doi: 10.3969/j.issn.1003-3114.2018.01.07
引用格式: 汤汉伊,孙其博,周傲,等.情境感知的网络用户可信评估模型[J].无线电通信技术,2018,44(1):34-38.
[TANG Hanyi,SUN Qibo,ZHOU Ao,et al.A Context-aware Network User Trusted Evaluation Model[J].Radio Communications Technology,2018,44(1):34-38.]

情境感知的网络用户可信评估模型

汤汉伊,孙其博,周　傲,李静林
(北京邮电大学 网络与交换技术国家重点实验室,北京 100876)

摘　要: 互联网已经成为人们生活不可或缺的一部分,但是网络安全问题仍然影响着互联网发展,可信评估逐渐成为保障网络安全的核心,而网络用户又是可信评估的重点评估对象。当前网络可信评估模型没有充分考虑用户所处的情境以及用户的欺诈行为,影响网络用户可信评估的精确性,导致恶意用户的漏判和误判。针对该问题,提出了一种情境感知的网络用户可信评估模型(CAMETNU)。该模型通过对用户访问时所处的情境计算恶意行为的惩罚力度,而又依据用户累计恶意行为加大惩罚力度。实验结果证明了所述方法的有效性。

关键词: 可信评估;情境感知;用户行为;信任值
中图分类号: TN915.08　　**文献标志码:** A　　**文章编号:** 1003-3114(2018)01-34-5

A Context-aware Network User Trusted Evaluation Model

TANG Hanyi,SUN Qibo,ZHOU Ao,LI Jinglin
(State Key Laboratory of Networking and Switching Technology,Beijing University of Posts and Telecommunications,Beijing 100876,China)

Abstract: The Internet has become an indispensable part of people's life,but the network security problem still affects the development of the Internet.Trusted evaluation gradually becomes the core of network security,and network users are the important target of evaluation in trusted evaluation.The current network trusted evaluation model does not give full consideration to users' situation and their fraud behavior,which affects the accuracy of network user trusted evaluation,leading to the false judgment and misjudgment of malicious users.To solve this problem,a context-aware network user trusted evaluation model (CAMETNU) is proposed.The model calculates the punishment of malicious behavior through the situation the user is in,and increases the punishment according to the accumulated malicious behaviors of the user.Experimental results demonstrate the effectiveness of the proposed method.

Key words: trusted evaluation;context awareness;user behavior;trust value

0　引言

近些年来,网络的可信性研究已经逐渐成为了又一个研究热点,研究人员提出了多种网络可信评估模型[1-6]。随着信息通信技术的发展和演进,人们对网络的依赖性与日俱增,网络安全的重要性日益明显,网络信息安全的内容不断扩展,从最早的信息保密性到信息完整性、可靠性和不可否认性,进一步发展到网络服务的安全性。现如今由防火墙、入侵检测、防病毒系统组成的安全防范技术不断推陈出新,但网络恶意攻击的破坏性却没有呈下降趋势。究其原因是因为信息安全最主要的攻击者来自于恶意用户本身,所以解决信息安全问题要抓住本质,从解决用户的可信性为主。就如美国国家工程院院士David Patterson教授所说"以往的研究以追求高效为目标,而如今计算机系统需要建立高可信的网络服务,可信性必须是可以度量和检验的性能。"因此可信网络是一种解决网络安全的新方法。

基于用户行为的可信性评估研究对解决可信网络的评估具有深远的影响。当前存在一些基于用户行为可信性的模型和方法用于可信网络评估,如文献[7-10]中所阐述的,但是这些方法依然存在一些问题。如信息源是否可信,大部分现有的模型和方法仅仅基于用户之间的交流反馈,而没有考虑对用

收稿日期: 2017-07-27
基金项目: 国家自然科学基金项目(61571066)

