

一种支持扩展指标体系的 SSUT 网络安全态势评估

李纪真¹, 孟相如¹, 杨 栋², 康巧燕¹

(1 空军工程大学 信息与导航学院, 陕西 西安 710077; 2 空军工程设计研究局, 北京 100068)

摘 要: 提出一种支持扩展指标体系的 SSUT 网络安全态势评估模型. 该模型将传统网络安全指标重新归类 and 量化, 并支持对常见或新指标的扩展. 采用支持向量机分类方法实现对网络安全态势的评估与分析. 仿真实验结果表明 SSUT 模型比普通模型分类准确率提高了近 15.4%~16.67%, 有效提升了网络安全态势评估的准确性.

关键词: 网络安全; 指标体系; 态势评估; 支持向量机

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2015)02-0015-05

An SSUT Network Security Situation Awareness Method Based on Supporting Extended Index System

LI Ji-zhen¹, MENG Xiang-ru¹, YANG Dong², KANG Qiao-yan¹

(1 School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China;

2 Air Force Engineering Design Institute, Beijing 100068, China)

Abstract: An SSUT network security situation awareness method based on supporting extended index system is proposed, it is to solve the problems that the current index system of network security situation awareness is lack of extendibility and unified norms, can not to meet the practice application environment and the personalized demand which cause the awareness result is not accurate enough. The traditional network security index system is reclassified and quantified in this method, which support for extending the common or new index. The Support Vector Machine is adopted as the classification method to evaluate and analyze the network security situation. It's proved through the simulation experiment results that the classification accuracy is increased about 15.4%~16.67% by the SSUT model than the traditional model, and the accuracy of the network security situation awareness is enhanced effectively.

Key words: network security; index system; situation awareness; Support Vector Machine

1 引言

网络安全态势评估(Network Security Situation Awareness, NSSA)是指通过相关技术和手段,感知并获取在一定时间和空间内网络安全态势的相关因素^[1],通过对数据信息的量化和关联分析,从整体上动态反映网络的安全状况,其结果可作为网络安全预警的依据,进而可以根据网络安全预警趋势进行应急响应决策^[2].该领域目前已成为网络安全领域中的一个研究热点.

构建指标体系是安全态势评估的关键,当前网络安全态势评估指标体系存在扩展性差,缺乏规范,难以满足实际应用环境和个性化需求等问题,导致评估结果不精准^[3-4].针对上述问题,本文从改进指标分类的角度出发,提出支持扩展指标体系的 SSUT 网络安全态势评估模型,结合支持向量机(Support Vector Machine, SVM)分类方法,将所选取的相关指标元素构成多维向量进行分类和评估.

收稿日期: 2014-06-06; 修回日期: 2014-07-23

基金项目: 国家自然科学基金资助项目(61201209)

2 安全指标 SSUT 分类及量化方法

2.1 安全指标 SSUT 分类法

本文将常规网络安全指标重新划分为内部安全指标 Safety、外部安全指标 Security 和用户类型的安全等级指标 User-Type, 记为网络安全指标 SSUT 分类法, 如图 1 所示。

