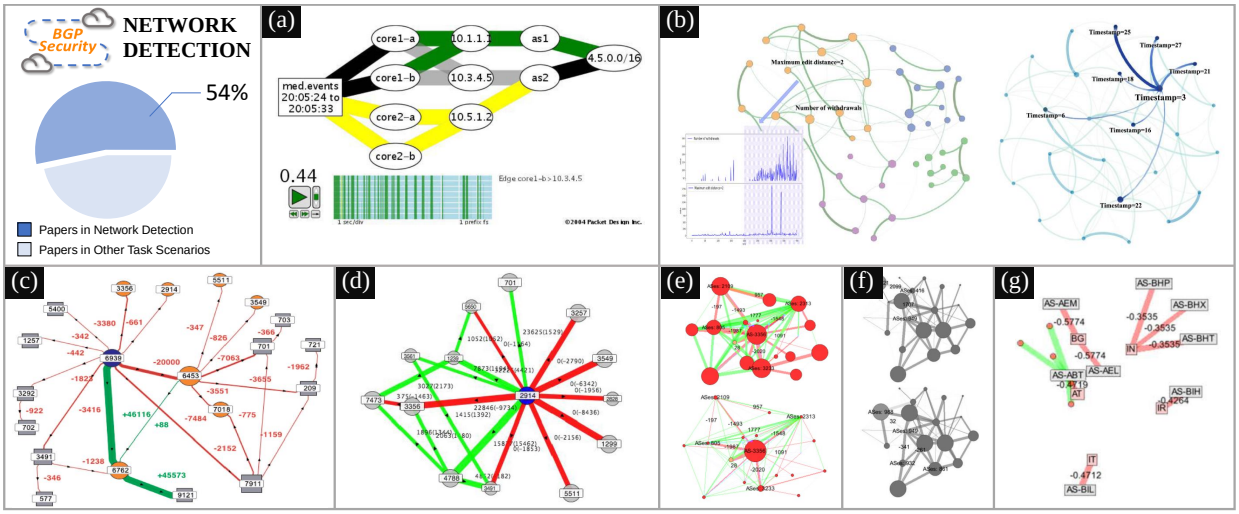

Fig. 3. Visualization of network detection. (a) TAMP [69] visualizes large-scale BGP routes for real-time anomaly detection in networks using a dynamic tree. (b) Multi-view [70] combines GAT with visual and temporal features analysis for BGP traffic anomaly detection. (c) Link-Rank [71] develops rank-change graphs to diagnose global network routing changes, aiding in dynamic detection. (d) Link Weights [72] employs expected weight and variance to pinpoint origins of routing changes in global networks. (e) AS-Graph [73] introduces hierarchical visualization to track path losses and gains in BGP routing. (f) BGPGraph [74] utilizes hierarchical clustering with IP-based weighted edges for detecting anomalies in BGP routing. (g) BGPfuse [75] features Parallel Coordinates and individual graphs for effective detection of BGP path hijacking.

message structure makes it challenging to directly identify the causes and sources of system anomalies. To detection and analyze BGP network anomalies, it is necessary to examine a series of factors, such as the quantity of BGP route announcements and withdrawals, AS-path length, and the number of rare ASes involved [20].

1) Anomaly Incident Detection: This category aims to identify anomalous events or behaviors in the network that deviate from the expected patterns of network activity, encompassing fluctuations in network traffic, configuration errors, sudden changes in routing paths, and may be the result of errors or operational mistakes. Researchers utilize a variety of anomaly detection techniques, including machine learning algorithms, statistical analysis, data mining, and rule-based methods, to monitor network traffic, event logs, and device behaviors for the purpose of detecting potential anomalous patterns. In the research depicted in Fig.3(b), Multi-view [70] utilized a weighted undirected graph for feature analysis to scrutinize the relationships among features extracted from the Nimda dataset, complemented by the employment of graph neural networks for the inference of network anomalies events.

2) Malware Intrusion Detection: Research in this category aims to identify malicious intrusion activities within a network. Malicious programs can infect routers or other network devices, leading to insecure network activities. This includes router malware, malicious BGP operations, and IP address spoofing. Intrusion detection relies on the identification of malicious programs characteristics, analysis of anomalous behaviors, and traffic analysis. These objectives can be achieved through the utilization of techniques such as signature-based detection, heuristic analysis, behavioral analysis, and deep learning.

A. Data Sources

Researchers typically extract data from various perspectives of BGP propagation, employing multiple anomaly detection and visual analysis methods to identify BGP anomalies. These data encompass both control plane and data plane aspects. The data sources encompass BGP raw data, routing registry databases, and other types of BGP data sources.

Routing Message Update data is utilized in both the control plane and data plane, encompassing timestamped messages such as BGP route update messages, TCP timestamps, ICMP timestamps, and more. These temporal indicators serve as valuable metrics for detecting suspicious prefixes. BGPmon [77] and relevant works collect relevant data sources to facilitate the detection of anomalous events, including prefix hijacking and fiber optic disruptions. Fig. 3(f) illustrates how BGPGraph [74] presents a time series of anomaly scores, aiding analysts in identifying and concentrating on crucial time periods for in-depth analysis. This enables the detection of anomalies of varying scales in BGP routing.

Routing Table Topology data is utilized to extract relevant information such as propagation paths in AS-PATH, global routing tables, and the flow of packets between actual nodes in the data plane. Subsequently, graph mining and visual analytics methods are applied to uncover anomalous routing propagation scenarios [54]. In the realm of Autonomous System (AS) network topology, the AS graph is typically constructed based on the AS paths found in BGP announcements. This process involves aggregating information from all announcements up to a specific point in time when a snapshot is captured to represent the network's state. As shown in Fig.3(e), AS-Graph [73] introduces a novel approach to visualize BGP route changes in a layered manner, incorporating information-theoretic measurement methods to quantify and optimize the analysis of route change events.

B. Visualization Techniques

Visual analytics techniques are extensively employed in the domain of anomaly detection, particularly for visualizing the large-scale structure of BGP routing. These techniques assist network operators in answering questions such as the nature of significant traffic updates, the origin of network

anomalies, and the impact of these anomalies on specific ASes. Link-Rank [71] develops rank-change graphs (see Fig. 3(c)) to effectively represent and diagnose routing changes in the global networks, facilitating detailed detection of network dynamics. As shown in Fig.3(d), Link-Weights [72] extends the link-rank technique, providing a network detection solution that utilizes expected weight and variance to pinpoint the origins of routing changes within the intricate global routing infrastructure. Network graph visualization effectively condenses the voluminous routing data into an intelligible format, thereby offering a concise summary of the temporal dynamics involved in routing changes.

Additionally, automatic visual analytics techniques can also aid in diagnosing challenging BGP events that are difficult to detect, such as minor fluctuations in large volumes of data, unexpected route path leakage, and persistent route oscillations. Cyclops [78] offers a visual representation of topology changes and provides detailed information about the BGP messages used to infer each change. It enhances verification by including all the links in the observed AS paths and the BGP messages that can be utilized for anomaly detection, thereby providing a more comprehensive validation. VAST [42] employs the Octo-Tree algorithm to construct AS topology analysis, representing AS numbers as points in a 3-dimensional space. This approach enables the detection of anomalies such as prefix hijacking and route leaks.

Multi-view correlated visual analysis enables the joint analysis of multiple aspects of data to identify and analyze anomalous events. In Fig.3(g), Bgpfuse [75] integrating various visualization approaches like parallel coordinates, feature graphs, and combined graphs. The integration of multiple visualization views enhances user's perceptual capabilities concerning BGP characteristics. Bgpfuse provides structural similarities and filtering capabilities, aiding in the detection of suspicious behavior while enabling focused investigations into the most compelling scenarios. BGPViewer [32] uses graph representations to explore BGP route changes. It visualizes the changes in ownership of each AS prefix within a specific time window and maps the variations in the number of prefixes used by each link in the AS graph to the size of graph nodes and the width of graph edges. As shown in Fig. 3(a), TAMP [69] introduces a dynamic tree to visualize a large-scale structure of some set of BGP routes enabling real-time detection of routing anomalies in complex network environments.