户网络行为进行检测;还有一部分现有模型和方法没有充分考虑到用户本身是否使用了一些欺诈行为发出错误的行为暗示使得模型预测出现震荡现象,难以保证准确性。

1 相关工作

一些研究者对基于用户行为的可信网络评估做出了研究。在文献[11]中作者针对云计算服务提供商与云用户之间的信任危机,从中提出了一种在云计算环境下信任评估的方法,从而建立了一套从云服务的用户角度出发的云计算反馈可信性评估模型。作者通过引入可信评估因子,使得该模型对恶意用户行为更加敏感。在文献[12]中作者提出了一种基于用户行为证据的双滑动窗口的用户可信性评估,通过调整滑动窗口的属性来确保用户行为信任是可信的。最后作者用客观数据和理论分析得到了评估系统有效性的证明。该文章重点阐述了信任评估不仅仅可以针对服务,而且可以针对用户。在文献[13]中作者提出了一种评估用户间关系的度量机制,整合了用户间已确立的信任关系网络,从而综合地对用户间的信任关系做出预测,得到了更加准确的信任关系预测模型。在文献[14]中作者提出了一套针对P2P网络的可信网络评估模型,其中借鉴了人际网络中的信任关系得出了一套解决方案,从而建立一种基于信誉的可以面向全局的信任模型。

通过对前人研究的对比发现,之前的研究一般集中于解决基于用户的可信评估,或者基于反馈的可信评估,没有充分考虑两者之间的情境信息,本文提出了一种基于情境的方法对这一情况做出了很大的改进,从而使得可信评估的准确性得到了很大的提高。并且之前的研究没有充分考虑恶意用户的反复欺诈行为,使得系统具有震荡性,本文提出了一种基于用户行为反馈的算法,使得用户可信评估可以基于用户的当前状态行为和历史行为做出判断,并执行不同的惩罚力度,从而解决了可信评估中的信任震荡问题,提高了可信网络评估的鲁棒性。

2 情境感知的网络用户可信评估算法

2.1 系统框架

图1展示了基于情境感知的网络用户可信评估模型的系统框架图。本系统主要包含3个部分,分别是用户行为及用户情境收集模块、数据存储模块以及用户可信值计算模块,最后得到关于用户行为的可信评估值。用户行为及用户情境收集模块包括行为数据采集、情境数据采集功能,并且包含了协议分析提供者。数据存储模块包含用户历史行为数据库、行为匹配数据库、管理存储行为数据及用户信任值的模块,在图中表示整体概括在了行为数据库中。用户可信值计算模块根据用户历史行为数据以及情境信息统计分析得到的数据进行可信值的计算,该模块包含了用户信任归一化,是否为恶意行为判断及惩罚度阈值超标判断,提升或者降低用户信任值,最后做出可信值的评估与计算。

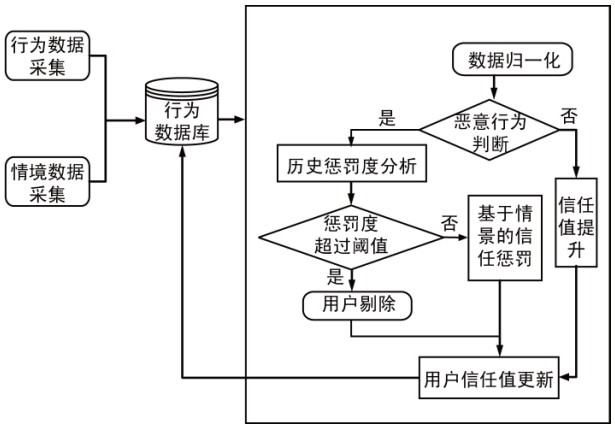

图1 情境感知的网络用户可信评估系统框架图

行为及用户情境收集模块使用网络嗅探技术对用户在网络中的行为进行了分析。本模块主要负责对可信网络评估中所针对的网络进行数据获取,并且将得到的数据存储在缓存队列或者可持久性存储设备中供下一步分析。缓存队列主要作用是使得本系统可以实时处理可信网络评估过程中用户的可信问题,可持久性存储设备主要用于应对在高并发情况中网络丢包率显著提升时,为了确保可信网络评估的准确性不会受太大影响,所以转存到存储空间更大存储更持久的外部设备,以备分析使用。

在数据存储模块中使用了模式匹配技术和数据分析技术对用户的历史可信行为给出相关数据,以及使用统计分析技术得到用户本次交互行为与行为数据库中的何种行为相似,并且给出了相关的情境