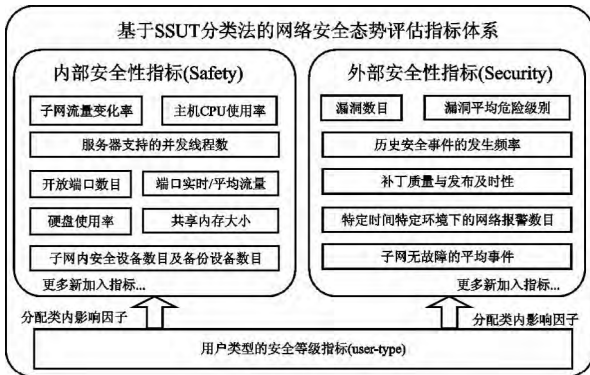


图 1 基于 SSUT 分类法的网络安全指标体系
Safety 指标更强调网络系统及其主机本身的可

表 1 安全指标数据预处理示例

类别	指标 ID	指标名称	数据来源	原始数据	预处理(归一化)结果	影响因子
内部安全指标 Safety	Sa1	CPU 使用率	Cacti 软件监测	45%	归入区间 $[0,1] \geq 0.45$	$R1=0.15$
	Sa2	硬盘使用率	Cacti 软件监测	30%	归入区间 $[0,1] \geq 0.30$	$R2=0.15$
	Sa3	内存使用率	Cacti 软件监测	65%	归入区间 $[0,1] \geq 0.65$	$R3=0.15$
	Sa4	支持并发链接数	服务器性能指标读取	500	按 1 000 上限, 归入区间 $[0,1] \geq 0.50$	$R4=0.05$
	Sa5	开放端口数目	命令探测	47	占总端口数比例归入 $[0,1] \geq 0.11$	$R5=0.25$
	Sa6	端口平均流量	Cacti 软件监测	23 kb/min	与最大流量之比归入 $[0,1] \geq 0.25$	$R6=0.05$
	Sa7	(非)安全设备百分比	读取监测结果并计算	15/20	归入区间 $[0,1] \geq 0.75$	$R7=0.1$
	Sa8	(非)备份设备百分比	管理员读取并计算	7/20	归入区间 $[0,1] \geq 0.35$	$R8=0.1$
外部安全指标 Security	Se1	漏洞数目	统计 Ovaldi 检测结果	24	按 100 上限, 归入区间 $[0,1] \geq 0.24$	$T1=0.2$
	Se2	漏洞平均危险级别	对检测结果做统计分析	6.4	按 CVSS 评分 $[0,1]$, 求平均值 ≥ 0.64	$T2=0.3$
	Se3	补丁及时性	从补丁库读取信息	7 天	按 100 上限, 归入区间 $[0,1] \geq 0.07$	$T3=0.1$
	Se4	补丁质量	对补丁来源分类量化	6.7	按 10 上限, 归入区间 $[0,1] \geq 0.67$	$T4=0.1$
	Se5	安全事件发生频率	读取报警日志	0.3 次/天	每天 3 次为上限, 归入 $[0,1] \geq 0.10$	$T5=0.15$
	Se6	(非)无故障平均时间	读取日志做计算	22.7 小时/天	除以 24 比值归入区间 $[0,1] \geq 0.05$	$T6=0.15$

定义 1 内部安全指数:内部安全指数是指各内部安全指标与其影响因子的内积, 即

$$\text{Safety} = \sum_{i=1}^8 (Sa_i \times R_i) = 0.385 \quad (1)$$

定义 2 外部安全指数:外部安全指数是指各外部安全指标与其影响因子的内积, 即

$$\text{Security} = \sum_{i=1}^6 (Se_i \times T_i) = 0.336 \quad (2)$$

靠性; Security 指标更强调对于外界攻击的防护水平; User-Type 指标根据用户对安全等级的需要或参考信息系统等级保护对安全设计的要求进行级别划分和扩展, 对各个级别采用不同的标识进行标记。

2.2 SSUT 指标量化方法

构建好网络安全指标体系并获取相应原始指标数据之后, 需要对数据进行融合, 即按照 SSUT 分类将指标进行量化, 从而得到一个具体的值。首先是原始指标数据的预处理, 表 1 中给出了一组原始指标数据预处理的示例。其中, 内部安全指标 Safety $\{Sa1, Sa2, Sa3, Sa4, Sa5, Sa6, Sa7, Sa8\}$ 对应的

影响因子为 $\{R1, R2, R3, R4, R5, R6, R7, R8\}$, 且满足 $\sum_{i=1}^8 R_i = 1$; 外部安全指标 Security $\{Se1, Se2, Se3, Se4, Se5, Se6\}$ 对应的影响因子为 $\{T1,$

$T2, T3, T4, T5, T6\}$, 且满足 $\sum_{i=1}^6 T_i = 1$; 影响因子由原始数据来源的用户等级指标 User-Type 所决定。

定义 3 用户类型指数:用户类型指数是指各类用户的安全等级(总共为 N 级), 即

$$\text{User-Type} = \{1, 2, \dots, N\} \quad (3)$$

网络安全指标体系 SSUT 量化方法由上述三类指标组成一个三维向量, 记为 $\text{SSUT} = \{\text{Safety}, \text{Security}, \text{User-Type}\}$, 作为态势评估模型的一条基础数据。SSUT 分类法最大的好处是可提高模型的扩展性, 当有新指标加入或者用户安全等级发生变

更时,只需对三个维度其中之一做出改变,其他两个维度及其指标评价则不受影响.指标量化即获取三维向量指标数据的流程如图2所示.