TABLE V
THE PRIMARY ANALYSIS PERSPECTIVES OF NETWORK DETECTION AND THE ASSOCIATED DATA SOURCES, VISUALIZATIONS AND TOOLS.

Data & Tools / Analysis perspectives	Data Sources	Visualization Techniques	Typical Works
Graphs Feature Analysis	Weighted undirected graphs, AS routing propagation	Graph neural networks, Graph Embedding	Multi-view [70], AS-Graph [73]
Anomaly Incident Sequencing	Time series data, BGP route updates	Time series analysis, Rank-change graphs	BGPGraph [74], Link-Rank [71], Link-Weights [72]
Layered Data Insights	Global routing tables, AS paths	Layered visualizations, TreeMap, 3D topology analysis	VAST [42], Cyclops [78]

C. Key Findings

The presence of multiple factors contributes to the occurrence of anomalies in the BGP system, making anomaly detection a complex task and anomaly mitigation challenging. Visual analytics applications in BGP security can aid in identifying anomalous behavior, improving the accuracy of anomaly detection, and facilitating timely responses to network failures and security threats, thereby enhancing network performance and ensuring network resilience. The existing research in the field of network detection primarily centers around network topology analysis, with some efforts focusing on time-series data analysis.

As shown in Table. V, combining different analysis perspectives from the table highlights the multifaceted approach to visual analytics in network detection. Graph feature analysis focuses on understanding network topology through weighted graphs and AS path information, enabling the identification of structural anomalies. Anomaly event sequence analysis leverages time series data to trace and diagnose network activities over time, relying on the detailed examination of BGP route updates. Layered data insights offer a high-level view of network dynamics, employing layered visualizations and 3D topology analysis to dissect complex routing anomalies. Researchers can enhance BGP anomaly detection algorithms continuously by incorporating multidimensional data, thereby improving the accuracy and efficiency of detection.

VII. Visual Analytics on Network Verification

Amidst the ever-growing intricacies of the global network ecosystem, network administrators face substantial challenges in ensuring the precise realization of network intentions during the design and configuration processes. The presence of erroneous network configurations can significantly compromise both the security and availability of the network, yet manual verification procedures are hindered by their onerous nature. The complexity of network verification algorithms can make them opaque and challenging to understand. Integrating visual analytics with network verification enables rapid validation and automated responses, thereby enhancing the security and availability of the network.

1) Data Plane Characterizing: The task of detailed and systematic examination and modeling of the data attributes within a network's data plane involves a comprehensive understanding and precise validation of traffic's nature coursing through a network. By scrutinizing the data plane, analysts construct a detailed depiction of the data, encompassing its structure, protocols, patterns of behavior, and compliance with network policies. Building upon the extraction of data plane characteristics, the integration of visual analytics with projection clustering and machine learning algorithms can expedite the comprehension of how data is managed, processed, and prioritized. This contributes to enhancing the interpretability of temporal network data while simultaneously serving as a foundational element for subsequent analytical processes. It also plays a crucial role in guiding network enhancements and troubleshooting, thereby ensuring the resilient and efficient management of data across the network infrastructure.

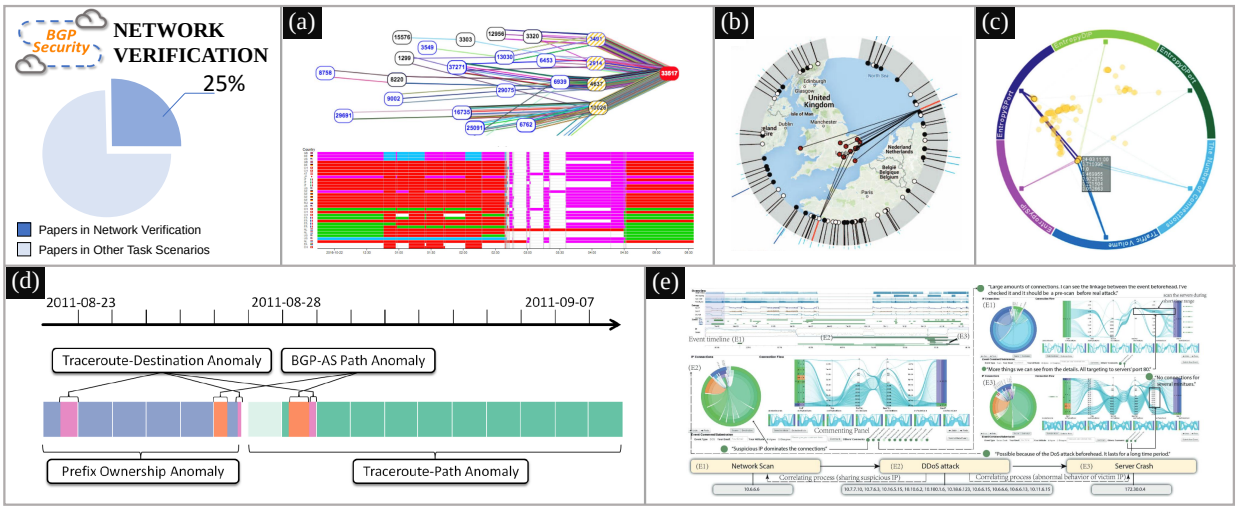

Fig. 4. Visualization of network verification. (a) Upstream Visibility [79] utilizes stacked area charts and matrices to effectively verify network routing outages and hijacks. (b) RoutingWatch [80] enables network operators to visually track and compare routing events, helping in swift problem resolution. (c) ENTVis [76] combines timeline, radviz, and matrix views to represent entropy-based metrics for detailed network traffic analysis. (d) VisTracer [81] offers a visual analytics framework with glyph and graph-based summaries for verifying large-scale network traceroute data. (e) OCEANS [33] aids in the verification of indirect threats by identifying and correlating events, focusing on multi-phase attack patterns and botnet behaviors.

Network operators can leverage data plane characterization to gain insights into performance bottlenecks, security vulnerabilities, and operational efficiencies. This activity is crucial for ensuring that the network operates as intended and is optimized to meet current and future demands. BGP-lens [82] utilizes multi-scale time-frequency analysis extraction such as Wavelet Transform and Median Filtering to assess the high-activity periods and stable update volume of the BGP system.

2) Control Plane Emulation: Creating a representation of the control plane's operations within a network simulation environment. Network emulation is considered an advanced iteration of network verification; it simulates real-world network operations to uncover device implementation errors that network verification alone may not detect. Within the realm of control plane network emulation, it typically involves variations in routing links and AS paths. Each arrival of a new routing message signifies potential route changes, encompassing announcements and withdrawals. Changes in AS paths can facilitate the discovery of insights into AS routing behaviors, such as the rarity of longer paths, and so forth. By emulating the control plane, network designers and operators can test and predict how network policies and routing protocols will behave under various conditions without the need for physical hardware. This practice is instrumental in prototyping network changes, verifying system integrity, and planning for capacity without impacting the live network. It allows for detailed experimentation and analysis, providing a safe space to understand the implications of new configurations and to ensure that they will behave as expected when deployed in the real world.

A. Data Sources

Network verification can be approached from two perspectives: the data plane and the control plane [83]. The data plane entails the verification of packet forwarding along BGP announced paths, ensuring their effective transmission [10]. The control plane primarily revolves around the rigorous validation of BGP's reception and transmission of control messages related to path announcement and withdrawal [84]. Time series data and network topology data correspond to the data sources of interest for the data plane and control plane.

