

文章编号:1001-9081(2016)09-2447-05

doi:10.11772/j.issn.1001-9081.2016.09.2447

基于聚类分析的可信网络管理模型

谢洪安^{1*}, 李栋², 苏旸¹, 杨凯¹

(1. 武警部队网络与信息安全保密重点实验室, 西安 710086; 2. 武警工程大学 电子技术系, 西安 710086)

(*通信作者电子邮箱 15529332695@163.com)

摘要:针对可信网络中动态信任模型对终端用户行为信任评估有效性问题,提出一种新的基于聚类分析的可信网络管理模型。该模型在传统信任模型的基础上引入聚类分析方法,从行为预期的角度研究用户的行为信任。通过对用户的历史行为数据进行聚类分析以构建行为预期,并利用行为预期评估用户行为,最后以信任评估结果为依据实现对网络中的用户的管理。实验表明该模型可以对长期接入的正常用户产生稳定的信任评估结果,同时迅速发现并隔离恶意用户,对可信用户与不可信用户有较高的区分度,与传统的信任模型相比具有更高的准确度及效率,达到了提高网络可靠性的目的。

关键词:可信网络;聚类分析;信任评估;网络管理;信任模型

中图分类号: TP309 **文献标志码:**A

Trusted network management model based on clustering analysis

XIE Hong'an^{1*}, LI Dong², SU Yang¹, YANG Kai¹

(1. Key Laboratory of Network and Information Security, Chinese People's Armed Police Force, Xi'an Shaanxi 710086, China;

2. Department of Electronic Technology, Engineering University of Chinese People's Armed Police Force, Xi'an Shaanxi 710086, China)

Abstract: To improve the availability of dynamic trust model in trusted network, a trusted network management model based on clustering analysis was built. Behavior expectations were used to describe the trust of user behavior by introducing clustering analysis to the traditional trust model. Clustering analysis of the user's historical data was used to build behavior expectation model, which was used to evaluate user's behaviors. Finally the trust evaluation results were utilized to realize the network user management. The experimental results show that the proposed model can generate trust evaluation results firmly, detect and isolate the malicious users rapidly, it has better accuracy and efficiency than traditional model, basically improving the network reliability.

Key words: trusted network; clustering analysis; trust evaluation; network management; trust model

0 引言

随着用户对网络安全需求的提升,提高网络环境的可信性成为一种迫切需求。因为信任具有不确定性、不对称性、部分传递性、异步性、上下文独立性等一系列复杂的动态属性^[1],又由于网络结构本身的复杂性,导致构建可信网络的困难性^[2],所以可信计算组织(Trusted Computing Group, TCG)提出了可信网络连接框架(Trusted Network Connection TNC)建立可信网络连接^[3]。TNC通过建立一系列的标准接口(IF-PEP、IF-T等)定义了一个公开标准,对将要接入可信网络的终端用户进行身份认证及完整性度量,验证其安全策略,以确定终端是否可以被允许访问网络,确保任何访问网络的终端具有符合安全策略的安全配置^[4]。TNC仅解决了终端用户的可信接入问题,但对接入后的终端管理存在不足,部分学者提出建立信任模型来解决这个问题,建立描述网络和用户行为的可信模型,对系统整体的可信性进行评估,有效改善了TNC的局限性。

建立动态的信任模型是可信网络的一个重要问题。动态

模型主要考虑用户的行为信任。动态的信任模型就是动态地收集相关的主观因素和客观证据的变化,以一种即时的方式实现对网络信任的度量、管理和决策^[5]。目前许多学者针对不同网络环境下的信任模型展开研究,比较典型的有:基于模糊理论中贝叶斯理论^[6]的信任模型,主要利用贝叶斯公式计算条件概率来对信任进行描述;基于 DS(Dempster/Shafer)证据理论的信任模型^[7-8],主要考虑信任的主观特性以评估目标实体的可信性、不可信性及不确定性的方法描述信任;基于行为状态关联的方法^[9];基于稳定组的方法^[10]等。但以上模型适用领域有限,且仍具有一定局限性。如基于行为状态关联的模型^[9]从时间以及上下文等角度评估用户信任,注重实体交互时的信任评价以及信任评估的不确定性与随机性。但传统的基于模糊逻辑建模的方法对终端用户信任描述仍不够合理全面,信任评估的可用性与准确性不足。

为解决上述问题,真实地反映用户信任,本文提出了一种新的基于聚类分析(Clustering Analysis, CA)的可信网络管理模型。模型在传统行为状态的信任模型基础上引入聚类分析方法评估用户信任,通过对终端用户的历史行为分析,发现用