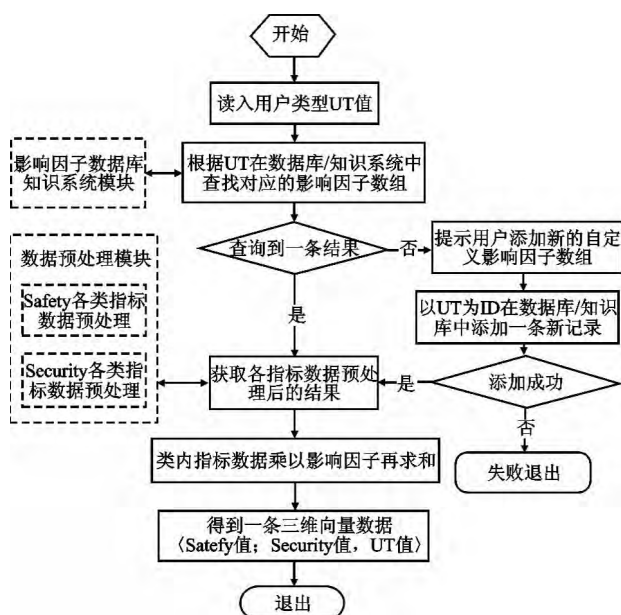


图2 获取三维安全指标向量流程图

对于指标体系基础数据的量化过程,结合影响因子的分配,可以看出:对于内部和外部两类安全指标,其类内指标可以具有相关性,这种相关性的强弱正是通过影响因子来进行调整;而内部和外部两类指标各自影响因子总和皆为1,即类间指标影响因子的分配互不影响,相关性相对较弱,甚至可以忽略.这样就在最大程度上减小了指标关联性对于评估模型及其评估结果的影响.

3 基于SVM的SSUT评估模型

根据上述网络安全指标SSUT分类方法和指标量化方法,结合SVM分类原理^[5-6],建立基于SVM的SSUT网络安全态势评估模型.评估模型主要由两部分组成,一是指标向量的获取,二是态势评估过程,如图3所示.

基于SVM的SSUT网络安全态势评估详细步骤描述如下:

Step1 首先通过相关软硬件或传感器在一定的网络环境中获取与网络安全有关的数据信息,并将获取的原始数据信息进行预处理和归一化,基本方法是如表1所示的数据预处理过程;

Step2 根据SSUT指标分类方法将预处理的数据进行指标归类,分别为内部安全指标Safety、外部安全指标Security和用户类型指标User-Type,

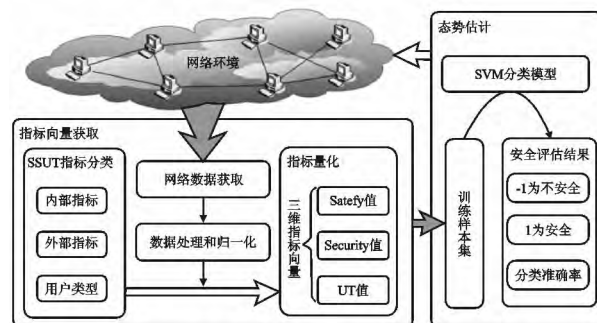


图3 基于SVM的SSUT网络安全态势评估模型
通过图2所示的量化流程将三类指标量化为一个三维向量 $SSUT = \{Safety, Security, User-Type\}$;

Step3 所有得到的三维向量构成模型的训练样本,根据先验知识对每组三维向量所代表的安全态势情况进行标记,标记为1表示当前处于安全状态,-1为不安全状态;

Step4 通过LIBSVM提供的相关函数对样本数据集进行训练,建立SVM分类模型;

Step5 LIBSVM建立的态势评估模型实现对样本数据的二分类,分类结果为1表示当前网络状态安全,-1表示当前网络状态不安全;

Step6 根据网络安全状态的评估结果,计算SVM分类模型的分类准确率,分类准确率越高代表评估结果就越准确,评估模型也就越优越.

4 实验与分析

实验的基础是一系列表征网络态势的原始数据,这些数据需要通过在相关主机上安装某些工具软件来获取,如cacti网络主机监测软件、nmap支持国标的漏洞扫描器、日志分析软件、简单的网络管理软件及相关命令等.通过上述软件获得240组原始部分数据,通过预处理得到240个三维向量构成实验训练样本集.

