计算机工程与应用
Computer Engineering and Applications
ISSN 1002-8331,CN 11-2127/TP

《计算机工程与应用》网络首发论文

题目：网络安全态势感知研究综述
作者：石乐义，刘佳，刘祎豪，朱红强，段鹏飞
网络首发日期：2019-10-24
引用格式：石乐义，刘佳，刘祎豪，朱红强，段鹏飞．网络安全态势感知研究综述．计算机工程与应用.
http://kns.cnki.net/kcms/detail/11.2127.TP.20191024.0952.002.html

网络首发时间：2019-10-24 10:12:09
网络首发地址：http://kns.cnki.net/kcms/detail/11.2127.TP.20191024.0952.002.html

网络安全态势感知研究综述

石乐义，刘　佳，刘祎豪，朱红强，段鹏飞

中国石油大学（华东）计算机与通信工程学院，山东 青岛 266580

摘　要：网络安全态势感知不同于传统的安全措施，它可以对网络中各种活动的行为进行辨识，从宏观的角度进行意图理解和影响评估，进而提供合理的决策支持，在提高网络的监控能力、应急响应能力及预测网络安全的发展趋势等方面都具有重要的意义。本文分别对态势感知和网络安全态势感知的定义进行了归纳梳理，对经典的态势感知模型和新发展的网络安全态势感知模型进行了总结与对比；介绍了网络安全态势感知的关键技术，主要分为基于层次化分析、机器学习、免疫系统和博弈论的技术；介绍了近年来网络安全态势感知在因特网、工控网和物联网中的应用；最后，对其未来发展趋势和待解决的问题进行了总结与展望。

关键词：网络安全；态势感知；数据融合；态势评估；态势预测

文献标志码：A　**中图法分类号：**TP393　doi：10.3778/j.issn.1002-8331.1906-0349

石乐义，刘佳，刘祎豪，等. 网络安全态势感知研究综述. 计算机工程与应用

SHI Leyi, LIU Jia, LIU Yihao, et al. Survey of research on network security situation awareness. Computer Engineering and Applications

Survey of Research on Network Security Situation Awareness

SHI Leyi, LIU Jia, LIU Yihao, ZHU Hongqiang, DUAN Pengfei

College of Computer and Communication of Engineering, China University of Petroleum, Qingdao, Shandong, 266580, China

Abstract: Different from traditional security measures , network security situation awareness can identify the behavior of various activities in the network and conduct intent understanding and impact assessment from a macro perspective so as to provide reasonable decision support .It is of great significance in improving network monitoring capabilities, emergency response capabilities, and predicting the development trend of network security .This paper first separately generalizes the definitions of situation awareness and network security situation awareness, and then sorts out the classical and newly developed system models. Secondly, it introduces the key technologies of network security situation awareness, which is mainly divided into hierarchical analysis, machine learning, immune system and game theory. Then the latest application of network security situation awareness in Internet, industrial control network and Internet of Things are explained. Finally, it summarizes and forecasts the future development trends and problems that need to be solved.

Key words： network security; situation awareness; data fusion; situation assessment; situation prediction

基金项目：山东省自然科学基金项目(No.ZR2019MF034)；国家自然科学基金项目(No.61772551)。

作者简介：石乐义(1975-),通讯作者,男,教授,CCF 会员(14178S),研究领域为计算机网络、信息安全等,E-mail: shileyi@upc.edu.cn; 刘佳(1995-),女,硕士研究生在读,研究领域为:网络安全、人工智能; 刘祎豪(1996-),男,硕士研究生在读,研究领域为:网络安全、深度学习; 朱红强(1993-),男,硕士研究生在读,研究领域为:网络安全、人工智能; 段鹏飞(1996-), 男,硕士研究生在读,研究领域为:网络安全。

1 引言

互联网基础设施的不断发展和新应用的不断涌现使得网络规模日益扩大，拓扑结构日益复杂，安全问题也日益突出，影响程度也越来越大，虽然采取了各种安全防护措施，但是它们只是从各自的角度发现网络中存在的问题，并没有考虑其中的关联性，无法系统、整体的发现网络中存在的问题。

网络安全态势感知（Network Security Situation Awareness，NSSA）[1]是近几年发展起来的一个热门研究领域。它能够融合所有可获取的信息并对网络的安全态势进行评估，为安全分析员提供决策依据，将不安全因素带来的风险和损失降到最低，在提高网络的监控能力、应急响应能力和预测网络安全的发展趋势等方面都具有重要的意义。

本文旨在对网络安全态势感知的含义、系统模型、主要技术和应用领域进行总结梳理，为安全领域相关研究人员提供参考。本文贡献如下：

(1) 对态势感知和网络安全态势感知的相关定义进行了梳理，列举了较为经典的态势感知模型和近几年新发展的网络安全态势感知模型；

(2) 从技术的角度出发，介绍了网络安全态势感知的主要方法，主要分为层次化分析、机器学习、免疫系统、博弈论等；

(3) 归纳总结了网络安全态势感知在因特网、工控网和物联网中的应用；

(4) 从应用范围、与其他技术的结合两个角度对网络安全态势感知的发展趋势进行了展望，从功能模块优化、人机交互与自动响应和“反态势感知”三个方面对今后需要解决的问题进行了分析。

2 网络安全态势感知的相关概念

2.1 态势感知的概念

虽然近几年对态势感知(Situation Awareness，SA)[2]的研究越来越多，但目前仍然处于探索阶段，在态势感知的定义方面，既有按照心理、环境和系统的定义方式，也有从个体、团体和系统的角度出发的定义方式[3,4]，尚未形成统一的认知。

