基于智能 Agent 的电力信息网络安全态势感知模型研究

蒋诚智 余 勇 林为民
(中国电力科学研究院国家电网公司信息网络安全实验室 南京 211106)

摘 要 网络安全态势感知(NSSA)是实现网络安全监控的一种有效的技术手段,对提高网络运行安全管控水平和主动防御能力有着重要的作用。在现有的 NSSA 模型研究的基础上,结合电力信息网络的现状与需求,提出了一种基于智能 Agent 的 NSSA 感知模型。模型从数据采集处理层、评估分析层、协调管理层和态势决策层几个层次介绍了涉及的 Agent 模型和功能模块,对电力信息网络安全监控和管理具有一定的指导意义。

关键词 信息安全,NSSA,智能 Agent
中图法分类号 TP393.08 **文献标识码** A

Research on Electric Information Network Security Situation Awareness Model Based on Intelligent Agent

JIANG Cheng-zhi YU Yong LIN Wei-min
(State Grid Information Network Security Laboratory, China Electric Power Research Institute, Nanjing 211106, China)

Abstract Network security situation awareness (NSSA) is one of the effective ways to implement network security monitoring. It can be utilized to improve the operational security management and to enhance the proactive defense ability of the network. On the basis of the research work on NSSA models, a NSSA model based on intelligent agent was proposed with the consideration of current situation and demand of electric information network. With the aim of directing the security monitoring and management of electric information network, the proposed model describes the agent modeling and functional modules of four layers that are data collection and processing layer, evaluation and analysis layer, coordination and management layer and situation decision layer.

Keywords Information security, NSSA, Intelligent agent

1 引言

随着电网企业信息化建设的全面推进和持续深化及其高度融入企业各项生产经营业务,信息化贯彻电网各环节建设,实现数据共享全面集成,推进企业精益化管理,提升企业管理水平。同时,信息化的深化应用及实用化推进、网络的广泛应用及规模的不断扩大,使得网络的信息安全问题越来越受到重视。为落实国家信息安全等级保护的要求,国家电网公司开展了信息系统的定级、备案、等级保护建设、整改及测评工作,并制定了相应的等级保护标准和信息安全防护方案,从边界、网络、主机、应用等几个方面进行了安全防护设计。依据"分区、分域、分级"的原则,电力信息系统划分为生产控制大区和管理信息大区,将管理信息大区划分为信息内网和信息外网。网络边界防御主要采用电力专用隔离装置、防火墙、入侵检测系统等来实现边界数据流的安全隔离交换和安全监控。网络防御主要采用网络分段、虚拟专网、网络扫描等来加强网络访问控制和安全监控。

然而,如何全面了解和掌握整体网络的安全状态、如何及时对网络安全事件采取有效的响应、控制和整改措施,对信息运维和安全监控提出了新的要求。信息外网方面,针对互联网攻击手段的多样化、对外服务网站漏洞的攻击和恶意篡改、链接、个人桌面终端防护不足而导致的信息泄漏、窃取事件等要求对互联网边界、终端、病毒木马情况等进行安全监控。信息内网方面,需对主要业务系统的实际应用情况进行监控,并进一步加强安全事件监控和威胁分析。随着智能电网建设的全面开展,网络边界向用户侧延伸,大量移动终端和业务采集终端的接入以及无线网络的应用均对网络安全监控和管理提出了新的需求。

Tim Bass 提出了将多传感器数据融合技术应用于入侵检测系统,从而实现网络态势感知(Cyberspace situational awareness)的概念[1]。网络安全态势感知(NSSA)是实现网络安全监控的有效技术手段,通过对网络安全设备与检测设备等的告警及其他安全信息的融合、关联,可以反映出网络整体安全状况,并对网络安全的趋势进行预测和预警。NSSA 的关键技术主要在于多传感器的数据融合技术、网络态势评估方法及态势值计算、态势预测方法[2]。西安邮电学院提出了一种基于 D-S 理论的网络安全态势评估算法,其利用 D-S 证据理论对多数据源信息进行融合,通过漏洞、服务和主机的