分析。

用户可信值计算模块是本系统的核心模块，该模块根据之前的收集、统计、分析、匹配得到的结果去判定本次用户的行为是否为恶意行为，如果不是恶意行为则增加用户的信任值，如果是恶意行为则根据相应的情境与行为降低用户的信任值，最终将用户的可信值更新到行为数据库中。

2.2 评估算法

① 可信值表示为(T,E,H)：其中T表示用户的信任值，随着用户交互次数的不断增加，系统根据每次用户的行为是否被判定为恶意行为或者正常交互行为对T值进行增加或者降低操作。并且对于恶意行为结合了当下的情境信息，给出了不同的惩罚力度。E、H表示用户当前的情境，分别代表了用户是否为内网用户，用户的可信等级评价。如果用户为内网用户算法对一些恶意行为的惩罚相应降低。用户当前的信任等级H对用户信任值的计算做出影响，H主要来源于用户历史行为的评价。算法使用$(C1,C2)$表示用户历史恶意行为次数和恶意行为严重性，通过对用户历史恶意行为次数的统计及恶意行为的严重性统计对用户的可信性进行了分级，主要分为5个等级，如表1所示。交互行为次数C，最终使用分段函数f得到用户的信任等级H，关系确定如下：

$$H = f(1 - (C1 + C2 * C1)/(C + C2 * C)) 。 \quad (1)$$

表1 用户信任等级

等级	描述
-1	不可信用户
0	初始化用户
1	用户可信程度较低
2	用户可信程度较高
3	用户可信程度很高

② 信任初始化：在系统最开始工作的阶段，用户之间没有过任何交互，所以对用户可信等级H确定为等级0，即用户的可信等级为初始化等级。之后随着用户可信交互次数的增多，用户可信等级逐渐提升。

③ 首先，算法通过评估用户交互行为做出评价，得到相应的可信上升值与可信下降值。当用户交互的次数逐渐增多，用户历史行为数据库数据充实，系统对用户的可信性会做出越来越准确的评价，因为系统对用户的行为越来越了解。如果用户的行为被检测出来是恶意行为，那么系统采取了一种依据用户历史行为加大惩罚力度的模型对用户的可信值进行下降操作。这种依据用户历史行为的方法可以有效避免系统中存在的恶意用户伪装成可信用户的行为。假如恶意用户通过多次可信行为去积累用户历史行为数据库中的可信数据时会造成系统误认为恶意用户可信，当积累够一定信誉值后，恶意用户对网络发起多次攻击后又开始积累信任值，这会对一般的模型造成震荡效果。而且算法考虑了用户当前的情境问题，如果存在内网用户的检查性访问，系统不会对恶意行为做出较为宽松的处理。最后算法还考虑了用户行为状态的影响。

当用户行为被判定为恶意行为或者交互失败时，用户的可信值将会根据如下公式下降：

$$\Delta T = Bb * Vl * e^{Hv} * Gb , \quad (2)$$

$$T = T - \Delta T 。 \quad (3)$$

公式参数说明：

ΔT表示每次交互之后对信任值的降低值，是模型调整主要依赖的一个值。

Bb表示的是恶意行为惩罚因子，通过调整Bb可以细化调整对恶意行为的惩罚力度。

Gb是算法中的一个惩罚项，根据本次算法下降是因为恶意行为还是交互失败，得到不同的惩罚因子。

Hv是算法中很重要的一个参数，表示用户等级H所对应的惩罚参数，这个参数使得算法可以实现加大惩罚力度的过程，保证可信评估过程不会出现震荡现象。

Vl是算法中另一个重要的参数，它依据的是在特定情境下用户恶意行为的评级，目前对恶意行为的分为6个等级，这些恶意行为显示如表2所示。

表2的恶意评级来自于引用文献[7]，并加入了情境信息。另外，对于惩罚度超过一定阈值的恶意行为，系统将会把该用户记录入黑名单，禁止该用

户对网络的访问行为，直到管理员进行用户资格审核通过，才可重新访问网络。

表 2　恶意行为评级表

恶意等级	事件描述	样例	安全情境 Vl	非安全情境 Vl
1	监测主机是否存活	Ping 命令	1	1
2	收集系统信息或者打开服务	Tcp 端口浏览	1	3
3	密码嗅探攻击	ftp 密码嗅探	2	5
4	攻击远程缓冲区溢出失败	Unicode 编码错误攻击失败	2	7
5	攻击远程缓冲区溢出成功	Unicode 编码错误攻击成功	3	9
6	系统崩溃	系统权限窃取	3	10

