计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190500169

网络安全态势感知研究现状与发展趋势的图谱分析

白 雪 努尔布力 王亚东
新疆大学信息科学与工程学院 乌鲁木齐 830046
(409429237@qq.com)

摘 要 文中以 Web of Science 中 1999—2019 年收录的 2456 篇以网络安全态势感知为主题的文献作为数据来源,主要运用 CiteSpace 可视化工具,基于图谱对国家与机构合作、文献共被引、关键词共现等进行分析,并分析了国际上该领域的研究热点及研究脉络。研究发现,网络安全态势感知在理论方面需要加强形成体系,并进一步深入研究;应用方面对于多源数据融合的研究较为成熟,但对态势实时感知可视化方面提出了更多的挑战。文中分析结果有助于为该领域的研究人员做进一步深层研究提供参考。

关键词:网络安全;态势感知;CiteSpace;可视分析;知识图谱
中图法分类号 TP393

Map Analysis for Research Status and Development Trend on Network Security Situational Awareness

BAI Xue, Nurbol and WANG Ya-dong
School of Information Science and Engineering, Xinjiang University, Urumqi 830046, China

Abstract Taking 2456 papers on network security situational awareness included in Web of Science from 1999 to 2019 as data sources, and mainly using CiteSpace visualization tools, this paper analyzes the international research hotspots and research context in this field by analyzing cooperation between countries and institutions, literature co-citation, keyword co-occurrence. The research finds that the network security situation awareness needs to strengthen the theoretical formation of a system for further in-depth research. In terms of application, the research on multi-source data fusion is relatively mature, but it poses more research challenges to the visualization of real-time situational awareness. The analysis results are helpful for the researchers in this field to do further research.

Keywords Network security, Situational awareness, CiteSpace, Visual analysis, Knowledge graph

1 引言

在当前大规模网络环境中,网络态势感知对能够引起网络态势变化的安全要素进行获取、理解、显示,并预测未来的发展趋势。

本文为了解国内外对网络安全态势感知研究的基本现状,运用 CiteSpace 工具的文献计量方法并结合网络安全态势感知相关知识,分析整理了近 20 年该领域的研究概况(Web of Science 中 SCI 论文为 1999 年至今),并构建了知识图谱。本文的主要目标是解决以下问题:1)国内外近 20 年在网络安全态势感知领域的研究现状如何? 2)网络安全态势感知未来的研究热点可能有哪些? 3)国内外网络安全态势感知领域的研究脉络发展有什么规律?

本文的具体工作如下:从多方面对网络安全态势感知研究现状进行具体分析,得到该领域的主要研究现状、研究热点及演化脉络,为相关人员做深入研究提供参考。

2 数据来源与研究工具

2.1 数据来源

因有关该领域研究的中文文献较少,并且该领域在国际上研究水平相对较为成熟,所以本文使用的数据来源于 Web of Science 核心合集(SCI-EXPANDED),以主题为检索项,主题词"network security\cyber security\network\cyber" AND "situation awareness\ situational awareness"交叉构成,领域限定为"SCIENCE TECHNOLOGY",文献类型限定为 "ARTICLE OR PROCEEDINGS PAPER",最终得到 2456 篇相关文献。

2.2 研究工具及方法

科学知识图谱的计量分析方法被广泛应用于从海量文献中提炼关键词、寻找领域研究前沿等问题[1],并以图表形式展示相关领域的知识结构与发展规律,有利于研究人员了解所研究领域的整体状况。

基金项目:国家自然基金重点项目(重大联合)(61433012);新疆维吾尔自治区创新环境建设专项项目(PT1811)
This work was supported by the Key Program of the National Natural Science Foundation of China (61433012) and Special Foundation for Innovative Environment Construction of Xinjiang Province (PT1811).
通信作者:努尔布力(nurbol@xju.edu.cn)