到稿日期:2012-02-15 返修日期:2012-07-26
蒋诚智(1982-),男,博士,工程师,主要研究方向为信息安全、安全测评,E-mail:jiangchengzhi_epri@163.com;余 勇(1970-),男,博士,研究员级高级工程师,主要研究方向为安全测评、安全管理。

态势值计算网络安全态势值[3]。中国科学技术大学提出了一种基于 Markov 三方博弈模型的态势评估方法，即通过评估系统的完整性态势和可用性态势，加权得出网络的整体安全态势[4]。北京系统工程研究所提出了一种基于关联融合的网络安全态势评估模型，即通过关联各个传感器的信息及安全事件，来评估当前的网络安全态势[5]。网络安全态势感知中的态势预测模型主要包括基于灰色理论的预测模型、基于灰色支持向量机的预测模型、灰色马尔可夫模型和基于神经网络的预测方法[6]。四川大学提出了一种基于卡尔曼算法的网络安全态势预测方法，即研究结果表明，其算法比 RBF 神经网络算法更具实用价值[7]。四川大学还提出了一种基于免疫的网络安全态势感知方法，采用灰色马尔可夫模型对网络安全态势进行预测[8]。

Endsley 在 1995 年提出的层次模型是态势感知的经典模型，它包括 3 个层次：态势要素感知(Perception)、态势理解(Comprehension)、态势预测(Projection of future status)[9]。国防科技大学提出的面向大规模网络的安全态势感知系统主要由数据集成、关联分析、指标体系及态势展示、态势预测 4 个部分组成[10]。河南大学提出的基于多源异构传感器的网络安全态势感知系统借鉴网络安全管理系统结构的优点，其框架结构包括信息获取层、要素提取层和态势决策层[11]。

因此，在借鉴已有 NSSA 的研究成果上，结合电力信息网络安全的需求，提出了一种基于智能 Agent 的网络安全态势感知模型，为电力信息网络的安全监控和管理提供一定的指导作用。

2 基于智能 Agent 的网络安全态势感知模型

电力信息网络规模的广泛、安全设备的多样性、网络环境的复杂性等使得网络安全态势感知系统面临的复杂性和不确定性增加。Agent 技术作为人工智能研究的分支，具有自主性(autonomy)、社交能力(sociability)、反应能力(reactivity)、主动性(Pre-activeness)、移动性(mobility)、真实性(veracity)、友好性(benevolence)和合理性(rationality)[12]。自主 Agent 与多代理系统代表了分析、设计和实施复杂软件系统的一种新方法[13]。东北石油大学分析了移动 Agent 在 NSSA 中的优势，包括减轻网络负载、响应能力增强、移动性、异构性、稳定性和容错性，并提出了一种基于移动 Agent 的网络安全态势感知模型[14]。

2.1 总体框架结构

如图 1 所示，本文提出的网络安全态势感知模型自下而上分为 4 个层次。

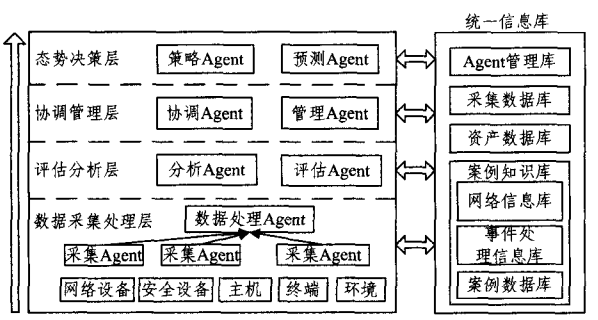

图 1 基于智能 Agent 的网络安全态势感知模型

(1)数据采集处理层主要功能：针对信息内、外网的安全防护重点不同，根据安全管理策略，对性能、告警、安全事件、配置等数据进行采集，规范数据采集接口，统一数据格式，对采集数据进行处理后为上一层评估与分析提供了数据基础。