Routing Message Update data is predominantly used for dynamic analysis, focusing on the temporal changes in the BGP system, such as the evolution of routing behavior over time. A series of control plane temporal features datasets is generated to facilitate the training of machine learning models for detecting BGP anomalous events [31]. The Fisher and minimum Redundancy Maximum Relevance (mRMR) algorithms are employed for feature filtering based on their strong correlation [85]. Machine learning techniques, including LSTM [86], Graph Attention Networks (GATs) [70], are employed to improve the real-time performance of BGP anomaly detection and enable the classification of unknown events. In the realm of analyzing routing behavior within BGP pressure flow intervals identified by algorithms, VisTracer [81] introduces a visual analytics framework that incorporates glyph and graph-based summaries to facilitate the security verification of large-scale time series inter-domain network traceroute data (see Fig.4(d)). RCAnalyzer [87] transforms the snapshots of a dynamic network into a series of connected triangular matrices. It then performs hierarchical clustering and optimal tree cutting on each matrix to detect network anomalies by identifying rare changes in the links between substructure nodes in the dynamic network.

In contrast, *Routing Table Topology* data, which is primarily used for static analysis, primarily focus on the given time slice of the BGP system's network topology. These methods analyze the structure, connectivity, and relationships between ASes in the BGP network. Network validation emulation can replicate the dynamic alterations in network routing paths. Upstream Visibility [79] utilizes stacked area charts and matrices for visualizing complex routing data. As shown in Fig.4(a), a routing topology-based graph provides a visual representation

of routing alterations during a defined time interval. It effectively facilitates the verification of network routing outages, hijacks, and other malicious attacks. Additional, as illustrated in Fig.4(b), RoutingWatch [80] facilitates network operators to visually trace and compare routing events across different network probes, geographic locations, and time frames, thereby identifying routing configurations and aiding in swift problem resolution.

By combining dynamic temporal data and static topological data analysis, researchers and network administrators could gain a comprehensive understanding of BGP systems, uncovering both temporal dynamics and network structure. The large-scale anomaly metric combines the entropy of edges and vertices, effectively capturing significant routing changes that indicate distributed anomalies. On the other hand, the small-scale anomaly metric combines four statistical metrics to collectively identify small-scale events deviating from normal behavior.

B. Visualization Techniques

Multivariate based visualizations leverage AS-path patterns, prefix distribution, and BGP update message features among other multi-dimensional data, to analyze different types of feature extraction. BGPfuse [75] employs parallel coordinates to visualize the multidimensional features of the BGP system and combines it with filtering functionality to analyze the correlation between features. For the extraction of multi-dimensional data features, dimensionality reduction projections, correlation matrices, and other visual analytics techniques can facilitate the interactive and rapid selection of features. As shown in Fig.4(c), ENTVis [76] integrates timeline, radviz, and matrix views to visually represent entropy-based metrics, enhancing the precision of network traffic verification by enabling detailed analysis of IP and port activities. Vahan et al. [88] utilized a correlation matrix to represent graph metrics, aiding in feature selection.

Graph based visualizations transform network data into node-link representations, enabling the exploration of in-depth data patterns through the optimization of visual features. Lad et al. [72] introduced a novel scheme that incorporates link weighting and change inference to enhance the Link-Rank method, thereby improving the detection of BGP peer session failures and route instability. NetFork [89] applies the BubbleSet techniques to aggregate network nodes and combines it with a multi-timeline visual representation to explore the dynamic changes in Internet routing. Cortese et al. [90] employ contour plots to visualize the hierarchical structure and path changes of ASes. By combining the contour plots with a map, where different contour lines represent ASes at different hierarchy levels, the flow of traffic across hierarchy levels can be clearly depicted.

Hierarchical based visualization can effectively represent hierarchical features of data, and IP prefix data is a typical example of such hierarchical data. Case study [45] presents an investigation into the Origin AS Change patterns by leveraging the hierarchical encoding of IP prefixes using quadtree and establishing associations between ASes and IPs. In addition, as shown in Fig.4(e), OCEANS [33] visualizes hierarchical IP data, enabling experts to efficiently identify and correlate complex events. This approach enhances the capacity for proactive detection of indirect threats by facilitating the discovery of external multi-phase attack patterns and the analysis of botnet behaviors.

TABLE VI
THE PRIMARY ANALYSIS PERSPECTIVES OF NETWORK VERIFICATION AND THE ASSOCIATED DATA SOURCES, VISUALIZATIONS AND TOOLS.

Data & Tools / Analysis perspectives	Data Sources	Visualization Techniques	Typical Works
Data Flow Checking	BGP routing update, network snapshots	Clustering, Hierarchical clustering, Timeline, Radviz, Matrix views	VisTracer [81], BGPfuse [75], RoutingWatch [80], OCEANS [33]
Operational Simulation	Routing links, AS paths	Network topology maps, routing path changes, AS path behaviors simulations	Radian [63]
Activity Pattern Analysis	BGP routing activity	Wavelet Transform, Median Filtering	BGP-lens [82]

C. Key Findings

The current research primarily revolves around network verification conducted within the control plane and data plane. Visualization techniques play a crucial role in aiding the verification of the network structure for BGP routing, identifying the origins of routing anomalies, and assessing their impact on specific autonomous systems. Through the use of data plane and control plane network verification, BGP system features can be effectively discovered and modeled. By combining dynamic and static analysis methods, as well as leveraging machine learning and visualization techniques, the stability and security analysis capabilities of BGP systems can be further enhanced. Conducting dynamic analysis of time-series data and static analysis of network topology data provides a comprehensive understanding of the BGP system. BGP message updates exhibit a significant volume, intricate structural characteristics, and continue to present challenges in aspects such as data storage, feature extraction, and algorithm design. To enhance the stability and security of the BGP system, it is imperative to expedite the deployment of security routing strategies such as RPKI and BGPSec.

As shown in Table. VI, the main analysis perspectives for network verification include activity pattern analysis, operational simulation, and data flow checking. These perspectives provide a structured approach to understanding and ensuring the integrity of network operations. Data flow checking delves into the specifics of data transmission within the network, ensuring that data flows as intended and complies with established policies. Operational simulation enables the emulation of network operations within a controlled environment, allowing for the testing and validation of network configurations and policies without impacting the actual network. Activity pattern analysis focus on deciphering the complex patterns of network behavior, particularly useful in identifying anomalies and optimizing network performance. Each of these perspectives employs specific tools and visualization techniques to facilitate a thorough examination and validation of network functions, ultimately contributing to a more secure and efficient network infrastructure.

