doi:10.3969/j.issn.1673-9833.2015.02.012

网络安全态势异常检测技术研究

文志诚，曹春丽

（湖南工业大学 计算机与通信学院，湖南 株洲 412007）

摘 要：网络安全态势感知已成为下一代安全技术的研究热点，有望解决网络安全与管理中某些方面的问题。针对目前网络安全态势异常检测的时空复杂度较高且不易操作等问题，提出通过一组观测样本，利用假设检验检测网络安全态势是否异常的一个可行的量化方法，该方法能预测系统安全态势变化趋势，为网络管理员制定决策和防御措施提供可靠依据，做到防患于未然。最后，利用仿真数据，对所提出的网络安全态势异常检测技术与算法进行了验证，结果验证了该方法的正确性且具有简捷可行性。

关键词：网络安全态势；异常检测；假设检验；网络安全；态势预测

中图分类号：TP393 **文献标志码**：A **文章编号**：1673-9833(2015)02-0064-05

Research on Network Security Situation Anomaly Detection

Wen Zhicheng，Cao Chunli

（School of Computer and Communication，Hunan University of Technology，Zhuzhou Hunan 412007，China）

Abstract：Network security situation awareness has become a hot research topic in the next generation security technology, and it is expected to solve the network security and management issues. In view of the current security situation anomaly detection with high space-time complexity and difficult operating problems, presents a feasible quantitative method through introducing a group of samples and using the hypothesis test for the abnormal detection of network security situation. The method can predict the trend of system security situation and provides a reliable basis for the network administrator's decision making and defensive measures, do nip in the bud. Finally, the proposed anomaly detection technique and algorithm of the network security situation are verified by using the simulation data. The results show that the method is correct and has the advantages of simple and feasible.

Keywords：network security situation；anomaly detection；hypothesis test；network security；situation prediction

0 引言

随着网络的飞速发展，计算机网络规模庞大，复杂性与不确定性也随之不断增加，安全问题日益突出，安全技术也一直在不断革新，虽然已经采取了各种网络安全防护措施，但是单一的安全防护措施没有综合考虑各种防护措施之间的关联性，无法满足从宏观角度评估网络安全性的需求。网络安全态势感知（network security situational awareness，NSSA）的研究就是在这种背景下应运而生的，它在融合各种网络安全要素的基础上从宏观角度实时评估网络的安全态势，并在一定条件下对网络安全态势的发展趋势进行预测预警，有望解决网络安全与管理问题。

T. Bass 于 1999 年首次提出了网络态势感知（cyberspace situational awareness，CSA）的概念[1]。

收稿日期：2015-01-15

基金项目：国家自然科学基金资助项目（61073186）

作者简介：文志诚（1972-），男，湖南东安人，湖南工业大学副教授，博士，主要从事网络安全，可信软件的研究，
E-mail：zcwen@mail.shu.edu.cn

网络态势是指由各种网络设备的运行状况、网络行为以及用户行为等要素所构成的整个网络当前状况与发展趋势。网络安全态势是网络态势的一种，通过网络安全态势感知来获取，是指对网络安全要素进行获取、理解、显示及预测未来发展趋势，综合各方面的安全因素，从整体上动态反映网络安全状况，并对未来安全状况的发展趋势进行预测和预警，为增强网络安全性提供可靠的参照依据。

网络安全态势感知研究是近几年发展起来的一个热门研究领域，它融合所有可能的信息实时获取网络的安全态势，为网络安全管理员的决策分析提供可靠依据，将不安全因素带来的风险和损失降到最低程度。网络安全态势感知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意义。网络安全态势通过网络安全态势感知获得，但是目前还没有明确定义，大多数学者用一个适当数值来综合表示当前安全态势的整体状况。