1988 年，Endsley 提出态势感知的概念，即“在一定的时空范围内，认知、理解环境因素，并且对未来的发展趋势进行预测”[2]，并提出由态势要素提取、态势理解和态势预测组成的三层模型。该概念源于航天飞行的人因研究，主要针对于个人态势感知，但由于团体中有着成员间的任务依赖以及协作沟通等特点，人们开始在团队环境中研究态势感知。

1993 年，Wellens 提出团体态势感知的概念，将其定义为“群体成员关于当前环境事件的共同观点”[5]。但目前对团体态势感知尚无统一的定义，被广泛使用的是由 Endsley 等人[6]、Salas 等人[7]和 Shu 等人[8]分别提出的团体态势感知模型。

以分布式认知理论作为基础，Artman 等人从系统层面对态势感知进行了讨论，并将其称作系统层面态势感知。分布式态势感知作为系统态势感知的方法之一，是从系统的角度研究团体态势感知，Stanton、Salmon 等人将分布式态势感知定义为“系统中与环境状态及其变化相关的特定任务的激活知识，态势感知是系统的涌现特性，来自系统中各智能体的交互”[9]。

除了上述主流的定义，其他研究人员对态势感知提出了自己的理解：

Gugerty L[10]认为态势感知是一种知识并对其给出了定义，“一种不可预测、多方面情况的不断更新的、有意义的知识，操作人员在参与实时多任务时可以用该知识来指导选择和行动。”不同于 Endsley 的观点，作者认为态势感知是一个更广泛的概念，应该包含焦点过程和更自动化的环境过程。

Dong Z 等[11]认为态势是一个系统中事物状态的合成，它拥有完整性和全局的态势；感知是一种认知映射，它基于数据融合和集成、风险评估、可视化以及其他相关技术得到准确的信息。态势感知则是对时空中环境因素的一种综合理解并预测未来一段时间后的状态以实现合理的决策的过程。

2.2 网络安全态势感知的概念

Bass 于 1999 年首次提出网络态势感知(cyberspace situational awareness，CSA)的概念[1]，并指出，“基于融合的网络态势感知”是网络管理的发展方向，并且根据应用领域的不同，将网络态势分为安全态势、拓扑态势和传输态势等。

Franke U 等人认为[12]“态势感知是一种可以在不同程度上达到的状态”。以该理念为基础，作者将网络态势感知作为态势感知的一个子集，即网络态势感知是与网络环境有关的态势感知的一部分。

从 Bass 开始相关研究均是围绕着网络的安全态势展开，逐渐对网络安全态势感知的概念进行研究，例如龚俭等人提出网络安全态势感知是对网络系统安全状态的认知过程[13]，但是目前对网络安全态势感知尚未形成统一、全面的定义，大多是对 Endsley 的态势感知定义的详细解释，并没有针对网络安全这一领域做出特定的阐释。

本文认为，网络安全态势感知是指通过收集网络环境中综合、全面的安全要素并进行数据融合后，对网络的安全态势有宏观、全面的认知，并且能对网络系统的安全趋势进行预测的过程，是保障网络安全的有效手段。

虽然目前大部分研究都将网络安全态势感知分为态势提取、态势评估和态势预测三个功能模块，但仍然存在着不同研究人员对网络安全态势感知几个阶段的划分不统一、对于不同阶段之间的关系理解不同的问题。因此，对网络安全态势感知给出科学、全面的定义，对不同阶段进行合理的划分仍是需要讨论和解决的问题。

3 网络安全态势感知的模型

3.1 经典的态势感知模型

态势感知模型作为系统的核心，能够帮助人们组建一个良好的态势感知系统，从而顺利地进行态势的提取、评估、预测等工作。其中，经典的态势感知模型包括 Endsley 的三层模型、数据融合模型和 OODA 控制循环模型。

态势感知的提出源于美国军方的军事对抗且主要应用于航空领域，Endsley 提出的三层模型如图 1 所示，分为态势要素提取、态势理解和态势预测三个阶段[14]。该模型为态势感知的研究奠定了重要基础，且成为目前广泛使用的架构。

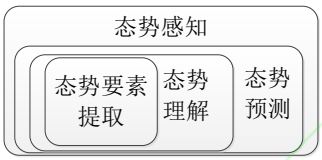

图 1 Endsley 的态势感知模型

数据融合作为态势感知的核心，其中最具影响力的是 JDL(Joint Directors of Laboratories)数据融合模型。JDL 模型将融合分为 4 个层次[15]：目标细化、态势细化、风险细化、过程细化，其中：态势感知作为中间层次，向下从低层次融合接收网络元素的监测数据，为态势感知提供信息来源；向上为高层次融合提供态势信息，用于威胁分析和决策支持。

OODA 循环（Observe-Orient-Decision-Act loop）模型描述了目的与活动的感知过程，并将态势感知循环过程分为观察、导向、决策、行动 4 个阶段，如图 2 所示。其中，观察实现了从物理域到信息域的跨越；判断和决策属于认知域；而行动实现了信息域到物理域的闭合，完成循环。OODA 控制循环模型完整地展示了态势感知的动态执行过程，虽然它在层次性和分工明确性上略弱于 Endsley 三层模型，但是该模型的循环结构和动态协作能很好地适应庞杂的网络空间的态势感知。

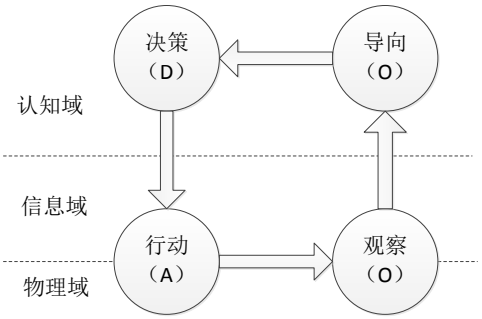

图 2 OODA 控制循环模型

3.2 网络安全态势感知模型的发展

基于上述经典的模型和理念，近几年对传统的态势感知模型也有一定的融合和发展，形成了多种不同场景下的网络安全态势感知模型。

龚正虎等[16]提出的网络态势感知研究框架以 JDL 数据融合模型为基础，概括了网络态势感知的研究内容，相比传统模型，该模型突出了动态循环、不断细化的本质，强调反馈的重要性。