常用的知识图谱研究工具为陈超美教授开发的计量分析软件——CiteSpace5.3.R4。CiteSpace 可针对检索结果中的论文对关键词、作者、共被引文献、国家与机构等进行分析，追踪研究领域热点与发展趋势[2]。该软件已经成为计量分析方向影响力较大的软件之一，并且免费提供使用。本文研究方法流程如图 1 所示。

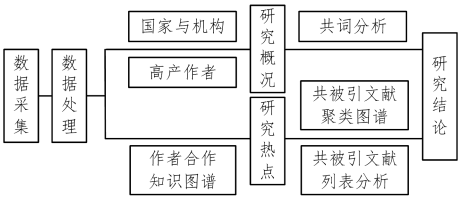

图 1　研究方法流程图

Fig. 1　Flow chart of research method

3　研究概况

3.1　主要国家和机构分析

网络安全态势是近年来各国主要研究热点领域之一，因此可以首先通过对国家和机构进行分析，直观了解各国或相关机构的合作情况，并从发文量解析目前态势感知的研究程度。

在分析国家与机构合作图谱时，我们通过整理数据得到表 1。其中列出了发文量前 10 的国家与该国家发文量在 6 篇以上的机构，中心性为该国家在此领域中的研究程度占比，中心性越高的国家在该领域越权威。以目前统计的发文量，美国以 952 篇遥遥领先，中国以 302 篇占据第二，但英国以 176 篇文献占据了中心性第一(0.29)，证明英国在该领域研究水平更高；排在其后的 7 个国家的发文量与前 3 的国家呈现较大差距。

不同的研究领域都会有较为权威的研究机构，并且这些研究机构在该领域的研究具有前沿性。从表 1 可以看出，仅排名前 3 的国家含有 3 个及以上的机构，部分国家的发文量靠前，但其研究机构发文量却不在机构发文前列，证明该国家机构的分布相对分散。国家与机构的首次发文时间集中在 2006 年之后，证明网络安全态势感知的研究从 2006 年开始普遍受到国际的重视。

表 1　文献数量排名 TOP10 的国家和机构

Table 1　TOP10 countries and institutions for literature quantities ranking

国家	中心性	发文数量	首发年份	机构	发文数量
美国	0.24	952	2000	美国空军实验室	25
				麻省理工学院	23
				乔治梅森大学	22
中国	0.09	302	2005	哈尔滨工程大学	16
				中国科学院	7
				中国科技大学	6
英国	0.29	176	2003	南安普顿大学	23
				牛津大学	6
				布鲁内尔大学	6
德国	0.12	118	2006	—	—
意大利	0.11	116	2007	—	—
加拿大	0.18	95	2006	—	—
韩国	0	79	2006	韩国科学技术研究院	7
法国	0.12	69	2007	—	—
澳大利亚	0.04	68	2007	悉尼科技大学	7
				莫纳什大学	6
西班牙	0.13	65	2006	瓦伦西亚理工大学	6

3.2　作者合作分析

3.2.1　高产作者分析

作者的发文量可间接反映作者在此研究领域的研究水平和权威性。如表 2 所列，在发文数量前 10 的作者中，发表 6 篇文献居多，其中 ERIK BLASCH 发文量第一(26 篇)；高产作者的首次发文时间都在 2007 年以后，处于 2004－2011 年的发展阶段，其完善了网络安全态势感知的研究模型，不断地推动此领域的发展。

表 2　高产作者 TOP10

Table 2　TOP10 high-yield authors

高产作者	文献数量	首发年份	主要关注点
ERIK BLASCH	26	2007	信息融合、可视化
GENSHE CHEN	20	2007	模式聚类、计算视觉
STANTON. NA	20	2009	情景意识、指挥控制
DAN SHEN	13	2007	云计算、机器学习
HUIQIANG WANG	11	2007	网络安全、可信计算
YILU LIU	9	2009	神经网络、可视化
YING LIANG	8	2007	遗传算法
GUY H. WALKER	6	2009	情景意识
SALMON. PM	6	2009	情景意识、道路安全
XIAOWU LIU	6	2007	神经网络、态势感知