当用户行为被判定为可信行为即正常行为时，用户的可信值将会根据如下公式上升：

$$\Delta T = Bg^{*}\ Hv^{*}\ Gg, \tag{4}$$

$$T = T + \Delta T。 \tag{5}$$

ΔT 表示每次交互之后对信任值的提升值，是模型调整主要依赖的一个值。

Gg 是算法中的一个奖励因子，根据本次算法下降是因为恶意行为还是交互失败得到不同的奖励因子。

Bg 表示可信行为的奖励因子，通过调整 Bg 可以细化调整对可信行为的奖励力度。

Hv 是算法中很重要的一个参数，表示用户等级 H 所对应的奖励参数，这个参数使得算法可以实现对用户历史行为的惩罚力度加大，保证可信评估过程不会出现震荡现象。

最终通过用户间多次交互，不断更新用户的可信值，对网络中的用户可信性做出了评价，并且记录这些信任值。

3　实验与分析

为了对模型进行实验分析，先设置实验参数。设置公式中的参数如表 3 所示。并且设置加入恶意行为用户黑名单的阈值，如本次惩罚值超过本次惩罚之前用户可信值的 80%，则将用户加入黑名单。

表 3　模型参数设置

H	f	Bg	Bb	Gg	Gb
−1	≤0.2	0.25	1	0.1/0.3	0.1/0.3
0	≤0.4	0.35	1	0.1/0.3	0.1/0.3
1	≤0.6	0.5	0.85	0.1/0.3	0.1/0.3
2	≤0.8	0.7	0.5	0.1/0.3	0.1/0.3
3	≤0.9	1	0.2	0.1/0.3	0.1/0.3

下面的实验将使用表 3 中的参数，为了测试公式参数和信任值之间的相关性，在这个章节中设计了如下的几组实验。在实验 1 中假设用户 U1、U2、U3、U4、U5、U6 的初始信任值为 10，然后用户 U1、U2、U3、U4、U5、U6 分别执行了一次恶意等级为 1、2、3、4、5、6 的恶意行为，实验结果如图 2 所示。在实验 2 中假设用户 U1、U2、U3、U4、U5、U6 的初始信任值为 30，然后让用户 U1、U2、U3、U4、U5、U6 在当前分别执行第 2 次恶意等级为 1、2、3、4、5、6 的恶意行为，并分别记录实验结果如图 2 所示。从两组实验中可以很清晰地看出当用户执行的恶意行为越严重时，模型的惩罚力度越大，即用户的信任值下降越快，并且当用户达到恶意等级为 6 的恶意行为时出现了拐点，用户的惩罚值将超过用户黑名单的阈值，该用户将被加入黑名单，可以看到恶意等级为 6 的行为已经涉及到系统权限窃取。因为系统对用户的安全情境有诊断机制，所以一些网络管理员的管理操作不会产生很大的惩罚，使得网络管理员被加入黑名单，所以模型很好地保证了可信网络评估的准确性。

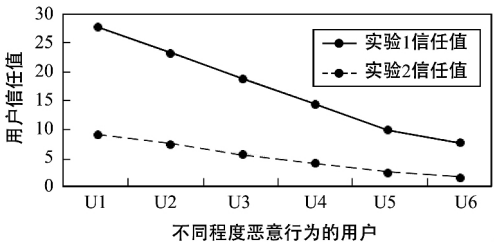

图 2　不同初始条件下信任值变化图

最后为了说明模型对于用户的欺诈行为有防范作用，在实验 3 中，设计了如下的规则。首先假设用户 U1、U2 的初始化信任值为 100，然后分别让用户 U1、U2 执行一次恶意行为，然后再执行一次正常交互行为，如此反复 3 次之后，实验结果如图 3 所示。在