An J 等[17]通过将 JDL 数据融合模型和 Endsley 的态势感知模型相结合并进行扩展，提出了网络态势感知模型，该模型由四层组成，从下往上依次为识别层、理解层、预测层和措施层。相比传统模型的三层架构，该模型新增了措施层，通过提供可选择的措施及其影响来协助决策者进行决策，考虑的更加全面。

Kokkonen T[18]提出的网络安全态势感知系统由输入接口层、信息归一化层、数据融合层和可视化层组成，该模型强调了可视化的作用，其中还包括人机交互接口和信息共享接口，更有助于实际环境中的操作。

根据 Endsley 的三层概念模型，Azhagiri M 等[19]提出一个多视角多层次的分析框架，在三层模型的基础上，作者增加了安全强化机制对分析员进行帮助和指导，以提高系统的安全态势。

陆耿虹等[20]创新性提出了工控网络态势感知模型，将态势感知应用到工控系统当中。该模型从下至上共包含三个部分：态势要素获取层、态势评估层以及后续态势感知过程，为工控系统的安全保障提供了新的方法。

不同于上述的层次化结构，Jajodia S 等[21]提出的网络态势感知框架集成了一系列技术和自动化工具，利用自动化工具代替网络分析员，并通过分析员向系统提问的方式不断了解系统的安全状况、攻击的影响与演化等情况。

当前大多数模型以传统模型的三层架构为基础，在动态循环、可视化、自动化等角度进行了补充，并根据不同应用场景的需求，实现对模型的丰富和细化。

4 网络安全态势感知的关键技术

本节对网络安全态势感知的关键技术进行了总结和分类，主要分为基于层次化分析、机器学习、免疫系统和博弈论的态势感知方法，如表 1 所示。

表 1 网络安全态势感知的关键技术研究

关键技术	技术特点	主要工作
层次化分析	分层处理、自下而上；先局部后整体	层次化安全威胁态势量化评估模型及其改进
机器学习	较好的自适应、自组织、无限逼近和预测的能力；描述非线性复杂系统的性能	SVM、RBF 神经网络和小波神经网络以及使用回归、粒子群算法、遗传算法等对其的改进
免疫系统	具有自我容忍、自适应和稳健等优点以及模式识别、学习和记忆能力	传统的基于免疫、抗体浓度的方法；协同人工免疫以及与云模型理论的结合
博弈论	考虑网络安全中攻防双方的对抗性，推测对方可能的策略并在此基础上制定自己的对策	马尔可夫博弈；攻防随机博弈模型

4.1 基于层次化分析的态势感知技术

层次分析法（analytic hierarchy process，AHP）是一种定量和定性相结合的多目标、多准则的决策分析方法，基于层次化分析法的态势感知将较为复杂的态势感知过程分层处理，将网络系统分为服务、主机、系统三个层面，简化每一层的处理过程，采取自下而上，先局部后整体的方针，通过计算底层安全要素的局部影响来评估系统整体的安全态势。

国内具有较大参考价值的是陈秀真等人的层次化网络系统安全威胁态势量化评估模型[22]，该模型从上到下分为网络系统、主机、服务和攻击/漏洞 4 个层次，如图 3 所示，采取“自下而上、先局部后整体”的评估策略，并且，该模型是基于 IDS 海量报警信息和网络性能指标，将服务、主机本身的重要性及网络系统的组织结构相结合而产生的。

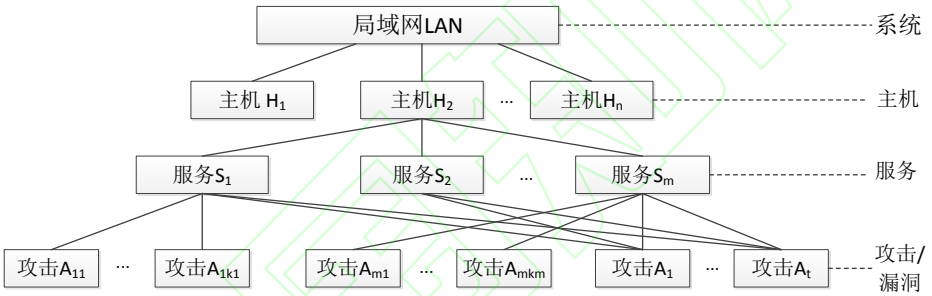

图 3 层次化网络系统安全威胁态势量化评估模型

但陈秀真等提出的模型中也存在一些不足：在其评估方法中只有 IDS 报警信息一种安全信息来源，而在实际网络系统部署中，诸如防火墙、系统日志等都是不可或缺的安全因素，如果不将这些信息纳入计算范围，就失去了网络安全态势评估技术在综合安全信息、整体反应网络安全态势上的优势。下面是对该层次化模型改进的相关工作：

赖积保[23]提出改进的层次分析法，构建了多层次多角度的网络安全态势量化评估模型，将实际网络系统按规模和层次关系自顶向下逐级分解为“网络层—主机层—攻防层”三个层次，以 IDS、Firewall、VDS 等提供的多源安全信息为原始数据，信息来源更加全面。张勇[24]从专题层次、要素层次和整体层次三个层次，每个层次分别从不同的角度，每个角度分别从不同的粒度对网络安全态势进行评估，构建了多层次多角度的态势评估框架。孟锦[25]提出了基于时变证据理论的层次化多源网络安全威胁态势评估模型，模型分为三层，由局部做起，逐步提升分析等级以至全局。实验结果表明，通过对陈秀真提出的层次化模型的改进，信息来源更加全面、可靠，提高了态势感知在现实场景中应用的真实性和可行性。