3.2.2　作者合作分析

在图 2 的作者合作知识图谱中，用作者名称大小表示发文数量，链接在周围的线条表示合作关系，颜色透明度代表活跃程度。通过图 2 可以分析得出该领域中贡献较大的团队。其中作者合作网络排前 3 的团队分别由 Erik Blasch，Stanton N A 和 Huiqiang Wang 带领。Eeik Blasch 教授团队排名第一，高产作者 Genshe Chen 也是团队成员，主要研究像素级数据融合与大型复杂攻击可视化、大型复杂多步网络攻击，在复杂性可控的状态下，实现攻击检测与预防，利用可视化复杂图识别所有可能的网络攻击路径[3]；Stanton N A 教授主要的研究领域是复杂环境中的态势感知，提出了基于分布式系统的协同系统态势感知模型，通过系统级分布式态势感知模型，针对复杂协作环境进行未来情况预测[4]；王慧强(Huiqiang Wang)团队来自哈尔滨工程大学，也是中国发文最多的一个机构，其主要研究方向是网络安全与分布式系统可信性领域研究。

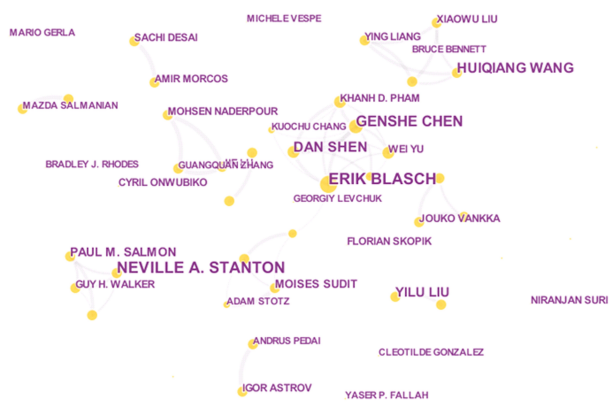

图 2　作者合作知识图谱

Fig. 2　Knowledge map of cooperative authors

3.3　共被引文献分析

文献的被引频次是体现该文献学术价值的重要指标。首先对检索结果中的文献数据进行聚类，再通过最大似然算法(LLR)从文献关键词中提取聚类标签，得到共被引文献聚类

图谱(见图 3)。根据每个知识群的聚类边界分布情况,可以看出国际上对网络安全态势感知的研究主要分为 3 个时期,不同时期呈现不同主题的共被引文献。下面对不同时期的知识群进行阐述。

(1) 1999－2006 年:#4、#5 和 #26 所在时期,该时期的文献施引文数量较少,研究热点主要集中在特征降维和语义网络等。Bass T 自提出网络态势感知概念后,与空中交通监管态势感知进行了比对,在文献[5]中提出了基于多传感器数据融合的入侵检测框架,并将其在下一代入侵检测系统和 NSAS 中使用。该模型提出融合大量异构分布式网络中获取的数据,通过推算方式识别入侵状况,从而评估网络空间的安全态势。该时期为网络态势感知研究的起步阶段,逐渐形成了研究分支,Bass T 提出的模型也为该方向的研究打下了基础。

(2)2007－2014 年:#1、#2、#7 和 #8 所在时期,该时期的研究热点主要集中在大数据、数据降维、多传感器信息融合及网络安全等。在有一定的研究基础后,大量机构开始尝试多种不同的方法,在技术上一般分为数据挖掘、数据融合和态势可视化。Jason Shifflet[6] 构造了一个网络入侵检测模型,运用数据融合实现了网络空间态势感知。Endsley MR 通过认知工程决策和数据融合模型,采用目标导向任务分析来改进模型,对情境感知中的信息融合算法提供了新的改进思路[7]。