(2)评估分析层主要功能：在采集数据的基础上，根据关联规则对安全事件、资产、脆弱性和威胁进行关联分析；根据网络安全指标，计算与评估信息内、外网网络安全态势参考值。

(3)协调管理层主要功能：在网络安全态势评估的基础上，对发现的或潜在的安全问题进行派单处理或核查，并对处理过程与结果提供记录功能。

(4)态势决策层主要功能：制定网络安全指标体系和整体网络安全策略；根据学习机制，对网络安全态势进行趋势预测，并形成安全问题处理建议。

2.2 数据采集处理层

数据采集处理层主要包含两类 Agent：数据采集 Agent 和数据处理 Agent。数据采集 Agent 部署在数据源中，而在电力信息网络中，为尽量减少采集对被监管设备的压力，应尽量采取“一次采集，多次使用”的策略，以避免对告警、性能、资产、安全事件等数据的重复采集。信息外网方面，由于面临的主要威胁来自于互联网的攻击与渗透、对外网站漏洞被攻击、网站被篡改或种植病毒与木马、外网桌面终端信息被窃取，因此，采集 Agent 在信息外网主要的采集内容为：信息外网与互联网的边界安全设备日志、互联网出口镜像流量信息、桌面终端管理软件监控信息等。信息内网方面，信息内、外网边界采用了电力专用逻辑强隔离装置，减少了来自外部网络的攻击威胁。然而，信息内网部署了主要的电力业务系统，对安全事件与威胁更为敏感，需进一步提高运维能力和安全监控水平。因此，采集 Agent 在信息内网主要的采集内容为：网络设备告警信息、网络设备、主机(包括服务器、数据库和中间件)、应用的性能数据、桌面终端管理软件数据、资产数据等。此外，数据来源还可以来自风险评估的结果(包括资产标识、类别、价值、脆弱性、威胁、影响等)。

如图 2 所示，Agent 管理库负责创建、增加、删除和配置数据采集 Agent 和数据处理 Agent。数据采集 Agent 根据统一配置的数据格式对探针数据进行统一格式转换。数据处理 Agent 则根据配置的处理规则将规范格式化的数据进行合并、归类、过滤等数据处理后存入网络信息库。类似于文献[10]的基于 Agent 的数据集成方法，此方法具有扩展性、实时性好的优势。

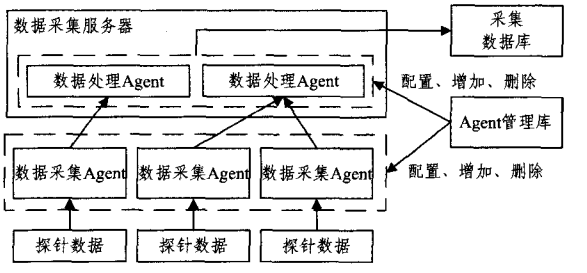

图 2 基于 Agent 的数据采集与处理

2.3 评估分析层

评估分析层主要包括两类 Agent：分析 Agent 与评估 A-

gent。分析 Agent 主要负责在采集数据的基础上进行安全事件分析与关联，如图 3 所示。由于国家电网公司建立了等级保护纵深防御体系，采取了“边界-网络-主机-应用和数据”的信息系统纵深防护措施，因此，分析 Agent 在关联安全事件时，主要从此 4 个方面的告警和性能数据进行分析。同时，为定位安全问题及降低相应的安全风险，应将资产自身的脆弱性、面临的威胁、可能造成的影响(损失)等与安全事件进行关联。所有的安全事件及其关联关系被存入网络信息数据库。