4.2 基于机器学习的态势感知技术

安全态势值具有不确定性和非线性的特点，而机器学习在描述非线性的复杂系统方面有着很好的性能，并且有着很好的自适应、自组织和无限逼近能力，因此使用机器学习来进行态势评估和态势预测的方法受到了人们的广泛关注。下面主要分为支持向量机（SVM）、RBF 神经网络和小波神经网络三种方法进行讨论。

由于 SVM 具有良好的泛化能力且不容易过拟合，很多研究人员使用 SVM 以及支持向量回归（SVR）的方法进行态势评估和预测。虽然与神经网络相比 SVM 具有收敛速度快、抗过拟合能力强等优点，但单独使用 SVM 做预测模型也存在训练过程中参数选取盲目的问题，因此为提高预测精度，Chen G 等[26]将回归预测的思想引入 SVM，提出了 RF-SVM 算法，该算法可以根据历史攻击数据预测

未来网络数据流中的潜在的攻击，不仅提高了预测准确率，而且降低了误差。许建华[27]将支持向量回归算法（SVR）优良的非线性拟合能力和果蝇优化算法（FOA）良好的全局寻优能力相结合，利用果蝇优化算法对支持向量回归的参数进行优化，避免了参数选择的盲目性，提高了网络安全态势预测的准确性。

RBF 神经网络具有函数逼近和自适应能力强、学习速度快等优点，可以描述非线性的复杂系统，因此适用于网络安全态势预测，例如，将 RBF 神经网络和时间序列预测法结合可以很好的实现网络安全态势预测[28]。但是神经网络在实际应用时会产生收敛速度慢、网络层次设计困难和容易陷入局部最优解的情况，因此很多学者结合其他方法来对 RBF 神经网络的参数和结构进行优化。江洋等人[29]提出采用改进的粒子群算法（PSO）优化 RBF 神经网络；谢丽霞等人[30]利用改进的遗传算法来对 RBF 神经网络的参数进行优化；李喜喜[31]则将 C-均值聚类（FCM）和混合递阶遗传算法相结合，来对传统 RBF 神经网络的学习过程进行改进。

对相同学习任务，小波神经网络（Wavelet Neural Network，WNN）结构更简单，收敛速度更快、学习能力更强、精度更高，在达到全局最优解的同时还能够保持局部细节最优解。由于这些显著优点，人们开始将小波神经网络应用到态势感知领域，并且可以使用遗传算法、种群优化算法等对小波神经网络进行优化。Cong H 等[32]提出基于优化的动态小波神经网络的网络安全态势感知，该方法可以将异构的安全数据和威胁的演化趋势的动态感知相结合，在一定程度上有着自我调节和控制的能力，不仅达到了态势感知的目标，并且提供了网络监督和管理的新方法。

4.3 基于免疫系统的态势感知技术

免疫是指生物体对感染具有的抵抗能力，计算机安全系统与生物免疫系统中遇到的问题非常相似，由于生物免疫系统有着特征提取、分布式检测、自我容忍、自适应、稳健等优势和模式识别、学习、记忆等能力，很适合用作态势感知的研究。

Sun F 等[33]提出基于抗体浓度的态势感知，对其原则和框架进行了描述，建立了用于态势感知的淋巴细胞生命过程的数学模型。该系统可以学习到所遭受的攻击以及入侵的地点、严重性和最严重的区域。

由于人工免疫系统有着可扩展性差和覆盖范围受限的缺点，Qiao Y 等[34]提出了协同人工免疫系统的概念和相关的态势感知模型。在该模型中，不同计算机中的记忆检测器可以共享不同点以提高人工免疫系统的覆盖率和可扩展性。

Ruirui Z 等[35]将人工免疫和云模型理论相结合，利用危险理论和云模型的入侵检测技术对网络攻击进行实时监控；通过抗体浓度的变化评估网络安全状况，利用基于云模型的时间序列预测机制进行预测。

4.4 基于博弈论的态势感知技术

传统的态势感知方法大都仅着眼于攻击或防守一方，忽略了攻防双方策略相互依存的情况，而在实际攻防过程中必须充分考虑对方可能的策略并在此基础上制定自身的对策。只要网络安全中的攻防双方存在，两者间的博弈过程也就始终存在，不考虑网络安全中攻防双方的对抗性，往往会导致结果不够准确，大大降低了态势感知模型对实际情况的描述能力[36]。

博弈论是研究具有斗争或竞争性质的数学理论和方法，博弈双方的概念、特征与网络安全中的攻防双方具有相似性，研究人员一直在探索博弈论方法的适用性，以解决网络中的安全问题，将博弈论的思想运用于网络安全态势感知逐渐成为一个热门的研究方向。

张勇等[37]提出一种基于马尔可夫博弈分析的网络安全态势感知方法，通过对威胁、管理员和普通用户的行为进行博弈分析，建立三方参与的马尔可夫博弈模型，并对相关算法进行优化分析，使评估过程能够实时运行。

Zhou B 等[38]提出基于阻止威胁传播的网络安全态势感知方法，通过在攻击者、防御者和中间人三者间构建博弈模型来帮助系统管理者进行实时分析，从而对最脆弱的节点进行加强。

针对现有的一些评估方法缺少对威胁信息、防护信息、环境信息的综合分析导致评估结果不准确的问题，翁芳雨[39]提出一种基于攻防随机博弈模型的网络安全态势评估模型。该模型通过建立威胁传播网络，对威胁动作和防护策略的博弈过程建立随机博弈模型并求解混合策略纳什均衡，基于纳什均衡的结果对攻防双方动作进行判断并对网络安全态势量化分析。

