集对分析的可信网络安全态势评估与预测

吴 琨, 白中英

(北京邮电大学 计算机学院,100876 北京,sherrywukun@163.com)

摘 要: 为了解决可信网络中网络管理和安全监控审计的问题,通过对可信网络连接框架(TNC)和网络态势感知体系(CSA)的研究,针对可信网络安全中多数据源确定性与不确定性的特点,提出了基于集对分析的网络安全态势评估与预测方法 SPSAF. SPSAF 首先采用基于特征库的方法审计网络连接信息、系统管理信息、系统监控信息和应用服务信息,然后综合改进的熵权法和层次分析法提取安全态势指标权重,再利用集对分析方法对安全态势指标进行评估得到网络安全态势值,进而绘制网络安全态势图,最后采用 Box-Jenkin 模型基于安全态势值预测网络安全趋势. 仿真实验结果表明 SPSAF 能够准确有效地反映当前及未来的网络安全态势,有助于管理员有效地制定网络安全策略,并能及时发现风险,迅速准确地调整策略和实施应对措施,提供更全面可靠的网络安全保障.

关键词: 可信网络连接;安全态势评估;集对分析;Box-Jenkin 模型

中图分类号: TP393.08 **文献标志码:** A **文章编号:** 0367-6234(2012)03-0112-07

Trusted network security situational awareness and forecast based on SPA

WU Kun, BAI Zhong-ying

(School of the Computer Science, Beijing University of Posts and Telecommunications, 100876 Beijing, China, sherrywukun@163.com)

Abstract: To solve the problems of network management and security monitoring and auditing in trusted network, by researching the framework of trusted network connect (TNC) and the architecture of cyberspace situational awareness (CSA), in view of the certain and uncertain characteristics of multi-source information in trusted network security, a new security situational awareness and forecast based on set pair analysis (SPA) called SPSAF is proposed. SPSAF audited network connection information, system management information, system monitoring information and application service information by the method based on feature base. The security situational indexes were extracted by the method of improved entropy method (EM) and analytic hierarchy process (AHP). The SPA method was utilized to assess these indexes to get the value of network security situation, and the security-situation-graph of network was drawn. The time series of the assessment results was analyzed via the Box-Jenkin model to forecast the network security trend. The simulation experiment results show that SPSAF is accurate and effective to reflect the network security situation and its trend, which can help the administrator to make security policies efficiently, to discover risks timely, to adjust policies and take relevant protective or emergency measures quickly and accurately, and to ensure overall and reliable security.

Key words: trusted network connect; security situational awareness; set pair analysis; box-Jenkin model

面对复杂网络环境中日益凸显的各种安全风险与威胁,可信计算组织(Trusted Computing Group, TCG)的可信网络连接(Trusted Network Connect, TNC)工作组定义了一个开放的体系架构从终端到网络自底向上地保证计算系统的可信. 它根据终端完整性度量决策其是否可以接入网络,同时利用网络中的安全检控设备实时监控已经接入网络的终端,以动态改变连接状态[1]. 虽然 TNC 在网络接入层面实施了有效可靠的措

收稿日期: 2011-11-22.
基金项目: 国家高技术研究发展基金资助项目(2007CB310704);
国家自然科学基金资助项目(60821001).
作者简介: 吴 琨(1980—),女,博士研究生;
白中英(1941—),男,教授,博士生导师.

施,但在访问控制及安全审计方面仍然需要做大量的改进和完善工作.

针对现有网络管理不足以及发展需求的问题,网络态势感知(Cyberspace Situational Awareness, CSA)研究了如何在大规模、复杂和不确定的网络环境中获取、理解、评估、显示引起网络态势变化的要素以及对未来发展趋势进行预测. 目前研究的热点集中在 CSA 模型、知识表示和评估方法 3 个方面. 本文针对可信网络管理及安全监控审计方面存在的问题,利用 CSA 技术体系,提出了一种层次化的安全高效的可信网络安全态势评估与预测方法 (Set Pair Situational Awareness And Forecast, SPSAF). SPSAF 基于增强的 TNC 功能架构,提取并综合评估可信网络安全多种因素,动态整体地反映网络安全状况,并预测和预警网络安全发展趋势. SPSAF 解决了传统的单一的检控设备无法满足网络安全需求的问题,为网络管理提供了重要、可靠的参考依据,增强了可信网络的安全性、完整性和可用性.

1　相关研究

基于 TNC 的可信网络要求终端在访问应用前,首先要通过用户和终端身份的认证,然后度量终端平台的完整性状态,判断其是否满足网络接入安全策略,如果符合策略,则允许终端接入网络,否则将终端连接到预先指定的隔离区对其进行安全性修补和升级. 同时,已入网的终端要接受网络安全检控设备的实时监测,系统依据其安全运行状况决策其连接状态.