(3)2015 至今:#3 所在时期,该时期的研究热点集中在态势感知方面。该阶段一直在不断完善该领域定义,在网络入侵检测领域的基础上不断延伸,目前的研究目标是以可视化方式进行呈现[8]。网络安全态势可视化技术,可以将海量异构数据及其分析内容以合适的方式呈现,便于分析与应用[9],并且可以呈现不同的数据信息给不同用户使用。

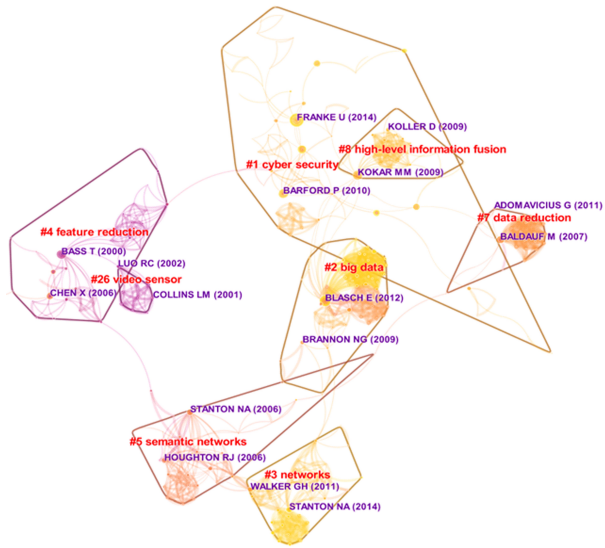

图 3 共被引文献聚类图谱

Fig. 3 Cluster atlas of co-cited references

从表 3 可以看出,共被引频次 Top13 的文献中有 8 篇处于 2007－2014 年,其中有 5 篇属于 #1 知识群,作为该时间段的集中知识群,其主要关注网络安全。这证明在大规模网络环境中,网络的安全问题得到了重视,促进了对网络安全态势预测的研究。

表 3 共被引文献列表 TOP13

Table 3 TOP13 cited references list

文献	共被引频次	被引频次	作者	发表年份	知识群
Cyber situational awareness－A systematic review of the literature	21	46	Franke U	2014	#1
Objective Assessment of Multiresolution Image Fusion Algorithms for Context Enhancement in Night Vision: A Comparative Study	18	198	Blasch E	2012	#2
Intrusion detection systems and multisensor data fusion	15	347	Bass T	2000	#4
Ontology-based situation awareness	15	113	Kokar MM	2009	#8
A Machine Learning Approach to TCP Throughput Prediction	14	46	Barford P	2010	#1
Measuring team situation awareness in decentralized command and control environments	14	122	Gorman JC	2006	—
Quantitative Hierarchical Threat Evaluation Model for Network Security	13	212	Chen X	2006	#4
Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale Sensor Networks	13	48	Jajodia S	2010	#1
A survey on context-aware systems	13	726	Baldauf M	2007	#7
Distributed situation awareness in dynamic systems: theoretical development and application of an ergonomics methodology	10	184	Stanton NA	2006	#5
Wide-Area Situational Awareness for Critical Infrastructure Protection	10	23	Alcaraz C	2013	#1
Context Aware Computing for The Internet of Things: A Survey	10	631	Perera C	2014	#1
Representing distributed cognition in complex systems: how a submarine returns to periscope depth	10	53	Stanton NA	2014	#3

4 研究热点与趋势分析

4.1 基于共词的研究热点分析

在文献主题中可以明确研究问题与方法,快速分析当前的研究热点,而关键词是对一篇文献中研究方法与研究热点的高度精炼。本文对检索结果中所有文献的关键词进行分析,经过筛选去重去后形成关键词频度排名 TOP15,如表 4 所列。本文通过关键词共现分析提取该研究领域的主要热点,并对该领域的发展过程与变化做出判断。