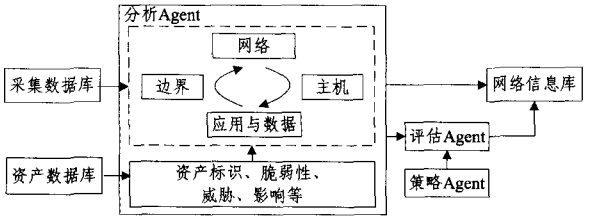

图 3　安全事件关联与分析

如图 4 所示，评估 Agent 根据安全事件分析结果，分别计算边界、网络、主机和应用的风险值及已采取的安全防护强度。风险值根据 4 个方面关联的采集数据(包括告警、性能和配置数据等)计算得出。安全防护强度根据已采取的安全防护措施，通过与等级保护安全技术措施的对比，并结合电力信息网络的结构特点计算得出。通过风险值与安全防护强度的比较，可以分别得到边界、网络、主机和应用的安全态势。通过安全策略 Agent 对此 4 个方面分别赋予权重值，经过加权后可以得到网络综合安全态势值。综合态势值应不仅包含加权后的整体值，还应包含 4 方面的态势值，以全面反应当前网络的安全态势与弱点所在。

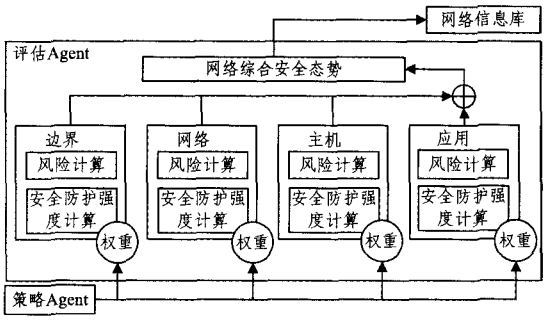

图 4　网络综合安全态势评估

2.4　协调管理层

协调管理层主要包含两类 Agent：协调 Agent 和管理 Agent。协调 Agent 主要负责协调各层 Agent 进行安全态势学习，具体的学习机制将在第 3 节详细描述。

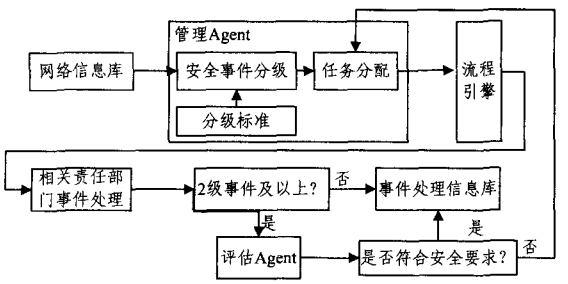

图 5　管理 Agent 任务流程

如图 5 所示，管理 Agent 根据当前的网络安全事件及态势评估，首先对发现的安全问题进行安全事件分级。参照 GB/Z 20986—2007《信息安全技术 信息安全事件分级分类指南》，将信息安全事件按严重性从低到高分为 0 级至 4 级，分级标准如表 1 所列。

表 1　信息安全事件分级标准

安全事件级别	特别重要信息系统影响	重要信息系统影响	一般信息系统影响	社会影响
0 级	可忽略	较小	较小	较小
1 级	较小	较大	严重	一般
2 级	较大	严重	特别严重	较大
3 级	严重	特别严重		严重
4 级	特别严重			特别严重

管理 Agent 将安全事件分级后，将相应的整改和核查任务提交给流程引擎，以分配给相应的单位或部门进行安全事件处理。如安全事件为 0 级或 1 级，则将事件处理的解决方案及处理结果存入事件处理信息库；如安全事件为 2 级(含)以上，则事件处理后需经评估 Agent 对采取的安全措施进行评估，在符合相关安全要求或安全风险接受标准后，再将相关处理信息存入事件处理信息库，否则，将其返回管理 Agent，对任务进行重新分配。

