大数据背景下网络安全态势感知的技术要点分析

文◆河南省肿瘤医院　**李素伟**

引言

随着互联网技术的深入普及，网络安全问题得到人们的高度关注。现阶段，网络安全技术的协同与管理仍存在很大弊端，无法实现安全数据的有效整合，降低了网络安全维护的效能。网络安全态势感知的出现解决了这一问题，弥补了传统单一网络安全技术存在的不足。网络安全态势感知能够对网络安全软硬件设备采集的信息进行整合，通过数据挖掘深入分析网络运行环境的安全态势，即对威胁网络安全状态的各个要素进行分析计算，根据已有的数据信息进行自我推理和完善，并以此为基础预测潜在的网络安全风险，制定针对性防护措施，保证网络运行安全。基于此，本文在分析传统网络安全防护不足的基础上，探讨网络安全态势感知关键技术，以期能够提高网络安全性，降低网络运行风险。

1 传统网络安全防护的不足

现阶段，网络安全防护体系主要由安全运维模型、线性防御模型以及立体防御模型构成，这种防护体系只能被动防护，对于黑客及病毒攻击只能做到后知后防，无法主动防护。此外，传统网络安全防护体系无法通过软件提高防护能力，只能进行硬件更新，但硬件更新不仅成本较高，还无法进行无限扩充。硬件更新过程中，由于攻击特征库的容量有限，在加入新攻击特征时，应删除不必要的攻击特征，应对层出不穷的网络攻击手段。弊端在于删除不必要攻击特征后，无法对被删除攻击特征进行准确识别，进而产生风险漏洞。

2 网络安全态势感知概念及其任务

2.1 网络安全态势感知概念

态势感知的应用最早起源于航空领域，随着科学技术的进一步发展，该技术逐渐在网络安全防护领域得到普及。态势感知是指在某特定情况下，综合多方面条件获取并预估环境等因素。网络安全态势感知则是指在特定网络环境下，通过收集、分析包括网络状态、恶意攻击等在内的各种数据信息，以此为基础预测潜在的安全风险。主要内容分为两个方面。

第一，安全预警。通过网络监测设备收集网络事件、网络流量等网络数据，并对这些数据进行全方位动态分析，对潜在的安全威胁进行判断，并进行安全预警。

第二，风险预测。整理、分析网络近段时间所有的运行数据，通过数据挖掘生成网络安全趋势图，以此预测网络系统出现的安全风险，并制定针对性防护措施。

2.2 网络安全态势感知的职责

网络系统运行过程中，安全态势感知的职责具体体现为 4 个方面。（1）态势观察。观察当前网络环境，通过搜集到的网络信息，判断安全威胁的攻击来源与攻击方式。（2）影响感知。预估网络安全影响，主要进行脆弱性分析，即影响评价、损害评价等。（3）数据采集。采集、分析网络原始安全数据，识别和预测潜在的网络安全威胁，并在此基础上提出网络安全优化措施，强化情报共享能力，提高网络安全防御能力。（4）态势预测。预估网络黑客采用的攻击手段等。

3 大数据背景下网络安全态势感知关键技术

3.1 数据融合技术

网络安全态势感知过程中，

【作者简介】李素伟（1979—），女，河南濮阳人，本科，网络工程师，研究方向：医院信息化建设与管理。

为确保系统运作有效性，应确保数据真实且完整。由于网络数据内容复杂，规模庞大，应对数据进行整合处理，通过数据采集、数据清洗、数据分析、数据关联等措施，保证数据具有可用性。除此之外，对网络数据进行分组以及结构化处理，有助于提高数据分析的有效性、可行性，以此提高数据可视化的精准性[1]。