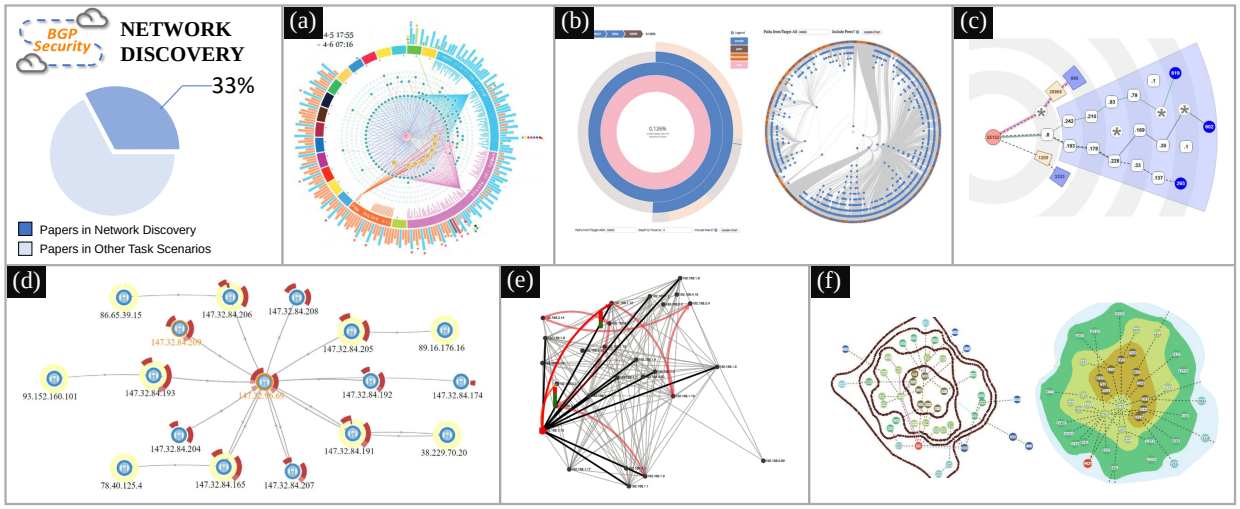

Fig. 5. Visualization of network discovery. (a) IDSRadar [91] displays abnormal network patterns using a radial graph to filter out false positives in security monitoring. (b) Contextual Navigation [4] merges topological mapping with commercial data for enhanced relationship analysis. (c) Radian [63] employs a radial graph for detailed analysis of evolving routing relationships. (d) HOCG [92] visualizes high-order anomalies correlations through a faceted Correlation Graph. (e) PERCIVAL [93] integrates proactive and reactive approaches in cyber-defense, representing network configurations and potential threats in critical infrastructures. (f) Topographic map [90] utilizes a topographic map metaphor to show the evolution of network relationships and IP prefix propagation.

VIII. Visual Analytics on Network Discovery

The continuous evolution of BGP system greatly influences the Internet's structure, performance, and dynamics. To gain insights into these complex dynamics, visual analytics emerges as a powerful approach, combining interactive visualizations and analytical techniques to explore and analyze large-scale BGP data [94].

1) Route Behavior Discovery: The evolution of BGP routing patterns over time refers to the understanding and analysis of how routing patterns in BGP networks change and develop [22]. As shown in Fig.5(c), Radian [63] defines a set of routing behavior analysis tasks, including route path tracing, topology distance calculation, reachability testing, single point failure detection, network peer relationship testing. This work also presents traceroute data in the form of a radial view cluster graph, allowing users to interact with Radian and observe the evolution of routing over time.

2) Business Relationship Discovery: The BGP system facilitates the exchange of routing reachability information among thousands of AS, forming the Internet's network topology. Each AS represents an independent company or organization. Measuring and analyzing the evolution of AS relationships can reveal their dynamic changes, interdependencies, and the overall network's evolutionary trends, providing insights to better understand and manage the Internet's routing system [69]. As shown in Fig. 5(b), Contextual Navigation [4] leverages the radial reingold-tilford tree design to analyze AS node provider-consumer relationships and identify the origins of route hijacking evolutions.

A. Data Sources

Evolutionary pattern analysis primarily focuses on *Routing Message Update* data to examine the temporal variations of networks. BGP-lens [82] incorporates Clothesline Detection and Prolonged Spike Detection to identify frequent anomalous updates in BGP routing and detect sustained burst events, enabling the detection of routing abnormal behaviors at multiple temporal scales. BGPATH [41] facilitates a comprehensive investigation into the dynamic variations occurring in interdomain routing. This is achieved through an analysis of the routing status associated with specific prefixes and the establishment of correlations with global Internet activities.

In addition, several research concentrate on dynamic network to analyze the temporal progression of *Routing Table Topology* data. As shown in Fig.5(a), IDSRadar [91] integrates IDS alerts and statistical information into its visual design for security alerting and real-time monitoring of large-scale network surveillance data. Network administrators can obtain an overview of the network security status from external histograms and radial graphs. In the event of identifying potential risks, users have the ability to retrospectively analyze specific risk types and detailed information by examining the interested time period.

Routing Event Log data also serves as an important means of presenting pattern evolution. Firewalls, as crucial network boundaries, have the capability to observe the evolution of incoming and outgoing messages [64], with relevant anomalous events being implicitly captured in the automatically recorded firewall logs. TVi [95] employs principal component analysis as a transformative method, while data entropy analysis serves as the foundation for the visualized data accessible to end users. This approach enables users to focus on relevant data pertinent to specific analysis objectives, such as anomaly detection, rather than scanning through extensive log files. As shown in Fig.5(d), HOCG [92] extracts event sequence data from network anomalies and introduces a faceted visualization of the High-Order Correlation Graph, which models the discovery of correlations among high-order anomalies.

Routing Spatial Mapping data could assist in locating and uncovering the propagation of routing in the actual physical space in network discovery. As shown in Fig5(f), Topographic map [90] utilizes a topographic map metaphor to depict the

hierarchical structure and routing paths of ISP, effectively illustrating the evolution of network relationships and the propagation of IP prefixes through the Internet.

B. Visualization Techniques

In the context of studying the evolution patterns of dynamic networks, several works have proposed novel visualization representations. Beck et al. [96] introduces Rapid Serial Visual Presentation (RSVP) into dynamic graph visual analytics, combining it with Parallel Edge Splatting [97] and incorporating temporal information. This approach enables the visualization of the temporal evolution of network structures within a single view. TimeArcs [98] utilizes force-directed layout to automatically generate a timeline that represents the dynamic relationships between entities in a network. RCAnalyzer [87] employ a triangular matrix representation of dynamic network snapshots to detect rare patterns in dynamic networks. The timeline view and matrix view provide visualizations that showcase the fundamental information and evolution of the network. As shown in Fig. 5(e), PERCIVAL framework [93] is designed to identify vulnerabilities, predict attack paths and evolution, provide critical situational awareness, and assess the evolution of risks in network systems using attack graphs. It assists operators in evaluating potential mitigation measures.

For time-series and log analysis optimization, Sequence Synopsis [99] is a technique that utilizes information theory-based minimum description length (MDL) to construct coarse-grained overviews of event sequence data. It also extracts sequential patterns and clusters event sequences to facilitate pattern matching across multiple levels of detail, enabling interactive data exploration. In the context of dynamic network analysis, Hadlak et al. [100] proposed an integrated approach combining computation, visualization, and interaction to uncover temporal patterns and facilitate exploration of both global-level and local-level problems. Their approach focuses on identifying sporadic changes in link quality, allowing for capturing variations in both network structure and temporal dynamics. Within the realm of spatio-temporal network attack data analysis, NetTimeView [101] seamlessly integrates network traffic and temporal information into a unified view. By employing multi-layered visualization techniques, it effectively processes extensive datasets, providing invaluable assistance to system administrators and network security analysts in conducting network forensic analysis. Bigfoot [39] employs filtering, organization, and analysis of BGP updates, along with map visualization, to assess various behaviors within BGP update streams. It incorporates a geographic polygon representation method to visualize IP network prefix announcements, enabling effective identification of route update behaviors in large-scale datasets.

C. Key Findings

In large-scale and complex network environments, network security analysts often tend to prioritize gaining an initial grasp of macro-level situational awareness. Subsequently, they delve into a more detailed analysis, comprehensively examining AS business relationships, network evolution patterns, regional routing load capacities, and other related aspects. Experts consider visual analysis tools highly effective and practical for studying route propagation and path exploration. For instance, tools like Radian [63] support the analysis of available data from traceroutes, contributing to better insights. Additionally, users believe that summarization and interactivity are essential when analyzing a larger volume of cases. They express a desire for enhanced interactivity in comparing network topology elements.

TABLE VII
THE PRIMARY ANALYSIS PERSPECTIVES OF NETWORK DISCOVERY AND THE ASSOCIATED DATA SOURCES, VISUALIZATIONS AND TOOLS.