虽然可信网络中的主机、组件和设备从不同角度对网络及设备安全运行状况进行监控,它们产生的日志和报警之间也存在大量的关联性,但传统的监控审计方法通常只分析单一数据源,且安全设备本身具有不确定性,这些导致了监控审计分析结果出现较大偏差. 而且,现有的监控审计设备并没有预知网络安全趋势的能力.

CSA 作为网络管理具有潜力的发展方向,与传统方法相比具有更多的优势:1)利用数据融合技术,综合考虑影响网络态势的多种因素,提供全面、宏观的网络状况分析,增强网络认知与检控,减轻网络管理负担;2)成为集成单元网管的平台,改变当前各单元网管各自为政的工作局面,实现信息共享,丰富决策信息并产生准确的分析结果;3)为评估风险和制定决策提供支持,决策几乎可以依态势感知的完成而自动生成[2]. 国内外的研究人员从不同角度对 CSA 进行了大量的研究,并取得了很多有价值的成果.

Bass[3-4] 于 1999 年首次提出 CSA 的概念. 在模型方面,提出了基于多传感器数据融合入侵检测系统(IDS)的层次结构. 在知识表示方面,区分了陈述式知识和过程式知识,还借用 SNMP MIB 模型表示安全威胁分类,建立 TCP/IP 威胁分类框架. 在评估方面,提出了预防、检测、矫正的信息保障机制,建立基于重要性、脆弱性和威胁三大风险要素的风险识别模型. 但没有实现具体的原型系统.

JDL 模型[5] 将融合分为目标细化、态势细化、风险细化和过程细化 4 个层次. 其中,态势感知作为较高层次的 level 2 融合,向下从 level 1 融合接收网络元素的监测数据,作为态势感知的信息来源;向上为 level 3 融合提供态势信息,用于威胁分析和决策支持.

Lau[6] 开发了 The Spinning Cube of Potential Doom 系统,将网络连接以点的方式映射到三维空间中,并根据连接时间和内容的危险性显示不同的颜色,但该方法只可视化了原始流量数据,并没有对高层态势信息进行抽象.

Blasch 等[7] 通过引入测度的概念建立标准化的融合系统性能评价方法,提出了最小测度集合,并明确了计算公式.

赵国生等[8] 提出了一种非等时距灰色 Verhulst 残差修正的安全态势感知模型. 由非等时距的原始采样风险数据序列入手,根据累加序列所呈现出“S”形或反“S”形的摆动特征,选用灰色 Verhulst 模型或其反函数模型预测出网络未来的风险值,然后基于多级残差对模型的预测精度进行修正,最后应用修正后的新模型得到直观的网络未来安全态势曲线图.

张勇等[9] 提出一种基于 Markov 博弈分析的网络安全态势感知方法. 该方法通过对多传感器检测到的安全数据进行融合,得到资产、威胁和脆弱性的规范化数据;对每个威胁分析其传播规律,建立相应的威胁传播网络;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 Markov 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.

依据上述文献为进一步解决和完善可信资源安全共享问题,本文增强了 TNC 的保护框架,结合 CSA 技术方法,提出了 SPSAF 方法. 在 SPSAF 中,对 TNC 环境中包括网络连接、系统管理、系统监控和应用服务在内的多数据源信息进行综合分析,采用基于特征库的方法审计安全态势指标信息,综合改进的熵权法和层次分析法提取安全态

势指标权重,再利用集对分析方法对安全态势指标进行评估得到网络安全态势值,进而绘制网络安全态势图,最后采用 Box-Jenkin 模型[10]基于安全态势值预测网络安全变化趋势.

2 SPSAF 架构

TNC 体系架构包括 5 个实体:访问请求者(Access Requestor, AR)、策略执行点(Policy Enforcement Point, PEP)、策略决定点(Policy Decision Point, PDP)、元数据访问点服务器(Metadata Access Point Server, MAPS)、元数据访问点客户端(MAP Client, MAPC). 其中:AR 收集平台完整性信息向 PEP 请求建立网络连接;PEP 征询 PDP 是否授权 AR 的访问;PDP 认证 AR 和平台的身份,并验证平台完整性状态是否满足本地安全策略,最终允许、禁止或隔离 AR 的访问;MAPS 聚集了由其他 TNC 组件发布、订阅、搜索的有关网络流量、网络管理和网络安全的数据,这些数据有助于决策生成和策略执行;MAPC 由流控制器(如防火墙)和传感器(如 IDS)组成,它们与 PDP 及 PEP 协同监控网络活动并一致执行网络安全策略.