2.5　态势决策层

态势决策层主要包含两类 Agent：策略 Agent 和预测 Agent。策略 Agent 的主要任务包括制定相应的安全指标及态势计算权重。如图 6 所示，此安全指标体系示例自上而下分为 4 级，各级指数可以通过图形化态势展示给管理者。

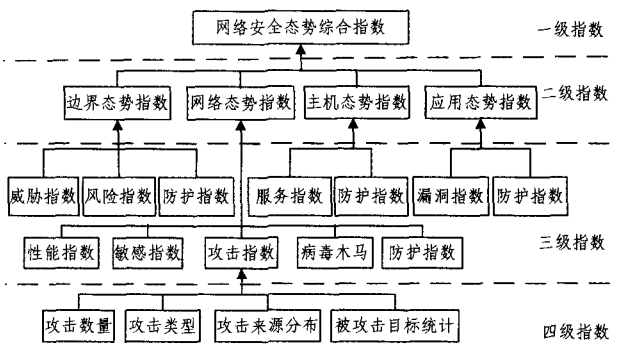

图 6　层次式网络安全指标体系示例

预测 Agent 的主要任务为通过与各层 Agent 协调来为学习机制提供当前安全处理措施建议及安全态势预测，具体的学习机制在第 3 节详细描述。

3　智能 Agent 学习机制

3.1　学习原理

本文提出的学习机制基于两种学习方法的理论基础：基于案例的推理(CBR，Case-Based Reasoning)与强化学习(RL，Reinforcement Learning)。CBR 方法从历史案例中学习与推理出问题的解决方法，一般包含以下 4 步[15]：

(1)从历史数据库中检索相似的案例；

(2)从检测的案例中产生解决新问题的方法；

(3)产生的解决方案可能需要经过评估与修正；

(4)将经过确认或修正的解决方案存入数据库，并不断更新历史数据库。

RL 是结合动态编程(dynamic programming)与监督学习(supervised learning)来实现机器学习的方法。其中 Agent 根据预先定义的目标从状态转换过程中得到回报(reward),以此进行学习,此回报可能为奖励或惩罚。一般强化学习方法中包含 3 个主要要素:状态集合、行动序列和行动所得回报的集合[16]。

3.2 学习机制

面对网络安全态势的动态性及网络环境的复杂性,本文提出的智能 Agent 学习机制如图 7 所示,案例知识库由网络信息库、事件处理信息库和案例数据库组成。具体步骤如下所示:

第 1 步　协调 Agent 发起一个学习周期 Δt_i。周期开始时,分析 Agent 与评估 Agent 将 Δt_i 内的安全事件关联信息及安全态势存入网络信息数据库;

第 2 步　协调 Agent 调用预测 Agent 开始案例学习。

(1)预测 Agent 从网络信息库的历史状态(事件处理前的安全状态)集合中检索出与 Δt_i 时安全状态相似度最高(或相似度排名前几位)的安全状态。

(2)根据检索出的安全状态,预测 Agent 在案例数据库中寻找与之相关联的事件处理信息标识及事件处理后的安全状态标识。

(3)预测 Agent 根据标识分别在网络信息库和事件处理信息库中检索出相应的信息,评估解决方案的合理性和适用性,必要时进行修订。

(4)预测 Agent 给出解决方案的建议及事件处理后可能的安全状态。

第 3 步　管理 Agent 根据相应的建议进行流程提交和任务分派,并将此次事件处理过程存入事件处理信息库;

第 4 步　在下一个学习周期 Δt_{i+1} 开始前,协调 Agent 调用分析 Agent 与评估 Agent 将 Δt_{i+1} 时的事件处理前的安全状态作为 Δt_i 时的事件处理后的安全状态。协调 Agent 将 Δt_i 时的完整案例存入案例数据库。