4.5 其他态势感知方法

可视化技术通过将大量的、抽象的数据以图形的方式表现，实现图形信息并行搜索，提高了可视化系统信息处理的速度和效率。Matuszak W J 等[40]针对智能电网系统安全，为智能电网系统中的网络信任提供算法和可视化技术，并开发了一种原型网络态势感知可视化工具，用于可视化网络信任并且提供与 SCADA 管理信息一起显示的操作决策辅助。Kotenko I 等[41]提出一种可视化分析技术，用于显示评估整体网络安全状态和保护机制效率的安全指标。网络安全态势感知的可视化技术在军事[42]和实

时风险跟踪[43]方面也有着一定的应用。通过利用多种数据源和多种方法，将可视化结果以各种图表类型、3D 视图的方式向用户展示，效果更加全面且直观，帮助用户对当前态势有更宏观的理解。

由 Dempster 和 Shafer 建立的 D-S 证据理论是进行数据融合和态势评估的重要方法，该方法不仅克服了用概率描述不确定性的不足，而且形式灵活多变，可以将 D-S 理论和模糊逻辑、神经网络、专家系统等其他方法相结合，进一步提高推理的准确性。例如可以使用跨层自适应变异粒子群优化算法（AMCPSO）对传统 D-S 理论进行改进。

刘玉岭等[44]提出基于时空维度分析的网络安全态势预测方法，不仅在时间维度上预测未来时段内的安全态势要素集，而且在空间维度上分析各安全态势要素集的相互关系以及对网络安全态势的影响。席荣荣等[45]提出基于环境属性的网络威胁态势量化评估方法。这两种方法分别考虑到空间维度和环境属性的影响，分析更加全面、结果更加准确。

云计算和大数据等技术也为态势感知提供了新的方法和思路。Saurez E 等[46]提出一种由雾节点和云代表的地理分布式计算连续体的编程基础设施 Foglets，解决了地理分布态势感知应用中存在的问题。在 Paik I[47]的研究中，提出一种从大数据中获取信息的自动化序列，获取信息可以通过重复的数据分析过程完成。可见，大数据也能为态势感知提供一定的便利。

5 网络安全态势感知的应用场景

态势感知这一概念源于航天飞行的人因研究，此后在军事战场[48]、空中交通监管[49]、医疗[50]等应急调度领域[51,52]得到了广泛应用。网络安全态势感知作为态势感知一个重要的分支，具备强大的全局网络监控与觉察能力，能够为操作人员提供全面且合理的决策支持。

针对态势感知在网络安全领域的应用，本文主要从因特网、工控网和物联网两个角度进行探讨。

5.1 因特网

由于因特网的普遍性与易操作性，态势感知在其中有着广泛的应用，利用态势感知强大的全局监控能力，实时掌握网络的运行状态并采取对应的安全措施，保证网络系统的安全。

在因特网中，态势信息主要通过防火墙日志、入侵检测日志、病毒日志、网络扫描等方法提取，通过层次化分析、机器学习、D-S 证据理论、博弈论、免疫系统等方法进行态势感知[53,54]，从资产、脆弱性、威胁等角度进行态势值的计算[55]，刘世文等[56]基于网络安全态势感知的主动防御技术的相关研究，来提高攻击的难度和成本，提高防御的针对性。

Jirsik T 等[57]提出网络范围的网络态势感知的理念，作为网络势感知的特定领域，它着眼于对计算机网络进行态势感知，考虑的因素是交换机路由器等网络物理设备，目标是提供对计算机网络动态深入的了解与决策。

Alcaraz C 等[58]提出对重要基础设施保护的广域态势感知，使用广域态势感知的方法监控重要基础设施的性能，进行动态的防护和响应服务，并且提出了基于上下文感知和混合视角的广域态势感知框架。

针对社交网络环境下舆情态势感知存在的问题，萧海东等[59]提出智能态势感知方法，该方法能够有效降低历史虚警数据的干扰，实现态势感知数据的自动汇聚，使态势感知更适用于小世界网络环境并且具有加速态势可视化的特点。

5.2 工业网和物联网

近年来，工业控制系统与互联网的深度融合使其暴露在很多威胁和攻击之下，这对国家安全、经济发展和社会稳定等方面产生了严重影响，因此可以利用态势感知对工控系统的整体运行情况进行有效地监测和控制，从而保证工控系统的安全运行。

美国信息能源部构建了网络入侵自动响应和策略管理系统，以实现工控系统重要基础设施的实时态势感知[60]。Lu G 等[61]提出完整性攻击下的工控系统网络安全态势感知，使用基于粒子滤波的安全态势感知框架为系统提供准确的态势评估，并且引入了投票机制来识别恶意节点。Fox S[62]提出将工业工程方法和态势感知建模相结合来实现可靠的自主生产系统，以应对工作环境以及不确定性等方面的挑战。能源互联网是新能源技术与互联网技术相结合，实现电力流、信息流和业务流高度融合的共享网络。针对能源互联网复杂的网络结构，田建伟等[63]提出基于威胁传播的多节点网络安全态势量化评估方法，该方法能够准确评估多节点网络的安全态势，有效计算边界连接关系。

由于电力系统重要的战略地位，有很多研究是专门针对电力系统的，其中，Wu J 等人[64]提出一种基于智能电网大数据分析的安全态势感知机制，将模糊聚类、博弈论和强化学习相结合，实现智能电网的安全态势分析。Chen L 等[65]提出基于分布式监控和多源信息融合的主动配电网态势感知系统，它由多源信息融合、源负载预测、快速仿真分析、风险认证、提醒和可视化模块组成。Bolzoni D 等[66]提出电力系统态势感知的网络架构和测试指标，对 DEnSeK (Distributed Energy Security Knowledge)项目架构的作用和度量方法进行了详细解释。由此可见，将网络安全态势感知应用于智能电网将作为未