Analysis perspectives \ Data & Tools	Data Sources	Visualization Techniques	Typical Works
Network Relationship Analysis	AS relationship data, Route hijacking origins	Radial reingold-tilford tree, Geographic polygon representation	Contextual Navigation [4], Bigfoot [39]
Route Behavior Analysis	BGP update data, Traceroute data	Radial view cluster graph, Timeline view, Matrix view	TimeArcs [98], RCAnalyzer [87]
Multi-granularity Event Correlation	Routing topology data, Routing event Log data	High-Order correlation graph, Topographic map metaphor	BGP-lens [82], BGPATH [41], IDSRadar [91], HOCG [92]

As shown in Table. VII, the challenges associated with network discovery involve addressing large-scale BGP data, identifying and analyzing dynamic changes in network topology and behavior, implementing efficient monitoring and anomaly detection mechanisms, as well as offering intuitive and interactive visualization tools. The integration of interactive visualization and analytical methods in visual analytics techniques provides a profound understanding of the BGP network's structure, performance, and dynamics. Technologies such as Clothesline Detection, Prolonged Spike Detection, and AS Core Graph enable the detection and analysis of anomalous routing behaviors and AS connectivity changes. Subsequent research should explore the impact of external factors such as security threats and network attacks on BGP pattern evolution and develop robust mechanisms for detecting and mitigating these threats. Integrating machine learning and artificial intelligence techniques can enhance the automated analysis of BGP pattern evolution and provide proactive measures to enhance the stability and security of BGP networks.

IX. Discussion and Open Challenges

Despite summarizing key findings in the previous sections, we further present comprehensive insights derived from the synthesis of the inter-domain security visualization survey. Specifically, we examine the current state-of-the-art in visualization practices concerning BGP security and identify potential avenues for future research. The analysis of inter-domain routing network encompassing tasks including monitoring, detecting, verifying and discovery, extensively employs automated analytical methods. The scalability of both automatic analysis methods and visualizations emerges as another critical issue. While conducting detailed traffic analysis on large traffic links is computationally infeasible, many data visualization methods struggle with visualizing large data volumes. Given that the network's health is largely dependent on the ability to analyze its behavior, addressing both scalability challenges is imperative. The widespread adoption of IPv6, combined with

the increasing number of internet users and devices, introduces significant challenges. Firstly, there is the daunting task of processing and deriving insights from the rapidly growing volume of data. Secondly, the complexity of discerning genuine cyber threats from a multitude of alerts is escalating. Integrating visual analysis techniques with domain expertise and automated results, administrators could greatly enhance the understanding of complex network systems. This empowers them to make informed decisions and undertake necessary adjustments and optimizations to ensure the network's reliability, stability, and security.

However, daily occurrence of security threats necessitates enhancing security mechanisms and expanding interactive visual analytics techniques. Visualizing BGP security involves handling substantial data and complex network topologies, requiring technical proficiency and algorithmic expertise. Limited individuals engaged in interdisciplinary research led to a scarcity of new developments in this domain.

Furthermore, the frequent and voluminous updates of BGP data present substantial challenges to the performance and efficiency of visualization tools. To address these issues, solutions such as the integration of blockchain technology and distributed storage systems are proposed for real-time data stream processing. Additionally, employing compression techniques and data summarization algorithms can significantly reduce storage requirements and expedite data access. Efficient algorithm and model design is crucial for BGP data, especially when utilizing visual analytics techniques, anomaly detection algorithms, and machine learning methods. These techniques are essential for identifying routing anomalies such as hijacking, leakage, and route flapping, enabling timely detection and response to security threats.

X. Conclusion

The Border Gateway Protocol is indeed the primary inter-domain routing protocol used in the infrastructure of the Internet. Due to the inherent vulnerabilities in the design of BGP, attackers can easily exploit the routing system through prefix hijacking techniques to engage in malicious activities. Researchers and engineers are collectively devoted to enhancing the security of BGP through the advancement of deployments such as RPKI and BGPSec. Our survey establishes an analytical framework that spans from monitoring to response, from analysis to optimization, and from local to global perspectives. We further present the taxonomy related to inter-domain routing security visualization by systematically categorizing target users, security threats task scenarios, data sources, and visualization techniques.

Our study contributes to elucidating and examining security aspects in inter-domain routing through the utilization of visual analytics methodologies. At the end of each task scenario, we summarize with a series of pertinent key findings. Furthermore, we discuss current practices and future research opportunities in the field of IDRS visualization, based on our analysis of the gathered studies. The inter-domain routing security continues to be an enduring subject of close examination, owing to its paramount role in preserving the security and robustness of the global routing ecosystem.

Acknowledgments

The work is partly supported by the National Key Research and Development Program of China (2022YFB3104800), Zhejiang Provincial Natural Science Foundation of China (LR23F020003 and LTGG23F020005), Fundamental Research Funds for the Provincial Universities of Zhejiang(RF-B2023006), and National Natural Science Foundation of China (62372411). Guodao Sun is the corresponding author.

References

[1] P. Sermpezis, V. Kotronis, P. Gigis, X. Dimitropoulos, D. Cicalese, A. King, and A. Dainotti, "ARTEMIS: Neutralizing BGP Hijacking Within a Minute," *IEEE/ACM Transactions on Networking*, vol. 26, no. 6, pp. 2471–2486, 2018.

[2] A. Ulmer, D. Sessler, and J. Kohlhammer, "ProBGP: Progressive Visual Analytics of Live BGP Updates," *Computer Graphics Forum*, vol. 40, no. 3, pp. 37–48, 2021.

[3] M. Syamkumar, Y. Gullapalli, W. Tang, P. Barford, and J. Sommers, "BigBen: Telemetry Processing for Internet-Wide Event Monitoring," *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 2625–2638, 2022.

[4] C. C. Gray, P. D. Ritsos, and J. C. Roberts, "Contextual Network Navigation to Provide Situational Awareness for Network Administrators," in *Proceedings of IEEE Symposium on Visualization for Cyber Security*, 2015, pp. 1–8.

[5] J. Jin, "BGP Route Leak Prevention Based on BGPsec," in *Proceedings of IEEE Vehicular Technology Conference*, 2018, pp. 1–6.

[6] T. Chung, E. Aben, T. Bruijnzeels, B. Chandrasekaran, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, R. van Rijswijk-Deij, J. Rula, and N. Sullivan, "RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins," in *Proceedings of the Internet Measurement Conference*, 2019, pp. 406–419.

[7] M. Zhao, S. Smith, and D. Nicol, "The Performance Impact of BGP Security," *IEEE Network*, vol. 19, no. 6, pp. 42–48, 2005.

[8] A. Mitseva, A. Panchenko, and T. Engel, "The State of Affairs in BGP Security: A Survey of Attacks and Defenses," *Computer Communications*, vol. 124, pp. 45–60, 2018.

[9] Y. Gilad, A. Cohen, A. Herzberg, M. Schapira, and H. Shulman, "Are We There Yet? On RPKI's Deployment and Security," in *Proceedings of Annual Network and Distributed System Security Symposium*, 2017, pp. 1–15.

[10] K. Butler, T. R. Farley, P. McDaniel, and J. Rexford, "A Survey of BGP Security Issues and Solutions," *Proceedings of the IEEE*, vol. 98, no. 1, pp. 100–122, 2010.

[11] L. Mastilak, P. Helebrandt, M. Galinski, and I. Kotuliak, "Secure Inter-Domain Routing Based on Blockchain: A Comprehensive Survey," *Sensors*, vol. 22, no. 4, pp. 1–26, 2022.

[12] J. Raynor, T. Crnovrsanin, S. D. Bartolomeo, L. South, D. Saffo, and C. Dunne, "The State of the Art in BGP Visualization Tools: A Mapping of Visualization Techniques to Cyberattack Types," *IEEE Transactions on Visualization and Computer Graphics*, vol. 29, no. 1, pp. 1059–1069, 2023.

[13] G. Huston, M. Rossi, and G. Armitage, "Securing BGP - A Literature Survey," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, pp. 199–222, 2011.

[14] C. Testart, "Reviewing a Historical Internet Vulnerability: Why Isn't BGP More Secure and What Can We Do About it?" in *Proceedings of Research Conference on Communication, Information and Internet Policy*, 2018, pp. 1–36.