如图 1 所示,在 TNC 框架的基础上增加了 5 个实体:认证服务器(Authentication Server, AS)、身份管理点(Identity Management Point, IMP)、密钥管理点(Key Management Point, KMP)、应用管理点(Application Management Point, AMP)、域管理点(Domain Management Point, DMP). 其中:AS 认证 AR 的身份;IMP 标识、分发和维护合法用户的身份,同时映射其他可信域的 AR;KMP 为用户和系统组件生成和管理私钥,以实现系统安全通信;AMP 管理本地应用和映射其他可信域的应用,同时管理应用评价和授权本地合法用户的访问,并实现单点登录;DMP 建立并维护域间交叉认证,并实现跨域身份注册和单点登录.

另外,本文在 PDP 中增加了 2 个模块:1)集成了多种认证插件以提取不同的身份凭证提交给相应的 AS;2)依据基本完整性信息、动态行为特征和历史访问评价计算 AR 的安全度值.

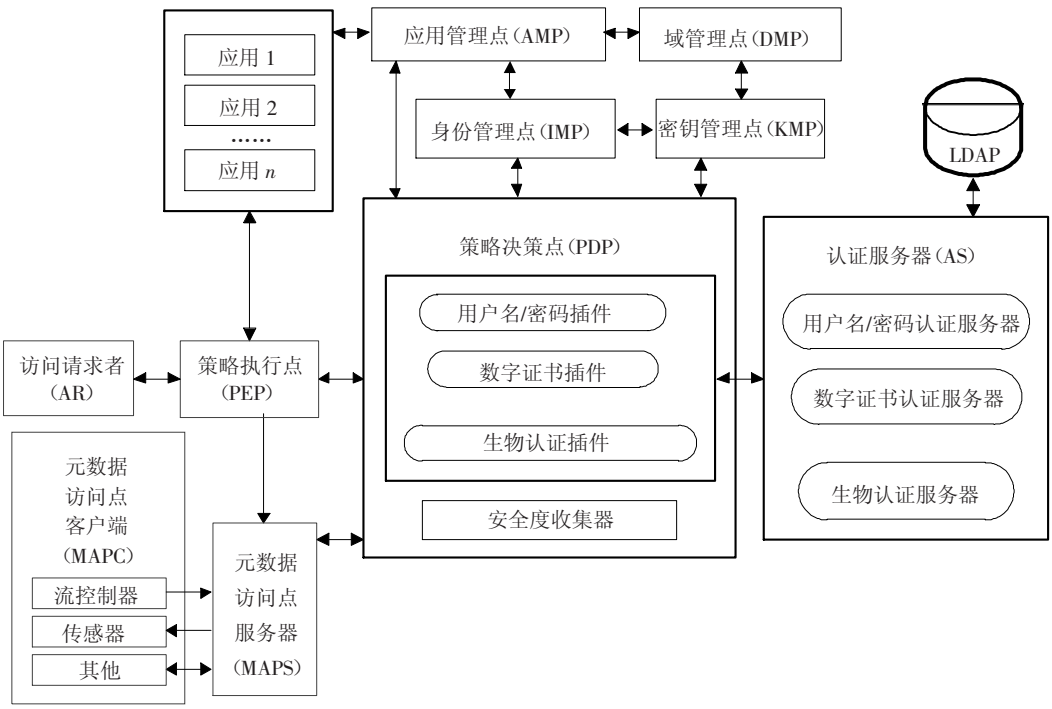

图 1 增强的 TNC 架构

依据增强的 TNC 架构中网络设备的不同功能和作用,将安全态势指标归纳为以下 4 类.

定义 1 连接信息(C)为

$C = (\mathrm{ID}_C, \mathrm{Time}_C, \mathrm{Type}, w_C, \mathrm{Data}_C, \mathrm{ID}_A, \mathrm{ID}_B)$.

式中 C 为一个七元组,主要包含了连接请求信息、连接执行信息、连接决策信息、连接认证信息及 AR、PEP、PDP 和 AS 的系统安全日志. 其中:ID_C 为连接信息的唯一标识符;Time_C 为连接信息产生的时间;Type 为连接信息的类型(其中包含 5 种类型:Req(连接请求信息)、Enf(连接执行信息)、Dec(连接决策信息)、Auth(连接认证信息)、Sys(系统安全日志));w_C 为连接权重;Data_C 为连接信息的内容;ID_A 为产生连接信息的节点标识符;ID_B 为连接信息作用的目标节点标识符.

定义 2 管理信息(G)为

$G = (\mathrm{ID}_G, \mathrm{Time}_G, w_G, \mathrm{Data}_G, \mathrm{ID}_P, \mathrm{ID}_Q)$.

式中 G 为一个六元组,主要包含了管理组件(包括 IMP、KMP、AMP 和 DMP)的日志记录. 其中:

ID_G 为管理信息的唯一标识符;$Time_G$ 为管理信息产生的时间;w_G 为管理权重;$Data_G$ 为管理信息的内容;ID_P 为产生管理信息的节点标识符;ID_Q 为管理信息作用的目标节点标识符.