来重要的发展方向。

物联网带来了全球信息产业的第三次发展浪潮，但物联网的安全问题也日渐凸显。为了提高监控、应急响应和预测能力，Xu G 等人[67]提出一种基于语义本体和用户自定义规则的物联网安全态势感知模型。Kolbe N 等[68]提出一种基于上下文的态势理论，能利用知识库和推理组件丰富物联网态势感知的框架。

物联网和可穿戴设备也为医疗护理提供了新的思路，Anzanpour A 等[69]通过部署无线体域网，利用可穿戴设备传感器收集患者体征信息和重要信号，利用数据置信度评估、患者健康状况知识库以及健康状况的自动化推理，对患者的健康状况进行整体态势感知和有效的监控。

车联网是物联网和车辆自组织网络的结合，Golestan K[70]提出一种注意力协助框架来实现车联网的态势感知，该框架利用低层数据融合和高层信息融合实现交通实体、态势、影响评估以及决策，从而实现更加安全完善的车联网系统。

6 总结与展望

本文对网络安全态势感知相关工作进行了归纳总结，介绍了态势感知和网络安全态势感知的起源、现有定义以及系统模型。从层次化分析、机器学习、博弈论等方面对网络安全态势感知的关键技术进行了详细的说明，归纳梳理了近几年的研究工作，并对网络安全态势感知的应用领域进行了分类汇总。

下文对网络安全态势感知的发展趋势和应用前景进行了展望，对其仍需解决和今后可能面对的一些问题进行了总结：

(1) 应用范围不断拓展。

传统的网络态势感知通常聚焦于传统网络应用，目前已在向工业控制系统、物联网、广域网等领域应用不断拓展。随着网络计算的泛在化，网络态势感知应用也将会深入拓展到移动计算、边缘计算、社会计算、机会网络、星际网络等方方面面。

(2) 与新技术结合更加紧密。

人工智能、机器学习等由于自身的优势和特点已经成为态势感知的重要方法，大数据、云计算、物联网等也为态势感知提供了新的思路并成为态势感知的应用场景，将区块链、蜜罐等技术应用到态势感知中将成为一种不可避免的趋势。态势感知与其他技术的结合定会为该领域带来新鲜活力，为解决态势感知中的问题提供新的方法与灵感。

(3) 功能模块优化问题。

数据融合方法的研究：由于态势感知的应用范围越来越广，随之产生的数据越来越庞杂，如何对海量异构数据进行高效、准确地处理是重要问题。

态势评估方法的研究：如何在不同的应用场景中全面地考虑到影响态势感知的因素也是一个重要问题；并且由于缺乏明确统一的度量标准，因此选取合适的度量指标也尤为重要。

态势预测方法的研究：提高预测的准确度，提高网络的前向预测能力，做到防患于未然。

态势感知的可视化：通过将网络状况实时或近实时的显示，为分析人员的决策提供有效的帮助。

(4) 人机交互与自动响应问题。

目前网络和系统仍离不开人为参与，如何建立良好的人机交互机制，帮助系统接受专家的建议并进行修改和调整，既是未来的发展趋势又是急需解决的问题。

虽然人在系统中扮演重要角色，但系统应是独立的整体，在面对入侵和攻击时，系统不仅能够报警，还应采取一定的防护措施，实现自动响应，提高系统的智能化。

(5) “反态势感知”问题。

“反态势感知”是指利用态势感知系统的弱点或缺陷来进行攻击和破坏或者直接采用其他技术对态势感知的不同阶段进行破坏和干扰的概念。例如，针对利用神经网络进行态势评估和态势预测的方法，攻击者可能通过添加恶意数据来干扰神经网络的训练过程，从而影响态势评估和预测结果的准确度，严重时，可能评估和预测出截然相反的结果，让攻击者有机可乘。

总的来说，态势感知的研究仍然处于初级阶段，仍有很多问题需要完善和解决，但随着相关技术和研究的不断完善，态势感知定会得到更大的发展，发挥其本身的优势和特点为网络安全提供强有力的保障。

参考文献

[1] Bass T, Gruber D. A glimpse into the future of id[J]. login:: the magazine of USENIX & SAGE, 1999, 24(4): 40-45.

[2] Endsley M R. Design and evaluation for situation awareness enhancement[C]//Proceedings of the Human Factors Society annual meeting. Sage CA: Los Angeles, CA: SAGE Publications, 1988, 32(2): 97-101.