(1)频数(Freq)指标计量分析

频数是指某一关键词出现的次数,通过分析可以得到该领域的研究现状。通过分析发现,频数较高的主题词主要是对态势感知模型或系统进行定义与研究,在网络态势感知研究的发展初期产生了一些频数较高但散落分布的关键词,例如“network”“awareness”“security”“communication”等,造成该现象的主要原因是在对该领域的定义时期,还未完全形成对网络态势感知的概念定义。在 2004 年后涌现了大量与该研究相关的其他主题词,证明新的技术、新的理念不断地加入到该研究中,网络安全态势感知开始得到各国机构的重视。

(2)中心性(Centrality)指标计量分析

关键词的中心性越大,则该关键词越重要。将共词分析结果以中心性大小排序后可以发现,态势感知(situational/

situation awareness）的中心性排第一，“sensor network”“wireless sensor network”“context awareness”的中心性相较其他关键词较高。其中传感器网络是网络态势感知中多传感器融合技术的数据基础，而传感器数据融合可以有效提高上下文感知的效果，提高检测的精确度。而一些主题词中心性较小甚至趋近于零，如“visualization”“big data”“machine learning”等，导致该现象的主要原因是随着网络安全态势感知的发展，涉及的研究领域逐渐增多，主题词间的影响力逐渐变小。

（3）突现（Burst）指标计量分析

突现指标指一个变量的值在短期内发生显著变化，可使用该指标探索文献的深层变化信息，分析该发展领域的前沿变化。热点主题词的出现时间与结束时间，预示着当时的研究热点，并且根据主题词的时间分布可以分析整个领域的发展过程。

表 4　基于共词分析的关键词频度排名 TOP15

Table 4　TOP15 keywords frequency ranking based on common word analysis

排名	关键词	频次	中心性	突现值
1	situation/situational awareness	470	0.59	6.07
2	network	144	0.18	—
3	cyber/network security	106	0.06	4.36
4	context awareness	73	0.11	6.26
5	wireless sensor network	60	0.08	3.34
6	awareness	54	0.08	—
7	sensor network	46	0.17	5.11
8	performance	44	0.06	3.81
9	bayesian network	44	0.03	4.60
10	decision making	37	0.03	3.43
11	neural network	33	0.14	8.60
12	smart grid	33	0.04	—
13	ad hoc network	30	0.04	—
14	information fusion	28	0.04	3.35
15	visualization	28	0.02	—

表 5 列出突现值大于 4 的关键词，产生高突现值的关键词经筛选大多与数据融合相关，其中“fusion”在多个关键词中出现，如“information fusion”“fusion”“data fusion”等。关于数据融合的关键词大多出现在 2006－2012 年，正处于网络数据大爆发的阶段，其促进了对于海量碎片化信息的数据融合技术[10]。“bayesian network”突现值排第 4（4.6），神经网络是当前热门的数据处理技术，贝叶斯网络则是神经网络和贝叶斯推理的结合，算法优化也是不断改进态势感知效果的必要途径[11]。这一系列关键词的高突现值印证了更完善的算法将有利于数据融合更好地应用于网络态势感知。

表 5　热点主题词爆发值 TOP17

Table 5　Outbreak of hot subject TOP17

关键词	突现指标	开始年份	结束年份
neural network	8.5973	2004	2010
sensor	5.5896	2004	2011
situation awareness	6.0708	2005	2006
bayesian network	4.5983	2005	2009
information fusion	3.3485	2005	2007
fusion	4.4129	2005	2011
command and control	3.6670	2006	2007
data fusion	5.6082	2006	2012
sensor network	5.1084	2007	2008
context awareness	6.2626	2007	2010
wireless sensor network	3.3422	2009	2011
network security	4.3588	2009	2011
communication	3.7394	2009	2010
artificial immune system	3.3155	2009	2011
instruction detection	3.1555	2010	2014
optimization	4.1337	2010	2011
visual analysis	4.0119	2011	2012