数据整合主要包括数据采集、数据清洗、数据关联、数据存储4个方面的内容，数据整合流程如图1所示。

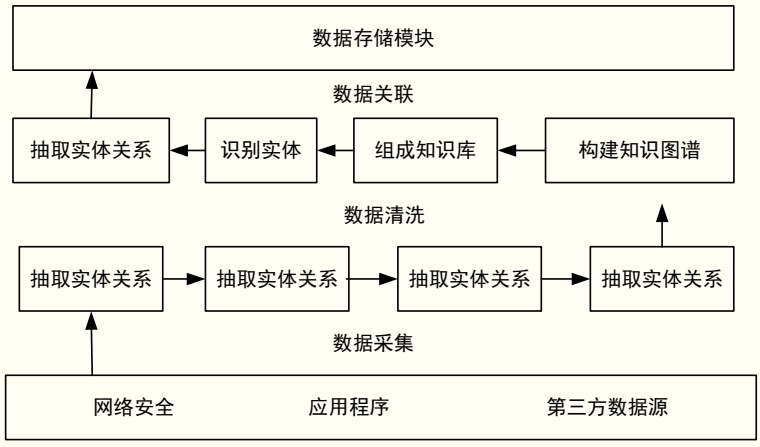

图1 数据整合流程

作为数据处理的关键环节，数据清洗在网络安全态势感知中发挥着至关重要的作用。通过数据清洗，在去除数据噪声的同时，能够筛选掉重复及冗余的数据，提高数据的精准度[2]。在数据清洗过程中，根据实际需求对数据进行校准、调补，有利于提高数据的完整性和精准性。网络安全数据清洗流程如图2所示。

3.2 危险评估技术

基于网络安全态势感知的网络危险评估，分析采集的网络日志、网络事件以及网络流量等信息，对潜在的安全威胁进行检测评估。需要注意的是，网络危险评估应从多渠道进行数据源地收集，保证数据源的全面性、完整性，避免因数据源过于单一影响网络安全评估结果。

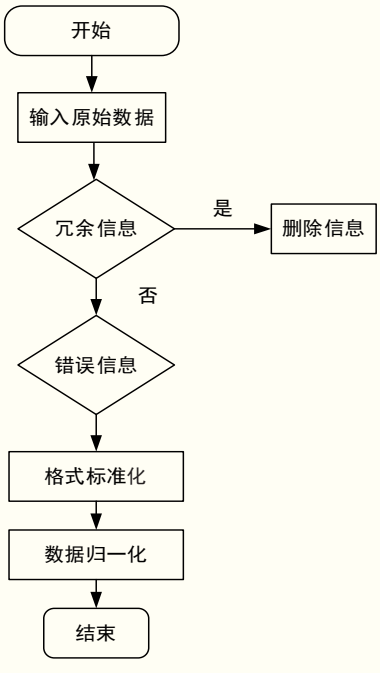

图2 网络安全数据清洗流程

基于上述评估需求，本次研究依托Sim Hash算法，在现有网络危险评估模型的基础上进行优化改进，具体内容如下[3]。

（1）增加网络拓扑结构。连接各硬件设备，提高数据的互通性与安全防护的协同性。

（2）增加节点服务信息。通过节点服务确定节点权重。

（3）增加日志信息。通过多渠道数据搜集，在危险评估模型中加入网络历史运行记录、网络安全数据等信息，并通过六元组对所有日志数据进行表述。1）id_l主要作用于日志数据的身份表述；2）id_{st}主要作用于日志数据产生节点表述；3）id_{dt}主要作用于日志数据目标节点表述；4）$time_l$主要作用于日志数据生成时间表述；5）type主要作用于日志数据类型表述；6）$info_l$主要作用于日志数据内容表述。

（4）增加漏洞信息。通过态势感知分析网络安全漏洞，以此确定安全风险发生率，并通过四元组对所有漏洞数据进行表述。

（5）增加攻击信息。通过态势感知确定攻击源，并通过六元组对所有攻击信息进行表述。1）ida主要作用在于攻击数据身份表述；2）dt主要作用在于攻击目的节点表述；3）idv主要作用在于攻击成功率表述：4）timea主要作用在于攻击数据产生时间表述；5）infoa主要作用在于攻击信息内容表述；6）st主要作用在于攻击起始节点表述。

（6）增加节点安全态势。对网络节点的安全状态进行量化。

（7）增加模块安全态势。对网络模块的安全状态进行量化。

（8）增加网络安全态势。对整个网络系统的安全状态进行量化。

在上述内容的基础上，本次研究基于Sim Hash进行网络安全评估模型的构建，网络安全评估模型如图3所示。

3.3 态势预测技术

传统网络安全态势检测过程中，主要依托检测设备对网络运行数据进行动态监测，以此评估网络安全状态。虽然操作便捷、成本较低，但缺点在于数据检测精准度不足，无法保证网络运行安全。大数据时代背