现代网络安全与管理必须能够在急剧动态的复杂环境中，高效组织海量不确定的网管信息并进行分析与评估，以及预测安全态势未来发展趋势。本文提出使用概率论中假设检验的方法检测网络安全态势发展是否正常及危险程度，掌握被管对象的详细信息，能提高网络管理员对整个网络运行状况的认知与理解，提供多样化、个性化的网络管理服务，当发现安全态势异常时，辅助指挥员迅速、准确地做出高层决策，弥补当前网络管理的不足。本方法主要根据网络中目前运行的状况，检测其安全态势是否异常，有2个主要创新：一是易于检测网络安全态势是否正常，操作方便简捷；二是易于了解网络安全态势偏离正常情况的程度，及时做出决策。

1　相关工作

近年来，网络态势感知技术已逐渐地被应用于网络安全与管理之中，但还没形成成熟的模型、方法和评价体系。国内外学者提出了很多可行的解决方法，为下一步的研究奠定了基础，但同时也存在着诸多不足：一般只停留在安全态势感知方法研究上，对安全态势发展趋势预测及异常检测还不够准确等，且大部分只侧重于概念研究，时空开销大，距离实际应用还有一段距离。

文献[2−3]给出了网络态势感知研究综述，在分析现有网络管理不足以及发展需求的基础上，介绍了网络态势感知的起源、概念、目标和特点，提出了一个网络态势感知研究框架，指出了研究重点以及存在的问题，着重评价了每种评估方法的基本思路、评估过程和优缺点，并进行了对比分析。

文献[4]提出了基于免疫理论的网络安全态势评估方法，并使用灰色理论进行预测，但该方法只能反映安全态势的趋势，对网络安全态势预测的实时性精度有待提高。

文献[5]采用线性回归的方法对网络态势进行预测，优化了网络带宽；文献[6]提出了一种基于似然BP（back propagation）的网络安全态势预测方法，通过态势评估模型建立态势序列作为训练序列，但是该方法参数训练过程复杂，收敛速度慢，不能满足实时性要求。

文献[7]提出了基于RBF（radial basis function）神经网络的态势预测方法，利用RBF神经网络处理非线性态势值，通过态势值之间的关系进行态势预测，但是该方法在实时网络态势感知中，容易陷入局部最优化问题，可能会导致结果不稳定。文献[8]提出了一种将ARMA（auto-regressive and moving average model）模型与HMM（hidden Markov model）模型相结合的网络态势预测方法，但由于建模时间较长，不能实时反映网络的安全态势。

文献[9]从理论与实际相结合的角度提出了一种基于隐Markov模型的实时网络安全态势预测模型HMM-NSSP（network security situation srediction method based on hidden Markov model），并给出了实时预测网络安全态势的方法。HMM-NSSP模型利用网络安全态势评估信息建立HMM网络安全态势预测模型，并通过网络节点的实时性能对参数进行动态修正，实现对整个网络安全态势实时监控与预测。