定义 3　监控信息(M) 为

$$M = (ID_M, Time_M, w_M, Data_M, ID_S, ID_T).$$

式中 M 为一个六元组, 主要包含了 MAPC(如 Firewall、IDS)日志中漏洞扫描、端口扫描和入侵检测的记录. 其中: ID_M 为监控信息的唯一标识符;$Time_M$ 为监控信息产生的时间;w_M 为监控权重;$Data_M$ 为监控信息的内容;ID_S 为产生监控信息的节点标识符;ID_T 为监控信息作用的目标节点标识符.

定义 4　应用信息(A) 为

$$A = (ID_A, Application, w_A, Data_A, ID_L).$$

式中 A 为一个五元组,主要包含了 MAPS 和各个应用节点的访问日志. 其中: ID_A 为应用信息的唯一标识符; Application 为应用名称; w_A 为应用权重;$Data_A$ 为应用信息的内容;ID_L 为应用信息所属节点标识符.

定义 5　网络安全态势(N) 为

$$N = (C, G, M, A).$$

式中 N 为一个四元组,由连接信息、管理信息、监控信息和应用信息共同组成.

SPSAF 架构如图 2 所示,由 4 个步骤组成.

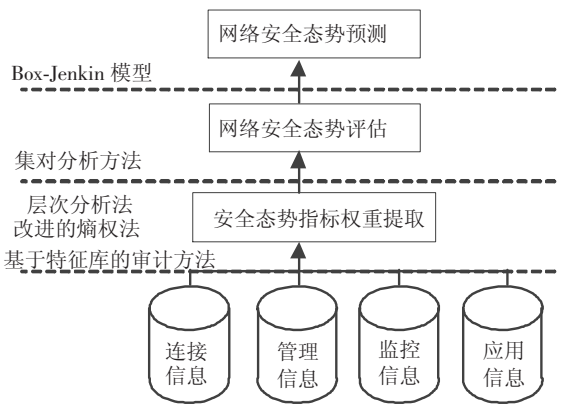

图 2　SPSAF 架构

1)采用基于特征库的方法审计 4 类信息的安全态势指标.

2)综合改进的熵权法和层次分析法提取安全态势指标权重.

3)利用集对分析方法评估安全态势指标计算出网络安全态势值.

4)采用 Box-Jenkin 模型依据不同时段的网络安全态势值预测可信网络安全态势变化趋势.

3　安全态势评估

集对分析方法[11]是处理不确定性问题的优良方法,具有分析步骤简洁、评价结果准确、客观、全面的优点. 它在指定问题背景下分析一个集合对的特性,找出它们的共性、对立性和既非共性又非对立性的差异性,由此建立起两个集合的同异反联系度,其中"同"和"反"代表确定性,而"异"代表不确定性. 同、异、反三者是相互联系、相互影响、相互制约的,在一定条件下它们可以相互转化. 可以将联系度推广到 >2 个集合时的情况进一步展开研究.

定义 6　集合 A 和 B 的联系度为

$$\mu = \frac{S}{N} + \frac{F}{N}i + \frac{P}{N}j. \tag{1}$$

式中: N 为集对特性总数;S 为集对中共性数目;P 为集对中对立性数目;F 为集对中差异性数目;$F = N - S - P$;S/N、F/N、P/N 分别为同一度、差异度、对立度. 令 $a = S/N, b = F/N, c = P/N$,则式(1) 可简写为

$$\mu = a + bi + cj. \tag{2}$$

式中: $a + b + c = 1$;$i \in [-1, 1]$ 为差异度系数,体现确定性与不确定性之间的相互转化. 当 i 为 1 时,不确定度转化为同一度;当 i 为 -1 时,不确定度转化为对立度;j 为对立度系数,运算时恒取 -1.

定义 7　扩展的联系度为

$$\mu = \frac{S}{N} + \frac{F_1}{N}i_1 + \frac{F_2}{N}i_2 + \cdots + \frac{F_m}{N}i_m + \frac{P}{N}j. \tag{3}$$

式(3)可简写为

$$\mu = a + b_1 i_1 + b_2 i_2 + \cdots + b_m i_m + cj. \tag{4}$$

式中: $a + b_1 + b_2 + \cdots + b_m + c = 1$;$i_1, i_2, \cdots, i_m$ 为差异度系数; j 为对立度系数.