4.1 评估模型有效性验证与分析

在实验环境和相关函数参数不发生变化的前提下,对原始数据未使用SSUT分类法得到的十四维向量直接使用SVM进行安全态势评估,通过实验对比结果验证SSUT指标体系的有效性.

实验对比结果如表2所示.可以看出,通过将网络安全指标按照SSUT分类法重新归类,并结合SVM对样本数据集进行训练,可将评估模型分类准确率从67.5%提升到82.92%,即提高了15.42%,由此可以验证基于SVM的SSUT态势评估模型的有效性和准确性.

表 2 实验结果对比

	直接取 14 个 指标评估	基于 SSUT 分类法的评估
样本总数/个	240	240
正样本数目/个	120	120
负样本数目/个	120	120
分类正确数目/个	162	199
分类准确率/%	67.50	82.92

图 4、图 5 为有效性对比试验结果的坐标图形表示,从图中可以直观地看出本文提出的基于 SVM 的 SSUT 网络安全态势评估方法能够有效提高分类正确数目及分类准确率。

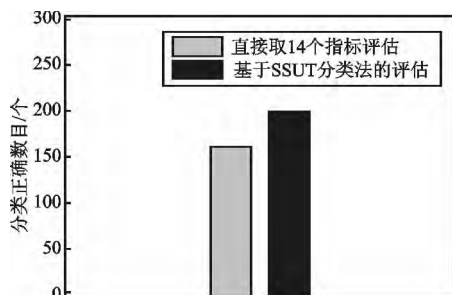


图 4 有效性实验验证结果对比图 1

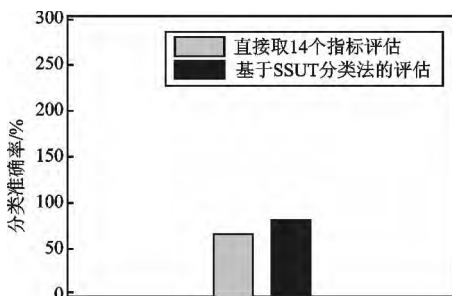


图 5 有效性实验验证结果对比图 2

基于 SVM 的 SSUT 网络安全态势评估模型能够取得良好实验结果的关键在于采用 SSUT 分类法对指标体系进行重新归类,重新归类的 SSUT 指标体系比普通指标体系更加合理有效。

4.2 评估模型扩展性验证与分析

为了验证 SSUT 态势感知模型的可扩展性,在实验环境和相关函数参数不发生变化的前提下,分别对 SSUT 分类指标体系和未使用 SSUT 分类的指标体系各扩展一个指标“子网内关键设备平均存活时间”,SSUT 分类法将其归为外部安全指标,当增加一个指标时,基于 SSUT 分类指标体系只需要修改模型的外部安全指标的其中一个因素即可,而未使用 SSUT 分类的指标体系需要对整个指标体

系进行调整,实验对比结果如表 3 所示。

表 3 扩展性实验结果对比

	直接取 15 个指标评估	基于 SSUT 分类法的评估
样本总数/个	240	240
正样本数目/个	120	120
负样本数目/个	120	120
分类正确数目/个	155	195
分类准确率/%	64.58	81.25

从实验结果可以看出,基于 SSUT 分类指标体系的分类准确率比未使用 SSUT 分类的指标体系的分类准确率高出 16.67% 之多,由此验证了 SSUT 评估模型具有良好的可扩展性。图 6、图 7 所示为扩展性验证实验结果的坐标图形表示,同样也可以明显看出基于 SSUT 指标体系的分类方法能够有效提高分类正确数目及分类准确率。

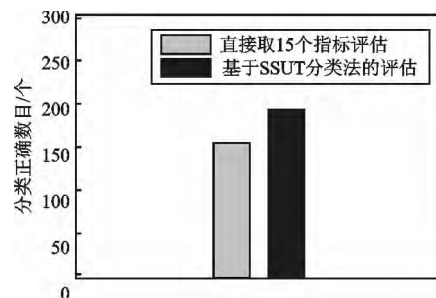


图 6 扩展性实验验证结果对比图 1

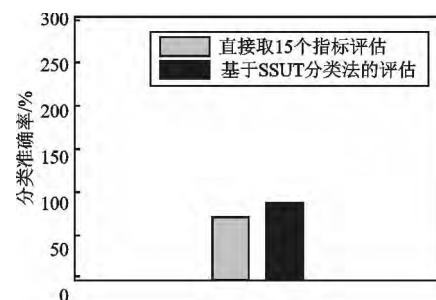


图 7 扩展性实验验证结果对比图 2

4.3 实验小结

基于 SVM 的 SSUT 网络安全态势评估模型通过上述两个实验验证了基于 SSUT 指标体系的网络安全评估模型的有效性和可扩展性。从实验结果可以看出,在同等条件下,基于 SSUT 指标体系的态势评估模型比未使用 SSUT 分类指标的普通模型分类准确率提高了近 15.4%~16.67%。