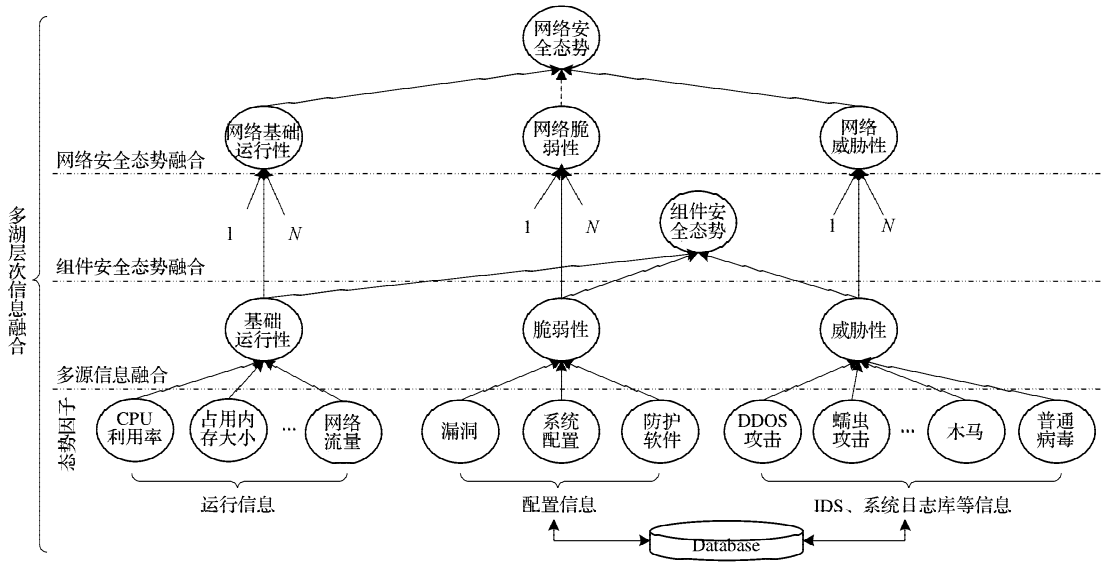
文献[10−11]通过对IDS（intrusion detection systems）与IPS（intrusion prevention system）等系统的报警信息融合处理，生成网络态势；文献[12]提出了建立一个能应用于其他领域的下一代网络态势感知系统，目的是提高决策者选择行为的过程，满足网络管理人员的真正需求。

2　网络安全态势

所谓网络安全态势是指由各种网络设备运行状况、网络行为以及用户行为等因素所构成的整个网络当前安全状态和变化趋势。值得注意的是，安全态势强调环境、动态性以及实体间的关系，是整个网络一种状态、一种趋势、一个整体和全局的概念，任何单一的情况或状态都不能称之为安全态势，涵

盖了实时依据安全网络设备告警与他类信息、融合数据、归并关联操作，进而有效反应实际网络的运行状况。网络安全态势一般通过网络安全态势感知获得，网络安全态势感知是指在大规模网络环境中，对能够引起网络安全态势发生变化的安全要素进行获取、理解、显示以及预测未来的发展趋势。目前，对网络态势感知还未能给出统一的、全面的定义，不同学者研究方法各异。

在安全态势生成方面，国内外相关研究多见于军事战场的态势生成，而网络安全领域的态势生成研究尚处于起步阶段，还没有普遍认可的解决方法。文献[12]中提出了一种计算综合威胁值的网络安全分级量化方法，该方法生成的态势值能够满足越危险的网络实体，威胁值越高。课题组将网络安全态势定义为由网络基础运行性（runnability）、网络脆弱性（vulnerability）和网络威胁性（threat）3个维度加权组成，向用户展示整个网络当前安全态势SA，是一个综合数值。网络安全态势感知框架如图1所示。



注：实线表示数据流，表示生成关系。

图1 网络安全态势感知框架示意图

Fig. 1 The framework for network security situation awareness

本文中，网络安全态势 SA_{n} 用一个具体数值表示，衡量安全态势的大小，一般由组件安全态势 SA_{c} 融合生成。网络的基础运行性、网络的脆弱性和网络的威胁性的每维可取“0, 1, 2”或“高、中、低”3等值，再由三维加权生成网络安全态势。根据专家经验，分配给每个维度的权重为 w_i（$i=1,2,3$），$w_1+w_2+w_3=100$，一般每个维度的值由分配的权重乘以取0的概率 $P_{j,0}$ 减去取2的概率 $P_{j,2}$。因为即使异常时，$P_{j,2}$ 一般也不会波动很大，毕竟正常网络组件占绝大多数，为了便于区分差别，扩大 $P_{j,2}$ 的λ倍，因此有：

$$SA_{\mathrm{n}}=\sum_{j=1}^{3}w_j\left[P_{j,0}-\lambda\cdot P_{j,2}\right], \tag{1}$$

$$P_{j,k}=\frac{1}{N}\sum_{i=1}^{N}P_{i,j,k}, \tag{2}$$

$$SA_{i,c}\leftarrow\sum_{j=1}^{3}w_j\left[P_{i,0}-\lambda\cdot P_{i,j,2}\right]。 \tag{3}$$