3.1　安全态势指标权重提取

3.1.1　采用基于特征库的方法审计 4 类安全态势指标信息

根据指定的采样点,将连接信息、管理信息、监控信息、应用信息分别与特征库进行匹配得到初步的安全事件,依据信息内容归并删除重复的安全事件,再通过关联分析抽象出攻击事件、不确定但偏攻击事件、不确定事件、不确定但偏非攻击事件和非攻击事件,它们分别对应联系度表达式中的 a、b_1、b_2、b_3、c,其值计算为

$$a = \sum_{i=1}^{x} w_a^{(i)}; b_1 = \sum_{j=1}^{y} w_{b_1}^{(j)};$$

$$b_2 = \sum_{k=1}^{z} w_{b_2}^{(k)}; b_3 = \sum_{p=1}^{s} w_{b_3}^{(p)}; c = \sum_{q=1}^{t} w_c^{(q)}. \tag{5}$$

式中: $w_a^{(i)}$、$w_{b_1}^{(j)}$、$w_{b_2}^{(k)}$、$w_{b_3}^{(p)}$、$w_c^{(q)}$ 分别为匹配成功的信息的权重;x、y、z、s、t 分别为匹配成功的信息

数量.

由上述分析得到安全态势指标的联系度矩阵为

$$U = \begin{bmatrix} a^{(C)} & b_1^{(C)} & b_2^{(C)} & b_3^{(C)} & c^{(C)} \\ a^{(G)} & b_1^{(G)} & b_2^{(G)} & b_3^{(G)} & c^{(G)} \\ a^{(M)} & b_1^{(M)} & b_2^{(M)} & b_3^{(M)} & c^{(M)} \\ a^{(A)} & b_1^{(A)} & b_2^{(A)} & b_3^{(A)} & c^{(A)} \end{bmatrix}.$$

运用式(4)计算每类安全指标信息的态势值分别为 μ_C、μ_G、μ_M、μ_A.

3.1.2 运用改进的熵权法(Entropy Method, EM)由算法 1 提取各安全态势指标的客观权重值

算法 1 安全态势指标客观权向量提取算法.

输入: 安全指标信息态势值.

输出: 安全态势指标客观权向量.

步骤 1 根据多个时段的态势采样值建立评估矩阵 $\boldsymbol{X} = (x_{ij})_{m\times n}$,其中:$m$ 为采样时段数;n 为安全指标数.

步骤 2 运用式(6)得到第 j 项指标的均值 $\overline{x_j}$;运用式(7)得到第 j 项指标的标准差 σ_j. 运用式(8)得到用标准化法改进的 x_{ij}.

$$\overline{x_j} = \frac{\sum_{k=1}^{m} x_{kj}}{m}. \tag{6}$$

$$\sigma_j = \sqrt{\frac{\sum_{k=1}^{m} (x_{kj} - \overline{x_j})^2}{m-1}}. \tag{7}$$

$$x_{ij} = (x_{ij} - \overline{x_j})/\sigma. \tag{8}$$

步骤 3 运用归一化 X,得到矩阵 $\boldsymbol{Y}$ 为

$$\boldsymbol{Y} = \left(\frac{x_{ij}}{\sum_{k=1}^{m} x_{kj}}\right)_{m\times n}.$$

步骤 4 计算第 j 项指标的熵值 z_j 为

$$z_j = -\frac{1}{\ln m}\sum_{k=1}^{m} y_{kj}\ln y_{kj}.$$

步骤 5 计算第 j 项指标的差异性系数 s_j 为

$$s_j = \frac{1}{z_j}.$$

步骤 6 到安全指标客观权向量为 $\boldsymbol{W}_{\text{obj}}$ 为

$$\boldsymbol{W}_{\text{obj}} = \left(\frac{s_j}{\sum_{j}^{n} s_j}\right).$$

3.1.3 运用层次分析法(Analytic Hierarchy Process, AHP)由算法 2 提取各安全态势指标的主观权重值

算法 2 安全态势指标主观权向量提取算法.

输入: 安全态势指标两两比较值.

输出: 安全态势指标主观权向量.

步骤 1 构造安全态势指标两两比较矩阵 $\boldsymbol{E}$ 为

$$\boldsymbol{E} = \begin{bmatrix} e_{CC} & e_{CG} & e_{CM} & e_{CA} \\ e_{GC} & e_{GG} & e_{GM} & e_{GA} \\ e_{MC} & e_{MG} & e_{MM} & e_{MA} \\ e_{AC} & e_{AG} & e_{AM} & e_{AA} \end{bmatrix}.$$

步骤 2 归一化 $\boldsymbol{E}$ 为

$$\overline{\boldsymbol{E}} = \left(\frac{e_{ij}}{\sum_{k=1}^{4} e_{kj}}\right)_{4\times 4}.$$