[15] N. Rodday, Í. Cunha, R. Bush, E. Katz-Bassett, G. D. Rodosek, T. C. Schmidt, and M. Wählisch, "The Resource Public Key Infrastructure (RPKI): A Survey on Measurements and Future Prospects," *IEEE Transactions on Network and Service Management*, pp. 1–1, 2023.

[16] M. S. Siddiqui, D. Montero, R. Serral-Gracià, X. Masip-Bruin, and M. Yannuzzi, "A Survey on the Recent Efforts of the Internet Standardization Body for Securing Inter-domain Routing," *Computer Networks*, vol. 80, pp. 1–26, 2015.

[17] P. Sermpezis, V. Kotronis, A. Dainotti, and X. Dimitropoulos, "A Survey among Network Operators on BGP Prefix Hijacking," *ACM SIGCOMM Computer Communication Review*, vol. 48, no. 1, pp. 64–69, 2018.

[18] H. Ballani, P. Francis, and X. Zhang, "A Study of Prefix Hijacking and Interception in the Internet," *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 4, pp. 265–276, 2007.

[19] A. Khan, H. Kim, T. Kwon, and Y. Choi, "A Comparative Study on IP Prefixes and Their Origin Ases in BGP and the IRR," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 3, pp. 16–24, 2013.

[20] B. Al-Musawi, P. Branch, and G. Armitage, "BGP Anomaly Detection Techniques: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 377–396, 2017.

[21] A. Komadina, Ž. Mihajlović, and S. Groš, "Analysis of the Design Space for Cybersecurity Visualizations in VizSec," in *Proceedings of IEEE Symposium on Visualization for Cyber Security*, 2022, pp. 1–11.

[22] 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, 2012.

[23] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "An Evaluation Framework for Network Security Visualizations," *Computers & Security*, vol. 84, pp. 70–92, 2019.

[24] E. Biersack, Q. Jacquemart, F. Fischer, J. Fuchs, O. Thonnard, G. Theodoridis, D. Tzovaras, and P.-A. Vervier, "Visual Analytics for BGP Monitoring and Prefix Hijacking Identification," *IEEE Network*, vol. 26, no. 6, pp. 33–39, 2012.

[25] V. T. Guimarães, C. M. D. S. Freitas, R. Sadre, L. M. R. Tarouco, and L. Z. Granville, "A Survey on Information Visualization for Network and Service Management," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 285–323, 2016.

[26] J. Youn, H. Oh, J. Kang, and D. Shin, "Research on Cyber IPB Visualization Method Based on BGP Archive Data for Cyber Situation Awareness," *KSII Transactions on Internet and Information Systems*, vol. 15, no. 2, pp. 749–766, 2021.

[27] R. Tamassia, B. Palazzi, and C. Papamanthou, "Graph Drawing for Security Visualization," in *Proceedings of Graph Drawing*, 2009, pp. 2–13.

[28] B. Shneiderman and A. Aris, "Network Visualization by Semantic Substrates," *IEEE Transactions on Visualization and Computer Graphics*, vol. 12, no. 5, pp. 733–740, 2006.

[29] A. Ulmer, J. Kohlhammer, and H. Shulman, "Towards Enhancing the Visual Analysis of Interdomain Routing," in *Proceedings of International Conference on Information Visualization Theory and Applications*, 2017, pp. 209–216.

[30] L. Wang, X. Zhao, D. Pei, R. Bush, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, "Observation and Analysis of BGP Behavior under Stress," in *Proceedings of ACM SIGCOMM Workshop on Internet Measurment*, 2002, pp. 183–195.

[31] P. Fonseca, E. S. Mota, R. Bennesby, and A. Passito, "BGP Dataset Generation and Feature Extraction for Anomaly Detection," in *Proceedings of IEEE Symposium on Computers and Communications*, 2019, pp. 1–6.

[32] S. Papadopoulos, K. Moustakas, and D. Tzovaras, "BGPViewer: Using Graph Representations to Explore BGP Routing Changes," in *Proceedings of International Conference on Digital Signal Processing*, 2013, pp. 1–6.

[33] S. Chen, C. Guo, X. Yuan, F. Merkle, H. Schaefer, and T. Ertl, "OCEANS: Online Collaborative Explorative Analysis on Network Security," in *Proceedings of IEEE Symposium on Visualization for Cyber Security*, 2014, pp. 1–8.

[34] M. Schuchard, A. Mohaisen, D. F. Kune, N. Hopper, Y. Kim, and E. Y. Vasserman, "Losing Control of the Internet: Using the Data Plane to Attack the Control Plane," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2010, pp. 726–728.

[35] N. Danneman and R. Gove, "Tuning Automatic Summarization for Incident Report Visualization," in *Proceedings of IEEE Pacific Visualization Symposium*, 2022, pp. 191–195.

[36] A. Cockburn, A. Karlson, and B. B. Bederson, "A Review of Overview+Detail, Zooming, and Focus+Context Interfaces," *ACM Computing Surveys*, vol. 41, no. 1, pp. 1–31, 2009.

[37] B. Al-Musawi, P. Branch, and G. Armitage, "Detecting BGP Instability Using Recurrence Quantification Analysis (RQA)," in *Proceedings of IEEE International Performance Computing and Communications Conference*, 2015, pp. 1–8.

[38] Q. Li, J. Liu, Y. Hu, M. Xu, and J. Wu, "BGP with BGPsec: Attacks and Countermeasures," *IEEE Network*, vol. 33, no. 4, pp. 194–200, 2019.

[39] M. Syamkumar, R. Durairajan, and P. Barford, "Bigfoot: A Geo-based Visualization Methodology for Detecting BGP Threats," in *Proceedings of IEEE Symposium on Visualization for Cyber Security*, 2016, pp. 1–8.

[40] M. Lad, A. Nanavati, D. Massey, and L. Zhang, "An Algorithmic Approach to Identifying Link Failures," in *Proceedings of IEEE Pacific Rim International Symposium on Dependable Computing*, 2004, pp. 25–34.

[41] L. Cittadini, T. Refice, A. Campisano, G. D. Battista, and C. Sasso, "Measuring and Visualizing Interdomain Routing Dynamics with BGPATH," in *Proceedings of IEEE Symposium on Computers and Communications*, 2008, pp. 780–787.

[42] J. Oberheide, M. Karir, and D. Blazakis, "VAST: Visualizing Autonomous System Topology," in *Proceedings of International Workshop on Visualization for Computer Security*, 2006, pp. 71–80.

[43] N. H. Hammood and B. Al-Musawi, "Using BGP Features Towards Identifying Type of BGP Anomaly," in *Proceedings of International Congress of Advanced Technology and Engineering*, 2021, pp. 1–10.

[44] M. Lad, L. Zhang, and D. Massey, "Link-Rank: A Graphical Tool for Capturing BGP Routing Dynamics," in *Proceedings of IEEE/IFIP Network Operations and Management Symposium*, 2004, pp. 627–640.

[45] S. T. Teoh, K.-L. Ma, S. Wu, and X. Zhao, "Case Study: Interactive Visualization for Internet Security," in *Proceedings of IEEE Visualization*, 2002, pp. 505–508.

[46] N. Tovanich, N. Heulot, J.-D. Fekete, and P. Isenberg, "Visualization of Blockchain Data: A Systematic Review," *IEEE Transactions on Visualization and Computer Graphics*, vol. 27, no. 7, pp. 3135–3152, 2021.

[47] Y. Shi, Y. Liu, H. Tong, J. He, G. Yan, and N. Cao, "Visual Analytics of Anomalous User Behaviors: A Survey," *IEEE Transactions on Big Data*, vol. 8, no. 2, pp. 377–396, 2022.