式（1）~（3）中 $P_{i,j}$ 表示组件的安全态势取值。

在生成网络安全态势之前，要生成第 i 个组件的安全态势 $SA_{i,\mathrm{c}}$，对于组件的安全态势 $SA_{i,\mathrm{c}}$ 的生成与网络的安全态势生成类似，如式（1）~（3）所示。网络安全态势生成，作者将在另文中详细阐述。

3 异常检测

网络安全态势 SA_{n} 由网络上的所有组件安全态势 SA_{c} 信息融合而成，一般由一个适当的数值表示当前网络安全态势状况。本文的网络安全态势异常检测，是通过采集一定量的安全态势样本，通过假设检验来检测网络是否处于正常状态。

3.1 假设检验

网络安全态势 SA_{n} 可以看成一个随机变量 X，设 $X_1, X_2, \cdots, X_n$ 来自总体 X 的 n 个观测样本，本文的主要问题是，从这 n 个观测样本判断目前网络安全态势是否正常，以及偏离正常状态的程度。基本的思路是，构造统计量，通过 t 统计量假设检验来检测假设是否成立。

设总体 $X\sim N(\mu,\ \sigma^2)$，μ表示随机变量 X 的数学期望，σ^2 表示 X 的方差，构造2个统计量：

$$\overline{X}=\frac{1}{n}\sum_{i=1}^{n}X_i;$$

$$S^2=\frac{1}{n-1}\sum_{i=1}^{n}\left(X_i-\overline{X}\right)^2。$$

其中，μ与σ^2都未知，用表示μ的无偏估计，用S^2表示σ^2的无偏估计。

检验网络安全态势是否正常可以转化为如下假设检验问题：

$$H_0:\mu=\mu_0,H_1:\mu\neq\mu_0。$$

式中：H_0为原假设，表示网络安全态势正常；H_1为备择假设，表示网络安全态势已产生异常情况。

由于$X_1,X_2,\cdots,X_n$是来自总体X的n个样本，具有独立同分布性质，式中σ^2未知，注意到S^2是σ^2的无偏估计，用S^2来代替σ^2，采用关于数学期望μ的检验（t 检验），令：$t=\dfrac{\overline{X}-\mu_0}{S/\sqrt{n}}$作为假设检验统计量。

当观察值$|t|=\left|\dfrac{\overline{X}-\mu_0}{S/\sqrt{n}}\right|$充分大时就拒绝$H_0$，拒绝域的形式为

$$|t|=\left|\frac{\overline{X}-\mu_0}{S/\sqrt{n}}\right|\geqslant k。$$

因此，由概率论知识可以得出，当H_0为真时，$t=\dfrac{\overline{X}-\mu_0}{S/\sqrt{n}}\sim t(n-1)$，故有

$P\{$当H_0为真拒绝$H_0\}=P\left\{\left|\dfrac{\overline{X}-\mu_0}{S/\sqrt{n}}\right|\geqslant k\right\}=\alpha$，这里$\alpha$为显著性水平。

设$k=t_{\alpha/2}(n-1)$，即得拒绝域为

$$|t|=\left|\frac{\overline{X}-\mu_0}{S/\sqrt{n}}\right|\geqslant t_{\alpha/2}(n-1)。$$

上述过程利用概率论中 t 统计量假设检验方法，从n个网络安全态势SA_n观测样本中计算μ无偏估计$\overline{X}$和σ^2无偏估计S^2，代入上式可计算出 t 统计量的值，通过查表获得$k=t_{\alpha/2}(n-1)$值，两值作对比。若在拒绝域之中，则备择假设H_1成立，表明网络安全态势已产生异常；若k值不在拒绝域之中，则原假设H_0成立，表示网络安全态势正常。再通过判断 t 统计量值的大小，得到此网络安全态势已偏离正常状态的程度，需要提前采取相应措施。这是本方法的 2 个主要创新之处。