[3] 高杨，李东生，程泽新. 无人机分布式集群态势感知模型研究[J]. 电子与信息学报, 2018, 40(6): 1271-1278.
[4] Stanton N A, Salmon P M, Walker G H, et al. State-of-science: situation awareness in individuals, teams and systems[J]. Ergonomics, 2017, 60(4): 449-466.
[5] Wellens A R. Group situation awareness and distributed decision making: From military to civilian applications[J]. Individual and group decision making: Current issues, 1993: 267-291.
[6] Endsley M R, Robertson M M. Situation awareness in aircraft maintenance teams[J]. International Journal of Industrial Ergonomics, 2000, 26(2): 301-325.
[7] Salas E, Prince C, Baker D P, et al. Situation awareness in team performance: Implications for measurement and training[M]//Situational Awareness. Routledge, 2017: 63-76.
[8] Shu Y, Furuta K. An inference method of team situation awareness based on mutual awareness[J]. Cognition, Technology & Work, 2005, 7(4): 272-287.
[9] Salmon P M, Stanton N A, Jenkins D P. Distributed situation awareness: Theory, measurement and application to teamwork[M]. CRC Press, 2017.
[10] Gugerty L. Situation awareness in driving[J]. Handbook for driving simulation in engineering, medicine and psychology, 2011, 1.
[11] Dong Z, Xu T, Li Y, et al. Review and application of situation awareness key technologies for smart grid[C]// Energy Internet and Energy System Integration (EI2), 2017 IEEE Conference on. IEEE, 2017: 1-6.
[12] Franke U, Brynielsson J. Cyber situational awareness-a systematic review of the literature[J]. Computers & Security, 2014, 46:18-31.
[13] 龚俭，臧小东，苏琪，等. 网络安全态势感知综述[J]. 软件学报, 2017, 28(4):1010-1026.
[14] Endsley M R. Situation awareness global assessment technique (SAGAT)[C]//Aerospace and Electronics Conference,1988. NAECON 1988.Proceedings of the IEEE 1988 National. IEEE,1988:789-795.
[15] Hall D L,Llinas J.An introduction to multisensor data fusion[J]. Proceedings of the IEEE,1997,85(1):6-23.
[16] 龚正虎，卓莹. 网络态势感知研究[J]. 软件学报，2010, 21(7)：1605-1619.
[17] An J, Li X H, You C L, et al. The Research of Cyber Situation Awareness Model[C]//International Conference on Intelligent and Interactive Systems and Applications. Springer, Cham, 2016: 232-238.
[18] Kokkonen T. Architecture for the Cyber Security Situational Awareness System[M]//Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Springer, Cham, 2016: 294-302.
[19] Azhagiri M, Rajesh A, Karthik S. A Multi-Perspective and Multi-Level Analysis Framework in Network Security Situational Awareness[J]. International Journal of Computer Networks and Communications Security, 2017, 5(4): 71.
[20] 陆耿虹，冯冬芹. 基于粒子滤波的工业控制网络态势感知建模[J]. 自动化学报, 2018, 44(8): 1405-1412.）
[21] Jajodia S, Albanese M. An Integrated Framework for Cyber Situation Awareness[M]//Theory and Models for Cyber Situation Awareness. Springer, Cham, 2017: 29-46.
[22] 陈秀真，郑庆华，管晓宏,等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报, 2006, 17(4):885-897.
[23] 赖积保. 基于异构传感器的网络安全态势感知若干关键技术研究[D][博士论文]. 哈尔滨工程大学, 2009.
[24] 张勇. 网络安全态势感知模型研究与系统实现[D][博士论文]. 中国科学技术大学, 2010.
[25] 孟锦. 网络安全态势评估与预测关键技术研究[D][博士论文]. 南京理工大学, 2012.
[26] Chen Gang. RF-SVM Based Awareness Algorithm in Intelligent Network Security Situation Awareness System[A]. Institute of Management Science and Industrial Engineering. Proceedings of 2017 3rd Workshop on Advanced Research and Technology in Industry Applications(WARTIA 2017)[C].Institute of Management Science and Industrial Engineering:,2017:5.
[27] 许建华. 基于机器学习的网络安全态势预测方法的研究与实现[D][硕士论文].北京邮电大学,2016.
[28] Jiang Y, Li C, Yu L, et al. On network security situation prediction based on RBF neural network[C]//Control Conference (CCC), 2017 36th Chinese. IEEE, 2017: 4060-4063.
[29] 江洋，李成海，魏晓辉，等. 改进 PSO 优化 RBF 的网络安全态势预测研究[J]. 测控技术, 2018(5).
[30] 谢丽霞,王亚超,于巾博.基于神经网络的网络安全态势感知[J]. 清华大学学报(自然科学版)，2013，53(12): 1750-1760.
[31] 李喜喜. 基于粒子群神经网络的网络安全态势评价研究[D][硕士论文].河北师范大学,2018.
[32] Cong H, Chao W. Network Security Situation Awareness Based on the Optimized Dynamic Wavelet Neural Network[J]. IJ Network Security, 2018, 20(3): 593-600.
[33] Sun F, Xu F. Antibody concentration based method for network security situation awareness[C]//Bioinformatics and Biomedical Engineering, 2009. ICBBE 2009. 3rd International Conference on. IEEE, 2009: 1-4.
[34] Qiao Y, Xu J. A network security situation awareness model based on cooperative artificial immune system[C]// Computer Science and Service System (CSSS), 2011 International Conference on. IEEE, 2011: 1945-1947.
[35] Ruirui Z, Tao L, Xin X, et al. A Network Security Situation Awareness Model Based on Artificial Immunity System and Cloud Model[C]//International Conference on Information and Management Engineering. Springer, Berlin, Heidelberg, 2011: 212-218.
[36] 刘景玮，刘京菊，陆余良，等. 博弈论在网络安全态势感知中的应用[J]. 计算机应用, 2017(a02):48-51.
[37] 张勇，谭小彬，崔孝林，等. 基于 Markov 博弈模型的网

络安全态势感知方法[J]. 软件学报, 2011, 22(3): 495-508.

[38] Zhou B, Zhong L. Network security situation awareness based on intercepting the threat spread[C]//Computer Science and Network Technology (ICCSNT), 2013 3rd International Conference on. IEEE, 2013: 876-879.

[39] 翁芳雨. 基于随机博弈模型的网络安全态势评估与预测方法的研究与设计[D][硕士论文]. 北京邮电大学, 2018.

[40] Matuszak W J, DiPippo L, Sun Y L. CyberSAVe: situational awareness visualization for cyber security of smart grid systems[C]//Proceedings of the Tenth Workshop on Visualization for Cyber Security. ACM, 2013: 25-32.

[41] Kotenko I, Novikova E. Visualization of security metrics for cyber situation awareness[C]//2014 Ninth International Conference on Availability, Reliability and Security (ARES). IEEE, 2014: 506-513.