协调 Agent 还需定期对案例知识库中重复的或相似度高的案例进行合并,以提高案例检索的效率。

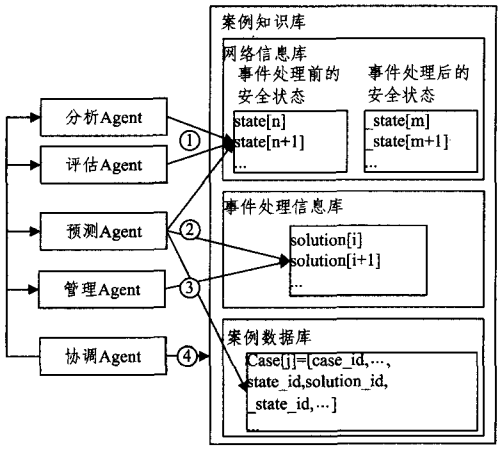

图 7　智能 Agent 学习机制

结束语　为满足电力信息系统及网络的安全监控和管理需求,全面掌握整体网络安全态势,本文提出了一种层次式的基于智能 Agent 的网络安全态势感知模型,从 4 个层次具体描述了 Agent 的模型、功能及学习机制。部分技术已在国家电网公司信息内网综合运维监管系统、信息外网安全监控系统中进行应用。在安全监控系统深化应用过程中,仍需解决若干技术难题,例如,在学习算法中需预先建立案例知识库并进行持续更新、网络安全状态的高效率检索匹配问题。此外,建立和完善网络安全指标体系也是下一步工作的计划。

参 考 文 献

[1] Bass T. Intrusion detection systems and multisensor data fusion: creating cyberspace situational awareness[J]. Communications of the ACM, 2000, 43(4): 99-105

[2] 李硕,戴欣,周渝霞. 网络安全态势感知研究进展[J]. 计算机应用研究,2010,27(9):3227-3232

[3] 王选宏,肖云. 基于信息融合的网络安全态势感知模型[J]. 科学技术与工程,2010,10(28):6899-6902

[4] 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

[5] 冯学伟,王东霞,马国庆,等. 网络安全态势感知中态势评估关键技术研究[J]. 计算机工程与应用,2011,47(19):88-92

[6] 李颖. NSSA 中网络安全态势预测研究[J]. 技术与市场,2010,17(12):43-44

[7] 向西西,黄宏光,李予东. 基于 Kalman 算法的网络安全态势预测方法[J]. 计算机仿真,2010,27(12):113-116

[8] 刘念,刘孙俊,刘勇,等. 一种基于免疫的网络安全态势感知方法[J]. 计算机科学,2010,37(1):126-129

[9] Endsley M R. Toward a theory of situation awareness in dynamic systems[J]. Human Factors The Journal of the Human Factors and Ergonomics Society, 1995, 37(1): 32-64

[10] 贾焰,王晓伟,韩伟红,等. YHSSAS:面向大规模网络的安全态势感知系统[J]. 计算机科学,2011,38(2):4-8

[11] 赖积保,王颖,王慧强,等. 基于多源异构传感器的网络安全态势感知系统结构研究[J]. 计算机科学,2011,38(3):144-149

[12] Wooldridge M, Jennings N R. Intelligent Agents: Theory and Practice[J]. Knowledge Engineering Review, 1995, 10(2): 1-67

[13] Jennings N R, Sycara K, Wooldridge M. A roadmap of agent research and development[J]. Autonomous Agents and Multi-Agent Systems, 1998, 1(1): 7-38

[14] 卢爱平,郝洪亮,穆殿宝,等. 基于移动 Agent 的网络安全态势感知模型[J]. 科学技术与工程,2011,11(19):4646-4651

[15] Chen S H, Jakeman A J, Norton J P. Artificial Intelligence techniques, An introduction to their use for modelling environmental systems[J]. Mathematics and Computers in Simulation, 2008, 78: 379-400

[16] Harmon M E, Harmon S S. Reinforcement learning: A tutorial [R/OL]. http://www.nada.kth.se/kurser/kth/2D1432/2004/rltutorial.pdf, 1996