步骤 3 得到 $\overline{\boldsymbol{E}}$ 的权向量 $\overline{\boldsymbol{W}}$ 为

$$\overline{\boldsymbol{W}} = \left(\sum_{k=1}^{4} \overline{e_{ik}}\right).$$

步骤 4 运用归一化 $\overline{\boldsymbol{W}}$ 得到 $\boldsymbol{E}$ 的权向量 $\boldsymbol{W}$ 为

$$\boldsymbol{W} = \left(\frac{\overline{w_i}}{\sum_{k=1}^{4} \overline{w_k}}\right).$$

步骤 5 $\boldsymbol{E}$ 的特征方程为

$$\boldsymbol{E}\boldsymbol{W} = \lambda_{\max}\boldsymbol{W}.$$

式中: $\lambda_{\max}$ 为最大特征根;$\boldsymbol{W}$ 为相应的特征向量. 解出 $\lambda_{\max}$,进行一致性和随机性检验. 如果检验通过,则 $\boldsymbol{E}$ 和其权向量 $\boldsymbol{W}$ 可以接受,此时 $\boldsymbol{W}$ 即为安全指标主观权向量 $\boldsymbol{W}_{\text{sub}}$;否则调整 $\boldsymbol{E}$,直到检验通过.

综合 $\boldsymbol{W}_{\text{obj}}$ 和 $\boldsymbol{W}_{\text{sub}}$ 得到安全态势指标权向量 $\boldsymbol{W}_N = (w_C, w_G, w_M, w_A)$,计算方法为

$$\boldsymbol{W}_N = \left(\frac{w_{\text{obj}}^{(i)} \cdot w_{\text{sub}}^{(i)}}{\sum_{k=1}^{4} w_{\text{obj}}^{(k)} \cdot w_{\text{sub}}^{(k)}}\right).$$

3.2 安全态势值评估

根据安全态势指标权重和联系度矩阵计算集对联系度得到

$$\mu_N = [w_C, w_G, w_M, w_A] \cdot \begin{bmatrix} a^{(C)} & b_1^{(C)} & b_2^{(C)} & b_3^{(C)} & c^{(C)} \\ a^{(G)} & b_1^{(G)} & b_2^{(G)} & b_3^{(G)} & c^{(G)} \\ a^{(M)} & b_1^{(M)} & b_2^{(M)} & b_3^{(M)} & c^{(M)} \\ a^{(A)} & b_1^{(A)} & b_2^{(A)} & b_3^{(A)} & c^{(A)} \end{bmatrix} \begin{bmatrix} 1 \\ i_1 \\ i_2 \\ i_3 \\ j \end{bmatrix} =$$

$$a_N + i_1 + i_2 + i_3 + c_N j. \tag{9}$$

计算网络安全态势值为

$$H_N = \frac{c_N}{a_N}. \tag{10}$$

根据多个时段的网络安全态势值可以绘制网络安全态势图以反映可信网络安全总体状况.

4　安全态势预测

时间序列是参数集和状态空间都可列的随机过程,是按照时间顺序取得的一系列观测值,它的本质特征是相邻观测值的前后依赖性. 基于时间序列分析的方法立足于概率论与统计学,能够很好地刻画序列的前后依赖关系,准确预测序列的变化趋势. 首先采样过去和当前多个时段的网络安全态势值得到时间序列,然后利用 Box-Jenkin 模型[10]预测未来网络安全趋势.

Box-Jenkin 模型对原序列进行周期差分和趋势差分,将非平稳时间序列转化为平稳时间序列,再根据新序列的自相关函数和偏相关函数的性质,建立自回归滑动平均模型分析新序列的变化规律.

首先由算法 3 得到 Box-Jenkin 时间序列输出值.

算法 3　时间序列分析算法.

输入:网络安全态势值.

输出: Box-Jenkin 模型时间序列输出值.

步骤 1　计算时间序列 T_i 的均值,使 $T_i = T_i - \overline{T_i}$,设置趋势差分阶数 $\alpha = 3$.

$$\overline{T_i} = \frac{1}{L}\left(\sum_{i=1}^{L} T_i\right).$$

式中 L 为 T_i 的周期长度.

步骤 2　计算 T_i 的自相关函数估计 β_k 为

$$v_k = \frac{1}{L}\sum_{i=1}^{L-k} T_i \cdot T_{i+k},$$

$$\beta_k = \frac{v_k}{v_0}.$$

式中: $k = \{1, 2, \cdots, \lfloor L/4 \rfloor\}$; v_0 为 T_i 的方差估计; v_k 为 T_i 的自协方差估计.

步骤 3　如果 β_k 的滞后期延长很快趋于零,则 T_i 为平稳时间序列,转到步骤 6.

步骤 4　如果 $\alpha > 0$,则对 T_i 做一阶趋势差分 $T_i = T_i = 1 - Z$,其中 Z 为后移算子, $ZT_i = T_{i-1}$. 同时 $\alpha = \alpha - 1$,转到步骤 2.