4.2　研究趋势分析

通过前文对 Web of Science 核心合集库中的 2 456 篇相关文献的分析与研究，可将网络安全态势感知研究的发展分为 3 个阶段（见表 6）：1）摸索阶段（1999－2003 年），在该阶段提出的下一代入侵检测技术获取的数据来源单一，无法达到预期目标；2）发展阶段（2004－2011 年），在该阶段主要针对多源异构数据融合技术进行研究，为了更精准地进行网络态势感知，提出了多种不同的模型进行评价；3）增长阶段（2012 年－至今），数据融合算法一直得到在不断的改进和优化，研究人员还提出了可视化来对网络态势进行更为精准的表达[12]，但目前对于网络安全所评估的态势没有明确的边界定义。

表 6　研究阶段分析表

Table 6　Analysis table of research stage

主题	摸索阶段（1999－2003）	发展阶段（2004－2011）	增长阶段（2012 至今）
研究热点	入侵检测技术、多源传感器数据融合技术等	神经网络、传感器网络、数据挖掘、数据融合技术等	贝叶斯网络、支持向量机、大数据处理技术、可视化技术等
研究领域	军事领域、入侵检测领域等	数据挖掘领域、网络安全领域等	网络安全领域、可视分析领域等
研究脉络	首次提出网络安全态势感知，并未明确定义；主要针对下一代入侵检测系统的模型研究	尝试多种功能模型，研究相关算法和技术，解决网络安全中海量异构数据的融合问题	着重网络安全态势评估，对态势评估进行边界定义；通过完善数据融合技术，使用可视分析进行网络态势实时分析预测，最终提高网络态势感知能力

结束语　本文使用 CiteSpace 可视化工具，基于图谱对国家与机构合作、文献共被引、关键词共现等进行分析，并分析了国际上该领域的研究热点及研究脉络。

（1）网络安全态势感知是在美国军事领域中首先被提出，且美国的文献数量第一；英国文献中心性最高，且南安普顿大学文献数量在机构中占优。虽然中国相较于其他国家对该领域研究起步较晚，但发文数量已居世界第二；国内的哈尔滨工程大学对该领域的研究较为前沿，国内其他机构也提出了多个态势感知模型，对我国网络态势感知的研究具有重大意义。

（2）网络安全态势的发展，从入侵检测技术的改进，到目前大规模网络的实时态势感知，在降低网络负载的前提下，改进了数据融合算法，提高了数据融合的准确性与可用性。近年来，网络安全态势感知对多源数据融合技术的研究日益成熟，有大量对于数据融合算法的改进与优化，其中贝叶斯网络与支持向量机是在该领域中进行数据融合较为热门的

（下转第 348 页）

[8] KIPNIS A, SHAMIR A. Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization[J]. Advances in Cryptology—CRYPTO'99, Lecture Notes in Computer Science, 1999, 1666: 19-30.

[9] BETTALE L, JEAN-CHARLES F, PERRET L. Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic [J]. Designs, Codes and Cryptography, 2013, 69(1): 1-52.

[10] BAENA J, CABARCAS D, ESCUDERO D E, et al. Rank Analysis of Cubic Multivariate Cryptosystems [C] // International Conference on Post-quantum Cryptography. Springer, Cham, 2018: 355-374.

[11] YUAN F, ZHAO S, OU H, et al. A New Public Key Signature Scheme Based on Multivariate Polynomials[M] // Web Information Systems and Mining. Springer Berlin Heidelberg, 2012: 239-245.

[12] CAO W W, NIE X Y. Cryptanalysis of Two Quartic Encryption Scheme and One Improved MFE Scheme [C] // International Conference on Post — quantum Cryptography. Springer Berlin Heidelberg, 2010: 41-60.

[13] DING J, SCHMIDT D. Multivariate public key cryptosystems [M] // Springer Science Business Media. LLC, 2006: 44-63.