有如下 2 种情况量化：

1）当$|t|<k$时，表示网络安全态势目前处于正常状态，若$|t|$值比较大，与k值相近，说明虽处于正常状态，但已接近异常状态，需提前作好防范措施；

2）当$|t|>k$时，表示网络安全态势目前处于异常状态，值越大，表明异常程度越严重。

3.2　检测算法

输入：网络安全态势的n个随机观测样本$X_1, X_2, \cdots, X_n$。

输出：判断假设检验H_0或H_1是否成立。

1）监测得到网络安全态势大样本数据，样本量足够大；

2）用大样本数据的平均值近似总体X的数学期望μ_0；

3）抽取最近网络安全态势n个随机观测样本$X_1, X_2, \cdots, X_n$；

4）计算样本的平均值$\overline{X}$与方差S^2；

5）取定显著性水平α，查表得出$k=t_{\alpha/2}(n-1)$值；

6）计算$|t|=\left|\dfrac{\overline{X}-\mu_0}{S/\sqrt{n}}\right|$值，若大于$k$值，则$H_1$成立，否则$H_0$成立。

H_0成立表示网络安全态势SA_n正常，若H_1成立表示网络安全态势产生异常，需要及时调整高层策略，防范于未然。通过判断 t 统计量值大小，还可以判断网络安全态势偏离正常状态的程度。

4　仿真试验

为了验证本文所提出网络安全态势异常检测技术及算法的合理性与正确性，采用 Matlab 7.0 进行仿真试验，试验过程中主要采用了随机抓取网络安全态势实时数据。

4.1　数学期望μ_0

检测网络安全态势是否正常，其实就是通过一组观测样本，给定一个显著性水平α，计算样本的均值μ是否在安全态势数学期望μ_0的拒绝之中，若在拒绝域之中，则备择假设H_1成立，表示安全态势已产生异常；若在拒绝域之外，原假设H_0成立，表示安全态势未产生异常。

因此首先需要获取网络安全态势数学期望μ_0，因为它是未知的，可通过大样本数据取其平均数。本文通过大样本，根据第 3 章中所述方法进行安全态势综合后，获得其数学期望近似为：

$$\hat{\mu}_0\leftarrow\overline{X}=\frac{1}{n}\sum_{i=1}^{n}X_i=96.16。$$

假设检验中的数学期望μ_0使用近似代替，这里样本量n要求充分大。

4.2　安全态势数字特征

网络安全态势异常检测，最重要的通过获得一组观测样本，计算其相关数字特征，如数学期望μ_0与方差σ^2的无偏估计，代入 t 检验的公式中，获得t值，通

过查表获取在显著性水平α下，其分位点$k=t_{\alpha/2}(n-1)$值，与之比较就可以确定是否落在拒绝域之中。

本试验通过监测得到n=20样本，经计算得到数学期望μ与方差σ^2的数字特征无偏估计如下：

$$\mu \leftarrow \hat{\mu}=\bar{x}=\frac{1}{n}(x_1+x_2+\cdots+x_n)=90.11,$$

$$\sigma \leftarrow \hat{\sigma}=\sqrt{\frac{1}{n-1}\sum_{j=1}^{n}(x_j-\bar{x})^2}=1.256。$$

4.3 异常检测

本文取显著性水平α=0.05，自由度为n−1=20−1=19，通过查t检验表，得：

$$k=t_{\alpha}(n-1)=t_{0.025}(19)=2.093\ 0。$$

把安全态势n=20个观测样本数学期望μ与方差σ^2的无偏估计$\overline{X}$与S^2代入

$$|t|=\left|\frac{\overline{X}-\mu_0}{S/\sqrt{n}}\right|=\left|\frac{99.11-96.16}{\sqrt{1.256}/\sqrt{9}}\right|=\left|\frac{-6.05}{3.36}\right|=1.801。$$