步骤 5　如果非平稳时间序列 T_i 存在周期为 D 的特性,则对 T_i 做 D 阶季节差分 $T_i = {}_D T_i = 1 - Z^D$. 同时重新设置 $\alpha = 3$,转到步骤 2.

步骤 6　计算 T_i 的偏相关函数估计 $\gamma_{k,j}$ 为

$$\begin{bmatrix} 1 & \beta_1 & \cdots & \beta_{k-1} \\ \beta_1 & 1 & \cdots & \beta_{k-2} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{k-1} & \beta_{k-2} & \cdots & 1 \end{bmatrix} \begin{bmatrix} \gamma_{k,1} \\ \gamma_{k,2} \\ \cdots \\ \gamma_{k,k} \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \cdots \\ \beta_k \end{bmatrix}.$$

步骤 7　根据 β_k 和 $\gamma_{k,j}$ 的性质判断 $ARMA(p, q)$ 的阶数 p 和 q,其中: β_k 在 $q - p$ 步滞后很快指数衰减或正弦波衰减, $\gamma_{k,j}$ 在 $p - q$ 步滞后很快指数衰减或正弦波衰减. $ARMA(p, q)$ 的计算方法为

$$\Phi(Z) T_i = \Theta(Z) g_i.$$

式中: g_i 为高斯白噪声; $\Phi(Z) = 1 - \Phi_1 Z - \cdots - \Phi_p Z^p$; $\Theta(Z) = 1 - \Theta_1 Z - \cdots - \Theta_q Z^q$.

步骤 8　采用最小二乘法和最大似然法估计模型参数. 采样数据越多,参数估计误差对模型影响越小.

然后将以上算法得出的时间序列应用到预测公式(11)中,得到网络安全态势预测值为

$$T_{L+1} = T_L + \frac{1}{L}\sum_{i=1}^{L} \tau^i (T_{i+1} - T_i). \quad (11)$$

式中 $\tau \in [0, 1]$ 为遗忘因子.

依据预测值绘制网络安全趋势图可以指导网络管理及安全决策.

5　结果和分析

根据图 1 构建了可信网络及管理系统来验证 SPSAF 的有效性和性能. 实验仿真了不同网络设备在 10 个时段中遭到蠕虫攻击、SQL 注入攻击或 SYN Flood 攻击的情况. 以第 1 时段 AMP 遭到蠕虫攻击为例,审计 4 类安全指标信息得到联系度矩阵为

$$\boldsymbol{U}_1 = \begin{bmatrix} 0.7 & 0.1 & 0 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.1 & 0.2 & 0.5 \\ 0.4 & 0.1 & 0.1 & 0.1 & 0.3 \\ 0.2 & 0.1 & 0.1 & 0.2 & 0.4 \end{bmatrix}.$$

运用式(4)计算安全指标态势值. 考虑联系度中的不确定性和负面影响, 令 $i_1 = 0.25$, $i_2 = 0$, $i_3 = -0.75$, $j = -1$,得到 $\mu_C^{(1)} = 0.550$, $\mu_G^{(1)} = -0.525$, $\mu_M^{(1)} = 0.050$, $\mu_A^{(1)} = -0.325$. 同理得到 10 个时段的安全指标态势采样值,并建立评估矩阵 $\boldsymbol{X}$. 由算法 1 计算得到 $\boldsymbol{W}_{\text{obj}} = (0.28,\ 0.31,\ 0.22,\ 0.19)$, 由算法 2 计算得到 $\boldsymbol{W}_{\text{sub}} = (0.29,\ 0.35,\ 0.21,\ 0.15)$,综合 $\boldsymbol{W}_{\text{obj}}$ 和 $\boldsymbol{W}_{\text{sub}}$ 得到 $\boldsymbol{W}_N = (0.307,\ 0.410,\ 0.175,\ 0.108)$.

将 $\boldsymbol{W}_N$ 和 $\boldsymbol{U}_1$ 代入式(9)得到第 1 时段的联系度为

$$\mu_N^{(1)} = [0.307, 0.410, 0.175, 0.108] \cdot \begin{bmatrix} 0.7 & 0.1 & 0 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.1 & 0.2 & 0.5 \\ 0.4 & 0.1 & 0.1 & 0.1 & 0.3 \\ 0.2 & 0.1 & 0.1 & 0.2 & 0.4 \end{bmatrix} \begin{bmatrix} 1 \\ i_1 \\ i_2 \\ i_3 \\ j \end{bmatrix} =$$

$0.347\,5 + 0.1i_1 + 0.069\,03i_2 + 0.151\,8i_3 + 0.331\,4j$.

令 $i_1 = 0.25, i_2 = 0, i_3 = -0.75, j = -1$，得到 $\mu_N^{(1)} = -0.072\,75$. 运用式(10)计算网络安全态势值为 $H_N = 0.954$. 同理得到10个时段的网络安全态势值，并绘制出网络安全态势图如图3所示.