[48] Y. Wang, Z. Zhu, L. Wang, G. Sun, and R. Liang, "Visualization and Visual Analysis of Multimedia Data in Manufacturing: A Survey," *Visual Informatics*, vol. 6, no. 4, pp. 12–21, 2022.

[49] G. Zhang, Z. Zhu, S. Zhu, R. Liang, and G. Sun, "Towards a better understanding of the role of visualization in online learning: A review," *Visual Informatics*, vol. 6, no. 4, pp. 22–33, 2022.

[50] W. Aigner, S. Miksch, W. Müller, H. Schumann, and C. Tominski, "Visual Methods for Analyzing Time-Oriented Data," *IEEE Transactions on Visualization and Computer Graphics*, vol. 14, no. 1, pp. 47–60, 2008.

[51] R. Gove, "Automatic Narrative Summarization for Visualizing Cyber Security Logs and Incident Reports," *IEEE Transactions on Visualization and Computer Graphics*, vol. 28, no. 1, pp. 1182–1190, 2022.

[52] W. Deng, P. Zhu, and X. Lu, "ROUSSEAU: A Monitoring System for Inter-domain Routing Security," in *Proceedings of Annual Communication Networks and Services Research Conference*, 2008, pp. 255–262.

[53] B. Huffaker, D. Plummer, D. Moore, and K. Claffy, "Topology Discovery by Active Probing," in *Proceedings of Symposium on Applications and the Internet Workshops*, 2002, pp. 90–96.

[54] 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 International Workshop on Visualization for Computer Security*, 2006, pp. 81–90.

[55] A. Dainotti, K. Benson, A. King, B. Huffaker, E. Glatz, X. Dimitropoulos, P. Richter, A. Finamore, and A. C. Snoeren, "Lost in Space: Improving Inference of IPv4 Address Space Utilization," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 6, pp. 1862–1876, 2016.

[56] Y. Zhang, Z. Zhang, Z. M. Mao, C. Hu, and B. M. Maggs, "On the Impact of Route Monitor Selection," in *Proceedings of the ACM SIGCOMM Conference on Internet Measurement*, 2007, pp. 215–220.

[57] L. Colitti, G. D. Battista, F. Mariani, M. Patrignani, and M. Pizzonia, "Visualizing Interdomain Routing with BGPlay," *Journal on Graph Algorithms and Applications*, vol. 9, no. 1, pp. 117–148, 2005.

[58] 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 ACM Workshop on Visualization and Data Mining for Computer Security*, 2004, pp. 35–44.

[59] A. Kalwar, M. H. Bhuyan, D. K. Bhattacharyya, Y. Kadobayashi, E. Elmroth, and J. K. Kalita, "TVis: A Light-weight Traffic Visualization System for DDoS Detection," in *Proceedings of International Joint Symposium on Artificial Intelligence and Natural Language Processing*, 2019, pp. 1–6.

[60] S. T. Teoh, K.-L. Ma, and S. F. Wu, "A Visual Exploration Process for the Analysis of Internet Routing Data," in *Proceedings of IEEE Visualization*, 2003, pp. 523–530.

[61] J. R. Goodall, E. D. Ragan, C. A. Steed, J. W. Reed, G. D. Richardson, K. M. Huffer, R. A. Bridges, and J. A. Laska, "Situ: Identifying and Explaining Suspicious Behavior in Networks," *IEEE Transactions on*

Visualization and Computer Graphics, vol. 25, no. 1, pp. 204–214, 2019.

[62] F. Mansmann, D. A. Keim, S. C. North, B. Rexroad, and D. Sheleheda, "Visual Analysis of Network Traffic for Resource Planning, Interactive Monitoring, and Interpretation of Security Threats," *IEEE Transactions on Visualization and Computer Graphics*, vol. 13, no. 6, pp. 1105–1112, 2007.

[63] M. Candela, M. D. Bartolomeo, G. D. Battista, and C. Squarcella, "Radian: Visual Exploration of Traceroutes," *IEEE Transactions on Visualization and Computer Graphics*, vol. 24, no. 7, pp. 2194–2208, 2018.

[64] M. Schufrin, H. Lücke-Tieke, and J. Kohlhammer, "Visual Firewall Log Analysis - At the Border Between Analytical and Appealing," in *Proceedings of IEEE Symposium on Visualization for Cyber Security*, 2022, pp. 1–11.

[65] A. Ulmer, M. Schufrin, D. Sessler, and J. Kohlhammer, "Visual-Interactive Identification of Anomalous IP-Block Behavior Using Geo-IP Data," in *Proceedings of IEEE Symposium on Visualization for Cyber Security*, 2018, pp. 1–8.

[66] M. Candela, M. Bartolomeo, G. Battista, and C. Squarcella, "Dynamic Traceroute Visualization at Multiple Abstraction Levels," in *Proceedings of International Symposium on Graph Drawing*, 2013, pp. 496–507.

[67] 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, 2006.

[68] F. Fischer, J. Davey, J. Fuchs, O. Thonnard, J. Kohlhammer, and D. A. Keim, "A Visual Analytics Field Experiment to Evaluate Alternative Visualizations for Cyber Security Applications," in *Proceedings of EuroVis Workshop on Visual Analytics*, 2014, pp. 1–5.

[69] T. Wong, V. Jacobson, and C. Alaettinoglu, "Internet Routing Anomaly Detection and Visualization," in *Proceedings of International Conference on Dependable Systems and Networks*, 2005, pp. 172–181.

[70] S. Peng, J. Nie, X. Shu, Z. Ruan, L. Wang, Y. Sheng, and Q. Xuan, "A Multi-view Framework for BGP Anomaly Detection via Graph Attention Network," *Computer Networks*, vol. 214, p. 109129, 2022.

[71] 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, 2006.

[72] M. Lad, R. Oliveira, D. Massey, and L. Zhang, "Inferring the Origin of Routing Changes Using Link Weights," in *Proceedings of IEEE International Conference on Network Protocols*, 2007, pp. 93–102.

[73] S. Papadopoulos, K. Moustakas, and D. Tzovaras, "Hierarchical Visualization of BGP Routing Changes Using Entropy Measures," in *Proceedings of Advances in Visual Computing*, 2012, pp. 696–705.

[74] S. Papadopoulos, K. Moustakas, A. Drosou, and D. Tzovaras, "Border Gateway Protocol Graph: Detecting and Visualising Internet Routing Anomalies," *IET Information Security*, vol. 10, no. 3, pp. 125–133, 2016.

[75] 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*, 2013, pp. 57–64.

[76] F. Zhou, W. Huang, Y. Zhao, Y. Shi, X. Liang, and X. Fan, "ENTVis: A Visual Analytic Tool for Entropy-Based Network Traffic Anomaly Detection," *IEEE Computer Graphics and Applications*, vol. 35, no. 6, pp. 42–50, 2015.

[77] H. Yan, R. Oliveira, K. Burnett, D. Matthews, L. Zhang, and D. Massey, "BGPmon: A Real-Time, Scalable, Extensible Monitoring System," in *Proceedings of Cybersecurity Applications & Technology Conference for Homeland Security*, 2009, pp. 212–223.

[78] Y. Chi, R. Oliveira, and L. Zhang, "Cyclops: The AS-level Connectivity Observatory," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 5, pp. 5–16, 2008.

[79] M. Candela, G. D. Battista, and L. Marzialetti, "Multi-view Routing Visualization for the Identification of BGP Issues," *Journal of Computer Languages*, vol. 58, p. 100966, 2020.

[80] D. Ceneda, M. D. Bartolomeo, V. D. Donato, M. Patrignani, M. Pizzonia, and M. Rimondini, "RoutingWatch: Visual Exploration and Analysis of Routing Events," in *Proceedings of IEEE/IFIP Network Operations and Management Symposium*, 2016, pp. 591–597.

[81] 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 International Symposium on Visualization for Cyber Security*, 2012, pp. 80–87.