因此有$|t|<k$。

此结果表示此组20个样本的t值落在拒绝域之外，原假设H_0成立，表示安全态势未产生异常。特别说明，本组样本t值离k值非常近，虽然目前安全态势还算处于正常区域内，但已非常接近异常，为此需要考虑提前调整安全策略。

5 结语

针对目前网络安全态势异常检测的时空复杂度较高且不易操作等问题，本文提出使用概率论中假设检验的方法，通过一组网络安全态势观测样本，检测网络安全态势发展是否正常及危险程度，预测网络系统安全未来变化趋势，当发现安全态势异常时，辅助网络管理员迅速、准确地做出高层决策，弥补当前网络管理的不足。

参考文献：

[1] Bass T. Multi-Sensor Data Fusion for Next Generation Distributed Intrusion Detection Systems[C]//In Proc. of the'99 IRIS National Symp. on Sensor and Data Fusion. Laurel：[s. n.]，1999：24-27.

[2] 龚正虎,卓 莹. 网络态势感知研究[J]. 软件学报,2010，21(7)：1605-1619.
Gong Zhenghu，Zhuo Ying. Research on Cyberspace Situational Awareness[J]. Journal of Software，2010，21(7)：1605-1619.

[3] Bradshaw J M，Carvalho M，Bunch L，et al. Sol：An Agent-Based Framework for Cyber Situation Awareness[J]. Künstliche Intelligenz，2012，26(2)：127-140.

[4] Shi Yuanquan，Li Tao，Chen Wen. A Quantitative Model for Network Security Situation Awareness Based on Immunity and Grey Theory[C]//Computing Communication Control and Management(CCCM). Sanya：IEEE，2009：14-18.

[5] Chang K C，Yin Xiaoyan，Saha R K. A Linear Predictive Bandwidth Conservation Algorithm for Situation Awareness [C]//Decision and Control，Proceedings of the 37th IEEE Conference. Tampa：IEEE，1998：4726-4731.

[6] 唐成华,余顺争. 一种基于似然BP的网络安全态势预测方法[J]. 计算机科学，2009，36(19)：97-100，168.
Tang Chenghua，Yu Shunzheng. Method of Network Security Situation Prediction Based on Likelihood BP[J]. Computer Science，2009，36(19)：97-100，168.

[7] 任 伟，蒋兴浩，孙锬锋. 基于RBF神经网络的网络安全态势预测方法[J]. 计算机工程与应用，2006，42(31)：136-138.
Ren Wei，Jiang Xinghao，Sun Tanfeng. RBFNN-Based Prediction of Networks Security Situation[J]. Computer Engineering and Application，2006，42(31)：136-138.

[8] Wang Yan，Yang Wu，Wang Wei. A Combined Prediction Method for Network Security Situation[C]//2010 International Conference on Computational Intelligence and Software Engineering (CISE). Harbin：IEEE，2010：1-4.

[9] 黄同庆,庄 毅. 一种实时网络安全态势预测方法[J]. 小型微型计算机系统，2014，35(2)：303-306.
Huang Tongqing，Zhuang Yi. An Approach to Real-Time Network Security Situation Prediction[J]. Journal of Chinese Computer Systems，2014，35(2)：303-306.

[10] Shen D，Chen Genshe，Cruz J，et al. A Markov Game Theoretic Data Fusion Approach for Cyber Situational Awareness[C]//Proceeding of SPIE 6571. Orlando：[s. n.]，2007：1-11.

[11] Robert F E，Deborah A F，Pak Chung Wongb，et al. A Multi-Phase Network Situational Awareness Cognitive Task Analysis[J]. Information Visualization，2010，9(3)：204-219.

[12] Zhou C V，Leckie C，Karunasekera S. A Survey of Coordinated Attacks and Collaborative Intrusion Detection [J]. Elsevier Computers & Security Journal，2010，29(1)：124-140.

（责任编辑：申 剑）