[42] Llopis S, Hingant J, Pérez I, et al. A comparative analysis of visualisation techniques to achieve cyber situational awareness in the military[C]//2018 International Conference on Military Communications and Information Systems (ICMCIS). IEEE, 2018: 1-7.

[43] López-Cuevas A, Medina-Pérez M A, Monroy R, et al. Fitoviz: A visualisation approach for real-time risk situation awareness[J]. IEEE Transactions on Affective Computing, 2018, 9(3): 372-382.

[44] 刘玉岭, 冯登国, 连一峰, 等. 基于时空维度分析的网络安全态势预测方法[J]. 计算机研究与发展, 2014, 51(8): 1681-1694.

[45] 席荣荣,云晓春,张永铮.基于环境属性的网络威胁态势量化评估方法[J].软件学报,2015,26(7):1638-1649.

[46] Saurez E, Hong K, Lillethun D, et al. Incremental deployment and migration of geo-distributed situation awareness applications in the fog[C]//Proceedings of the 10th ACM International Conference on Distributed and Event-based Systems. ACM, 2016: 258-269.

[47] Paik I. Situation awareness based on big data analysis[C]//Machine Learning and Cybernetics (ICMLC), 2016 International Conference on. IEEE, 2016, 2: 911-916.

[48] Lenders V, Tanner A, Blarer A. Gaining an edge in cyberspace with advanced situational awareness[J]. IEEE Security & Privacy, 2015, 13(2): 65-74.

[49] Friedrich M, Biermann M, Gontar P, et al. The influence of task load on situation awareness and control strategy in the ATC tower environment[J]. Cognition, Technology & Work, 2018, 20(2): 205-217.

[50] Green B, Parry D, Oeppen R S, et al. Situational awareness-what it means for clinicians, its recognition and importance in patient safety[J]. Oral diseases, 2017, 23(6): 721-725.

[51] Botega L C, de Souza J O, Jorge F R, et al. Methodology for data and information quality assessment in the context of emergency situational awareness[J]. Universal Access in the Information Society, 2017, 16(4): 889-902.

[52] Zambrano M, Esteve M, Pérez I, et al. Situation awareness in the large forest fires response. A solution based on wireless mesh networks[C]//Communications (LATINCOM), 2017 IEEE 9th Latin-American Conference on. IEEE, 2017: 1-6.

[53] 张玉臣, 张任川, 刘璟, 等. 应用深度自编码网络的网络安全态势评估[J/OL].计算机工程与应用:1-10. [2019-09-28].http://kns.cnki.net/kcms/detail/11.2127.TP.20190604.0944.004.html.

[54] 陈维鹏, 敖志刚, 郭杰, 等. 基于改进的 BP 神经网络的网络空间态势感知系统安全评估[J]. 计算机科学, 2018, 45(S2): 335-337+341.

[55] 宋进, 唐光亮. 网络安全态势感知技术研究与应用[J]. 通信技术, 2018, 51(6):1419-1424.

[56] 刘世文, 马多耀, 雷程, 等. 基于网络安全态势感知的主动防御技术研究[J]. 计算机工程与科学, 2018, 40(6): 1054-1061.

[57] Jirsik T, Celeda P. Toward real-time network-wide cyber situational awareness[C]//NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2018: 1-7.

[58] Alcaraz C, Lopez J. Wide-area situational awareness for critical infrastructure protection[J]. Computer, 2013, 46(4): 30-37.

[59] 萧海东, 陈宁. 移动社交信息智能态势感知分析[J]. 中国科学:信息科学, 2015,45(6):783-795.

[60] Saunders N, Khanna B, Collins T. Real-time situational awareness for critical infrastructure protection[C]//Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on. IEEE, 2015: 151-156.

[61] Lu G, Feng D. Network Security Situation Awareness for Industrial Control System Under Integrity Attacks[C]//2018 21st International Conference on Information Fusion (FUSION). IEEE, 2018: 1808-1815.

[62] Fox S. Reliable autonomous production systems: Combining industrial engineering methods and situation awareness modelling in critical realist design of autonomous production systems[J]. Systems, 2018, 6(3): 26.

[63] 田建伟, 田峥, 漆文辉, 等. 基于威胁传播的多节点网络安全态势量化评估方法[J]. 计算机研究与发展, 2017,54(4): 731-741.

[64] Wu J, Ota K, Dong M, et al. Big data analysis-based security situational awareness for smart grid[J]. IEEE Transactions on Big Data, 2018, 4(3): 408-417.

[65] Chen L, Jia M, Yuan X, et al. Construction and application research of Active Distribution Network Situation Awareness System[C]//Power and Energy Engineering Conference (APPEEC), 2016 IEEE PES Asia-Pacific. IEEE, 2016: 863-869.

[66] Bolzoni D, Leszczyna R, Wróbel M R. Situational Awareness Network for the electric power system: The

architecture and testing metrics[C]//Computer Science and Information Systems (FedCSIS), 2016 Federated Conference on. IEEE, 2016: 743-749.

[67] Xu G, Cao Y, Ren Y, et al. Network security situation awareness based on semantic ontology and user-defined rules for Internet of Things[J]. IEEE Access, 2017, 5: 21046-21056.

[68] Kolbe N, Zaslavsky A, Kubler S, et al. Enriching a Situation Awareness Framework for IoT with Knowledge Base and Reasoning Components[C]//International and Inter-disciplinary Conference on Modeling and Using Context. Springer, Cham, 2017: 41-54.

[69] Anzanpour A, Azimi I, Götzinger M, et al. Self-awareness in remote health monitoring systems using wearable electronics[C]//Proceedings of the Conference on Design, Automation & Test in Europe. European Design and Automation Association, 2017: 1056-1061.

[70] Golestan K. Information Fusion Methodology for Enhancing Situation Awareness in Connected Cars Environment[J]. 2016. http://hdl.handle.net/10012/10168.