类似的,对其他多种不同监测环境下的个性化网络数据也可做相应处理,将它们对应的三维向量

作为测试数据集运用到该 SSUT 分类后的安全态势评估训练模型中,通过模型的不斷自我学习即可得到态势评估的结果,从而告知网络管理员对标记为-1的不安全网络状态做出相应处理.可见,本文提出的支持扩展指标体系的 SSUT 网络安全态势评估模型对于提高网络安全性和辅助决策能力具有很好的指导作用.

5 结束语

从改进指标分类的角度出发,提出网络安全指标 SSUT 分类方法,建立支持扩展指标体系的 SSUT 网络安全态势评估模型,并结合 SVM 分类方法,将所选取相关指标元素构成的多维向量进行分类和态势评估,从而得到个性化用户对于网络安全态势评估的最佳结果.新模型与以往传统安全指标为基础的态势评估模型相比,在模型的有效性、准确性及扩展性方面有了很大改进;通过加入用户类型指标 User-Type 满足了不同网络用户的个性化网络安全需求,而指标影响因子的引入则对模型的自由度有了很大的提高,实验结果也验证了安全态势评估模型的优越性.

参考文献:

- [1] 龚正虎,卓营.网络态势感知研究[J].软件学报,2010,21(7):1605-1619.
- [2] Zhang Haoliang, Shi Jinqiao, Chen Xiaojun. A multi-level analysis framework in network security situation awareness [J]. Procedia Computer Science, 2013 (17): 530-536.
- [3] Cheng Xiaorong, Lang Su, Li Mingxuan. Research of network security situational assessment quantization based on mobile agent [J]. Physics Procedia, 2012 (25): 1701-1707.
- [4] 吴志军,杨义先.信息安全保障评价指标体系的研究[J].计算机科学,2010,37(7):7-10.
- [5] 丁世飞,齐丙娟,谭红艳.支持向量机理论与算法研究综述[J].电子科技大学学报,2011,40(1):2-10.
- [6] 梁海军.人工蜂群优化支持向量机算法在网络安全中的应用[J].微电子学与计算机,2013,30(2):95-98.

作者简介:

李纪真 男,(1986-),博士研究生.研究方向为计算机网络安全. E-mail:lijizhen1986@126.com.

孟相如 男,(1963-),教授,博士生导师.研究方向为宽带通信网络技术.

(上接第14页)

表1 动态窗口和固定窗口的比较

采用技术	响应速度	平均误差	收敛时间
固定窗口	无	0.5	15个观测周期
动态窗口	1~2个观测周期	<0.1	<5个观测周期

4 结束语

本文针对传感器网络中多证据的体系,设计了一种基于动态证据窗口的证据采集机制.仿真结果表明,对于三类典型的波动情形,动态窗口技术在线性复杂度条件下,其响应幅度、准确率、误差收敛速度上均优于传统固定采集窗口.本文设计的系统可代替传统的固定窗口技术,作为证据理论体系的前端采集模块.广泛适用于各类无线传感器网络.

参考文献:

- [1] 陆三兰,程铭东.基于D-S证据理论的组合数据融合算法[J].微电子学与计算机,2013,30(1):95-98.
- [2] 邓建春.可信网络的信任模型研究[D].成都:电子科技大学,2013.
- [3] 谭运宝,钟诚,张尊国.一种基于邻居合作检测的移动Ad Hoc网络信任模型[J].微电子学与计算机,2008,25(10):227-230.

作者简介:

肖夏 男,(1989-),硕士研究生.研究方向为无线传感器网络. E-mail:xiaoxia@ime.ac.cn.

陈岚 女,(1968-),博士,研究员,博士生导师.研究方向为超深亚微米芯片设计方法学、计算机体系结构及物联网关键技术.

李莹 女,(1982-),博士,副研究员.研究方向为物联网与嵌入式系统设计.