图中可以清晰地看到本文所提出的模型对于用户的欺诈行为有很好的防范作用，因为模型充分利用了用户历史行为的数据，并且结合了用户的相关情境。在基于情境的用户行为监测可信评估模型当中，用户的情境与历史行为被考虑在了可信值的计算过程当中，使得基于情境的用户行为监测可信评估模型拥有了更好的避免用户欺诈行为的能力，以及对于可信用户有避免误判的机制，即基于用户所处的情境。从图中可以看出当用户交替执行恶意和正常行为时，一般模型会对用户的可信值判定在可信附近，这就给了用户欺骗可信评估系统的机会，使得可信评估系统出现信任震荡效果。但是基于情境的用户可信行为评估模型却能很好地预测用户信任值。

通过上述几组实验，看到了基于情境的用户行为监测可信评估模型具有很好的可信评估能力，也具有很好的鲁棒性。

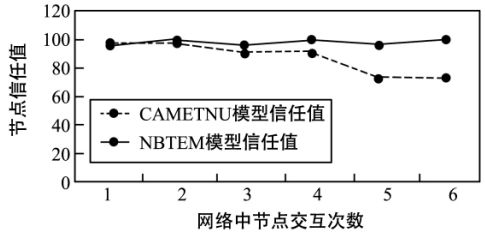

图 3　信任值对比图

4　结束语

基于情境的用户行为可信网络评估是一种有广泛作用的模型。根据应用场景的不同，对相应的情境做出对应的调整，模型将能在不同的应用场合下，给可信网络的评估结果可信度带来很大的提高。因为模型不仅考虑了基本的用户行为检测，而且融入了用户行为反欺诈功能和用户情境。通过实验和分析，证明了基于情境感知的网络用户可信评估算法确实是有效、鲁棒以及可靠的。下一步工作主要集中在如何将其运用在不同业务场景下，结合不同的情境信息进行可信网络评估。

参 考 文 献

[1] 周德海.基于状态的网络行为可信性评估 [J].计算机安全，2014(05)：2-7，11.

[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] 夏石莹.可信网络的可信认证与评估研究 [D].衡阳：南华大学，2011.

[4] 张晓琴，陈蜀宇，常光辉，等.可信网络中的信任评估模型 [C]//中国计算机学会容错计算专业委员会.第十四届全国容错计算学术会议(CFTC'2011)论文集.中国计算机学会容错计算专业委员会，2011：6.

[5] 李向前，宋昆.高可信网络信任度评估模型的研究与发展 [J].山东农业大学学报(自然科学版)，2006(02)：243-247.

[6] 蒋泽.可信网络中用户行为可信评估的研究 [D].重庆：重庆大学，2011.

[7] Sun Y L，Han Z，Yu W，et al. A Trust Evaluation Framework in Distributed Networks：Vulnerability Analysis and Defense Against Attacks [J].Proceedings of IEEE INFOCOM，2006：1-13.

[8] ZHANG Shi bin，HE Da ke，SHENG Zhi wei. Research and Development of Trust Management Model [J]. Application Research of Computers，2006，23(7)：18-22.

[9] Hongxingshan X U. Research and Implementation of a Level-based Network Intrusion Detection System [J]. Computer Engineering，2002，28(10)：69-71.

[10] 郭崇现.Ad Hoc 网络中节点可信评估算法研究与设计 [D].济南：山东大学，2015.

[11] 王颖，彭新光，边婧.云计算下信任反馈可信性评估模型研究 [J].计算机工程与设计，2014，35(6)：1906-1910.

[12] 田立勤，林闯.基于双滑动窗口的用户行为信任评估机制 [J].清华大学学报：自然科学版，2010(5)：763-767.

[13] 蔡国永，王丽媛，吕瑞.基于用户评论的信任预测方法研究 [J].计算机应用研究，2016，33(4)：1019-1023.

[14] 胡建理，吴泉源，周斌.一种基于反馈可信度的分布式 P2P 信任模型 [J].软件学报，2009，20(10)：2885-2898.

作者简介：

汤汉伊(1992—)，男，硕士研究生，主要研究方向：计算机科学与技术、网络安全、可信计算；

孙其博(1975—)，男，博士，副教授，主要研究方向：计算机科学与技术、下一代网络与网络智能化、服务计算与服务安全技术；

周　傲(1987—)，女，博士，讲师，主要研究方向：计算机科学与技术、网络安全。

李静林(1975—)，男，博士，副教授，主要研究方向：计算机应用、移动互联网、物联网、车联网等融合网络服务与安全技术。