[82] B. A. Prakash, N. Valler, D. Andersen, M. Faloutsos, and C. Faloutsos, "BGP-lens: Patterns and Anomalies in Internet Routing Updates," in *Proceedings of ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2009, pp. 1315–1324.

[83] Y. Li, X. Yin, Z. Wang, J. Yao, X. Shi, J. Wu, H. Zhang, and Q. Wang, "A Survey on Network Verification and Testing With Formal Methods: Approaches and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 940–969, 2019.

[84] M. Kowalski and W. Mazurczyk, "Toward the Mutual Routing Security in Wide Area Networks: A Scoping Review of Current Threats and Countermeasures," *Computer Networks*, vol. 230, p. 109778, 2023.

[85] N. M. Al-Rousan and L. Trajković, "Machine Learning Models for Classification of BGP Anomalies," in *Proceedings of IEEE International Conference on High Performance Switching and Routing*, 2012, pp. 103–108.

[86] M. Cheng, Q. Li, J. Lv, W. Liu, and J. Wang, "Multi-Scale LSTM Model for BGP Anomaly Classification," *IEEE Transactions on Services Computing*, vol. 14, no. 3, pp. 765–778, 2021.

[87] J. Pan, D. Han, F. Guo, D. Zhou, N. Cao, J. He, M. Xu, and W. Chen, "RCAnalyzer: Visual Analytics of Rare Categories in Dynamic Networks," *Frontiers of Information Technology & Electronic Engineering*, vol. 21, no. 4, pp. 491–506, 2020.

[88] V. Yoghourdjian, Y. Yang, T. Dwyer, L. Lawrence, M. Wybrow, and K. Marriott, "Scalability of Network Visualisation from a Cognitive Load Perspective," *IEEE Transactions on Visualization and Computer Graphics*, vol. 27, no. 2, pp. 1677–1687, 2021.

[89] V. D. Donato, M. Patrignani, and C. Squarcella, "NetFork: Mapping Time to Space in Network Visualization," in *Proceedings of the International Working Conference on Advanced Visual Interfaces*, 2016, pp. 92–99.

[90] P. F. Cortese, G. Di Battista, A. Moneta, M. Patrignani, and M. Pizzonia, "Topographic Visualization of Prefix Propagation in the Internet," *IEEE Transactions on Visualization and Computer Graphics*, vol. 12, no. 5, pp. 725–732, 2006.

[91] 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.

[92] J. Yan, L. Shi, J. Tao, X. Yu, Z. Zhuang, C. Huang, R. Yu, P. Su, C. Wang, and Y. Chen, "Visual Analysis of Collective Anomalies Using Faceted High-Order Correlation Graphs," *IEEE Transactions on Visualization and Computer Graphics*, vol. 26, no. 7, pp. 2517–2534, 2020.

[93] M. Angelini, N. Prigent, and G. Santucci, "PERCIVAL: Proactive and Reactive Attack and Response Assessment for Cyber Incidents Using Visual Analytics," in *Proceedings of IEEE Symposium on Visualization for Cyber Security*, 2015, pp. 1–8.

[94] M. Luckie, B. Huffaker, A. Dhamdhere, V. Giotsas, and K. Claffy, "AS Relationships, Customer Cones, and Validation," in *Proceedings of the ACM Internet Measurement Conference*, 2013, pp. 243–256.

[95] A. Boschetti, L. Salgarelli, C. Muelder, and K.-L. Ma, "TVi: A Visual Querying System for Network Monitoring and Anomaly Detection," in *Proceedings of International Symposium on Visualization for Cyber Security*, 2011, pp. 1–10.

[96] F. Beck, M. Burch, C. Vehlow, S. Diehl, and D. Weiskopf, "Rapid Serial Visual Presentation in Dynamic Graph Visualization," in *Proceedings of IEEE Symposium on Visual Languages and Human-Centric Computing*, 2012, pp. 185–192.

[97] M. Burch, C. Vehlow, F. Beck, S. Diehl, and D. Weiskopf, "Parallel Edge Splatting for Scalable Dynamic Graph Visualization," *IEEE Transactions on Visualization and Computer Graphics*, vol. 17, no. 12, pp. 2344–2353, 2011.

[98] T. N. Dang, N. Pendar, and A. G. Forbes, "TimeArcs: Visualizing Fluctuations in Dynamic Networks," *Computer Graphics Forum*, vol. 35, no. 3, pp. 61–69, 2016.

[99] Y. Chen, P. Xu, and L. Ren, "Sequence Synopsis: Optimize Visual Summary of Temporal Event Data," *IEEE Transactions on Visualization and Computer Graphics*, vol. 24, no. 1, pp. 45–55, 2018.

[100] S. Hadlak, H. Schumann, C. H. Cap, and T. Wollenberg, "Supporting the Visual Analysis of Dynamic Networks by Clustering Associated Temporal Attributes," *IEEE Transactions on Visualization and Computer Graphics*, vol. 19, no. 12, pp. 2267–2276, 2013.

[101] A. Shrestha, Y. Zhu, and K. Manandhar, "NetTimeView: Applying Spatio-temporal Data Visualization Techniques to DDoS Attack Analysis," in *Proceedings of Advances in Visual Computing*, 2014, pp. 357–366.

Jingwei Tang is currently a Ph.D. student in the College of Computer Science and Technology, Zhejiang University of Technology, HangZhou, China. He received his B.E. degree in communication engineering from Zhejiang University of Technology. His main research interests are data mining and information visualization.

Guodao Sun is a professor at the College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou, China. He received the B.Sc. in computer science and technology, and Ph.D. degree in control science and engineering both from Zhejiang University of Technology. His main research interests are urban visualization, visual analytics of social media, and information visualization.

Jiahui Chen is currently working toward the MS degree with the College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou, China. His main research interests are data mining and information visualization.

Gefei Zhang is currently a Ph.D student at the College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou, China. She received Bachelor of Education in education technology in College of Educational Science and Technology, Zhejiang University of Technology. Her main research interests include information visualization and educational data mining.

Qi Jiang is currently working toward the Ph.D. degree in computer science and technology from the Zhejiang University of Technology, Hangzhou, China. He received the B.E. degree in electrical engineering and automation from the Zhejiang University of Technology, in 2019. His research interests lie in natural language interface for visualization and intelligent visualization. Contact him at jiangqi@zjut.edu.cn.

Yanbiao Li received the B.S. degree in mathematics and the Ph.D. degree in computer science from Hunan University in 2009 and 2016, respectively. He is currently an Associate Professor with the Computer Network Information Center (CNIC), Chinese Academy of Sciences (CAS), and the University of Chinese Academy of Sciences (UCAS). His research interests include networked systems, packet processing algorithms and routing security.

Guangxing Zhang received the B.S. and Ph.D. degrees from Hunan University in 2002 and 2011, respectively. He joined the Institute of Computing Technology, Chinese Academy of Sciences (ICT, CAS) in 2007 and is currently serving as an Associate Professor. His research interests include SDN/NFV system, Internet measurement, and future Internet architecture.

Jian Liu received the Ph.D. degree from Louisiana State University in 2021. He is currently an Assistant Professor in the Department of Computer Science and Technology at Zhejiang University of Technology. His research interests include flash-based storage/caching systems, time-series data storage, data deduplication, object-based storage, etc.

Haixia Wang received her Ph.D. degree in 2012 from Nanyang Technological University, Singapore. She is currently a professor at Zhejiang University of Technology. Her research interests include image processing and pattern recognition.

Ronghua Liang received the Ph.D. in computer science from Zhejiang University. He worked as a research fellow at the University of Bedfordshire, UK, from April 2004 to July 2005 and as a visiting scholar at the University of California, Davis, US, from March 2010 to March 2011. He is currently a professor of College of Computer Science and Technology, Zhejiang University of Technology, China. His research interests include Visual Analytics and Computer Vision.