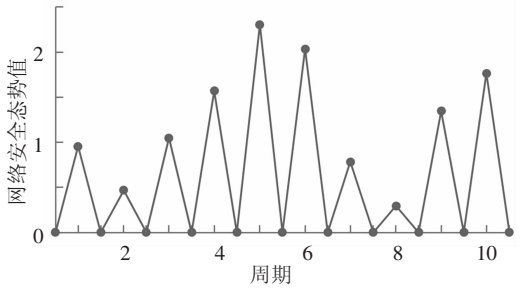

图3 网络安全态势图

由图3可以看出，网络安全态势曲线与仿真的网络安全状况基本一致，网络安全态势值越大表明网络安全状况越严重；安全指标信息权重越大、网络遭受攻击越多或攻击破坏度越大，则网络安全状况越差.

将以上10个时段的网络安全态势值作为时间序列输入值，运用 Box-Jenkin 模型得到时间序列输出值，利用预测公式(11)得到网络安全态势预测值. 如图4所示，预测结果与实际结果基本一致，表明 Box-Jenkin 模型预测误差较小，反映的安全态势因素与网络实际情况相符.

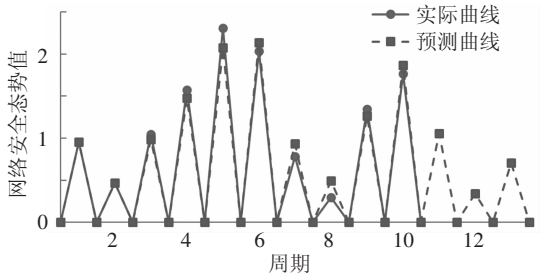

图4 网络安全态势预测结果与实际结果对比图

上述仿真结果表明，SPSAF 能有效提取不同网络设备的安全信息要素，综合分析影响网络态势的安全因素的确定性与不确定性，将各安全指标有机融合，准确评估当前网络安全状况，并通过时间序列分析法有效反映未来网络安全趋势，管理员可据此采取相应防护或应急措施，提高了网络安全性和可用性.

6 结 论

1）在增强的可信网络连接框架上，结合网络态势感知技术，提出了集对分析的网络安全态势评估与预测方法 SPSAF.

2）SPSAF 高效组织和审计可信网络中多种表示网络局部安全特征的要素，综合改进的熵权法和层次分析法提取安全信息指标权重，利用集对分析方法评估安全信息指标，根据得到的网络安全态势值绘制网络安全态势图. 同时，采用 Box-Jenkin 模型基于安全态势评估结果对网络安全变化趋势进行预测.

3）实验结果表明，SPSAF 能切实有效地反映可信网络安全态势及其发展趋势，实时量化的机制有利于管理员认知和理解网络安全状况，使其迅速准确地应对安全风险和威胁，更全面可靠地保障网络安全.

参考文献：

[1] TCG Trusted Network Connect. TNC Architecture for Interoperability Specification Version 1.4 Revision 4 [EB/OL]. (2009 - 05 - 18). http://www.t-rustedcomputinggroup.org/files/resource_files/51F9691E-1D09-3519-AD1C1E27D285F03B/TN-C_Architecture_v1_4_r4.pdf.

[2] 龚正虎，卓莹. 网络态势感知研究[J]. 软件学报，2010，21(7)：1605 - 1619.

[3] BASS T. Multisensor data fusion for next generation distributed intrusion detection systems [C]//Proceedings of the'99 IRIS National Sympon Sensor and Data Fusion. New York：Laurel，1999：24 - 27.

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

[5] HALL D，LLINAS J. An introduction to multisensor data fusion [J]. Proceedings of the IEEE，1997，85(1)：6 - 23.

[6] LAU S. The spinning cube of potential doom[J]. Communications of the ACM，2004，47(6)：25 - 26.

[7] BLASCH E，PRIBILSKI M，DAUGHTERY B，*et al*. Fusion metrics for dynamic situation analysis [C]//Kadar I，ed. Proceedings of the Signal Processing，Sensor Fusion，and Target Recognition XIII. Bellingham：SPIE，2004：428 - 438.

[8] 赵国生，王慧强，王健. 基于灰色 Verhulst 的网络安全态势感知模型[J]. 哈尔滨工业大学学报，2008，40(5)：798 - 801.

[9] 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.

[10] 张勇. 网络安全态势感知模型研究与系统实现[D]. 合肥：中国科学技术大学，2010.

[11] 郑贤斌，陈国明. 基于 SPA 安全综合评价方法及其应用[J]. 哈尔滨工业大学学报，2006，38(2)：290 - 293.

（编辑 张 红）