ZHANG Qi, born in 1994, master degree candidate. His main research interests include network security, multivariate public key cryptograghy.

NIE Xu-yun, born in 1975, Ph.D, associate professor. His main research interests include multivariate public key cryptography, big data security and privacy protection.

(上接第 343 页)

算法。但实时的网络安全状态评估与态势感知可视化[13]仍具有较高的研究价值。

(3)目前该领域正处在增长阶段,但对于网络安全评估的态势没有明确的边界定义,对于理论体系要进一步深入研究。在应用方面如何将大量异构的网络安全数据以可视化的形式呈现,并使其具有准确的预测功能、自动化的防御机制、智能化的专家系统和便捷的交互操作,都是网络安全态势感知目前热门的研究方向[14]。诸多的应用需求与挑战,都需要该领域的研究人员在今后的工作中一一应对。

参 考 文 献

[1] CHEN Y, CHEN C M, LIU Z Y, et al. The methodology function of CiteSpace mapping knowledge domains [J]. Studies in Science of Science, 2015, 33(2): 242-253.

[2] CHEN C M. CiteSpace II: Detecting and visualizing emerging trends and transient patterns in scientific literature [J]. Journal of the Association for Information Science & Technology, 2014, 57(3): 359-377.

[3] CHEN H, CHEN G, BLASCH E. Analysis and visualization of large complex attack graphs for networks security[C] // Defense & Security Symposium. International Society for Optics and Photonics, 2007.

[4] SALMON P M, STANTON N A, WALKER G H, et al. Is it really better to share? Distributed situation awareness and its implications for collaborative system design [J]. Theoretical Issues in Ergonomics Science, 2010, 11(1/2): 58-83.

[5] BASS T. Intrusion Detection Systems and Multisensor Data Fusion: Creating Cyberspace Situational Awareness[J]. Communications of the ACM, 2000, 43(4): 99-105.

[6] SHIFFLET J. A Technique Independent Fusion Model For Network Intrusion Detection[J]. Proceedings of the Mid states Conference on Undergraduate Research in Computer Science and Mathematics, 2005, 3(1): 13-19.

[7] ENDSLEY M R. Situation awareness misconceptions and misunderstandings[J]. Journal of Cognitive Engineering & Decision Making, 2015, 9(1): 4-32.

[8] SHIRAVI H, SHIRAVI A, GHORBANI A A. A survey of visualization systems for network security [J]. Visualization and Computer Graphics, 2012, 18(8): 1313-1329.

[9] GONG J, ZANG X D, SU Q, et al. Survey of Network Security Situation Awareness [J]. Journal of Software, 2017, 28(4): 1010-1026.

[10] LIN H L, WANG Y Z, JIA Y T, et al. Network big data oriented knowledge fusion methods: A survey [J]. Chinese Journal of Computers, 2017, 40(1): 1-27.

[11] FRANKE U, BRYNIELSSON J. Cyber situational awareness—A systematic review of the literature [J]. Computers & Security, 2014, 46(1): 18-31.

[12] GUANG K, SHUO W, GUANGMING T. Research on Key Technologies of Network Security Situational Awareness for Attack Tracking Prediction[J]. Chinese Journal of Electronics, 2019, 28(1): 162-171.

[13] BEAVER J, STEED C, PATTON R, et al. Visualization techniques for computer network defense[J]. Proc. of the SPIE Int'l Society for Optical Engineering, 2011, 8019(18): 6-9.

[14] WANG H Q, LAI J B, ZHU L, et al. Survey of network situation awareness system[J]. Journal of Computer Science, 2006, 33(10): 5-10.

BAI Xue, born in 1993, postgraduate, is a member of China Computer Federation. Her main research interests include network security and data visualization.

Nurbol, born in 1981, Ph.D, professor, is a member of China Computer Federation. His main research interests include network security and data mining.