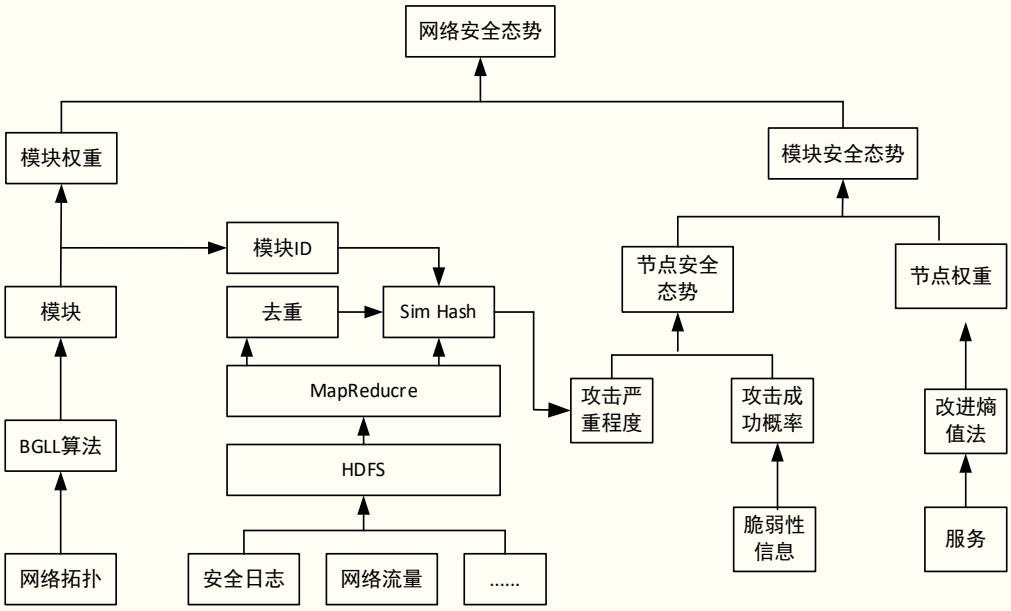

图 3 网络安全评估模型

景下，网络安全态势感知为计算能力以及存储能力提出了新的挑战和要求。在此基础上，本次研究从两方面着手，对网络安全态势进行预测。首先，提前确定提取特征，并统一网络数据格式，进一步提高网络安全数据采集的全面性、完整性，再借助 Bloom Filter 筛选、删除网络安全数据库中的重复内容。其次，借助 AML 模型，根据现有网络安全数据，对接下来一段时间内出现的网络安全风险进行预测，构建预测攻击图，以此实现对网络攻击概率及攻击路径的有效预测。在此基础上，根据网络攻击预测结果，进一步评估网络安全态势。

3.4 可视化技术

基于大数据的网络安全态势感知技术中的可视化技术，实现数据信息模型可视化。可视化技术能够实现数据模型的深入解读，以此提高数据的精准性、直观性，为后续网络安全态势感知奠定基础。数据信息可视化主要分为 3 个环节，具体如下。

（1）数据整合。网络安全态势感知过程中，为确保系统运作有效性，应确保数据真实且完整。由于网络数据内容复杂，规模庞大，应对数据进行整合处理，通过数据采集、数据清洗、数据分析、数据关联等措施，保证数据具有可用性。除此之外，通过对网络数据分组以及结构化处理，提高数据分析的有效性、可行性，提高数据可视化的精准性。

（2）数据分析。通过数据分析，实现对庞大安全数据量的有效分析、挖掘及处理，以此获取准确、全面的安全状态信息，预测安全事件的发展走向，进而为网络安全保护提供参考。

（3）数据呈现。将完成分析处理的数据通过可视化方式进行展示，使用户更加清晰、直观地了解数据内容，并以此进行决策。通常情况下，数据呈现应立足于实际业务需求，并针对网络安全态势感知痛点问题进行改进，构建功能健全、交互畅通、运行稳定的安全态势感知可视化系统。

结语

大数据时代背景下，传统的网络安全预测已经无法满足当前发展的需要，本文深入分析了传统网络安全防护存在的不足之处，并结合网络安全态势感知的具体职责，探讨了数据整合、数据可视化、危险评估以及态势预测等网络安全态势感知关键技术，提高网络安全性，降低网络运行风险。

引用

[1] 李泽慧,徐沛东,邬阳,等.基于大数据的网络安全态势感知平台应用研究[J].计算机应用与软件,2023,40(7):337-341.

[2] 谢凯,代康.基于决策树的联级网络安全态势感知系统设计[J].现代电子技术,2022,45(17):74-78.

[3] 谷洪彬,郑黎明,魏孔鹏.基于机器学习的网络安全态势感知关键技术研究与应用[J].电脑与信息技术,2022,30(1):40-42,49.