收稿日期:2016-02-29;修回日期:2016-03-30。

基金项目:国家自然科学基金资助项目(61402530);陕西省自然科学基金资助项目(2014JQ8301)。

作者简介:谢洪安(1992—),男,江西南昌人,硕士研究生,主要研究方向:网络安全、可信计算; 李栋(1993—),男,四川绵阳人,硕士研究生,主要研究方向:信息技术; 苏旸(1975—),男,陕西西安人,教授,博士,CCF会员,主要研究方向:网络安全; 杨凯(1983—),男,山东莱芜人,讲师,博士,CCF会员,主要研究方向:网络安全。

户的“性格特点”^[5],即行为预期,通过判断用户行为是否符合预期来决定用户的信任度,最后依据信任度管理网络中的用户。本模型强调行为信任的预期性,将用户行为的各项属性加入算法,并综合考虑正常与异常行为间的差异、当前行为与历史行为的差异作为计算信任的依据,能更有效地反映实体信任。实验表明,模型能够准确评估用户信任,快速鉴别恶意用户,对恶意行为响应迅速,能够有效依据安全策略管理网络,提高网络可信性。

1 基于聚类分析的网络管理模型

1.1 模型设计

传统的信任模型注重在网络中各实体相互间的信任评价,并以之作为可信评估的依据,但对终端用户行为自身的信任评估却存在不足。当前不同组织对可信的定义各有不同,本文借鉴 TCG^[2]组织对可信的定义。

定义 1 一个实体是可信的,则这个实体行为总是符合预期的行为方式。

模型的设计思路是在状态行为关联的可信模型基础上,基于以上信任的定义设计的。模型的设计思路是:1)利用行为状态关联模型对用户行为进行描述,使模型能够正确描述用户行为特点;2)选取合适的聚类方法从用户的行为特点以及上下文中提取出用户的行为预期;3)对当前用户的行为进行评价,即用户的信任度应是其行为与对应实体的预期的行为相符的程度;4)考虑到信任随时间变化而衰减的特性,引入时间窗口机制实现信任的更新。为方便说明,将网络管理模型抽象成如图 1 所示。

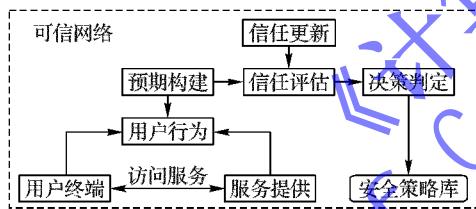


图 1 网络管理模型结构

模型主要流程包括预期构建、信任评估、信任更新以及决策判定。

1.2 预期构建

本文讨论的行为预期指的是通过分析用户已有的历史行为证据而对用户的未来行为的预测,因此本文使用知识发现(Knowledge Discovery in Database, KDD)中聚类分析的方法构建行为预期。知识发现即从已有的数据中找出特定知识的数据挖掘技术^[11]。数据挖掘是一个高级的数据处理过程,可以从大量的、不完全的、模糊的数据集中提取出可被理解的知识。其中基于密度的算法可以根据数据集中元素的密度差异对数据集进行聚类分析,能够快速分离高密度行为集合,提取行为预期,作为用户行为信任的评价指标以及网络管理的依据。

为了构建行为预期,采用了聚类分析方法对用户行为集合 B ,进行计算,并提取相关知识。聚类分析(CA)又称群分析^[12],是根据“物以类聚”的方法对样品或指标进行分类的一种多元统计分析方法。经过聚类得到的簇,簇中的元素会具有很大的相似性,因此选取聚类分析方法构建用户行为预期。DBSCAN(Density-Based Spatial Clustering of Applications

with Noise)是一种基于密度的聚类算法,此算法非常适合大量数据情况下的聚类分析,并且已经被广泛运用于各个领域。基于密度的聚类可以根据密度的差异分离样本中的数据,能够较好地构建用户行为预期。

本文对 DBSCAN 算法进行改进,使其既能够快速分离出高密度的簇类,又能够分离用户行为中具有较大偏离的“异类”。将这种“异类”作为用户行为不可信的参考,能提高用户信任评估的可靠性和稳定性。

在预期构建之前需要对用户行为进行定义,借鉴文献[9]在行为状态关联模型中对用户行为的定义,本文为了完备描述用户行为将用户行为定义如下:

定义 2 用户行为。

$$B = \{b_i(O, S, A, R, F, \dots) | b_1, b_2, \dots, b_n\}$$

其中:

1) 实体集合 $O^T = \{o_1, o_2, \dots, o_n\}$;

2) 实体状态集 $S^T = \{s_1, s_2, \dots, s_n\}$;

3) 实体动作集 $A^T = \{a_1, a_2, \dots, a_n\}$;

4) 实体行为状态信任熵 $R_{ij} = H(s_i, a_j)$;

5) 函数集 F ,其中,状态转移函数 $F_a(s_i \times a_i) \rightarrow s_k$ 表示实体状态 s_i 在动作 a_i 作用下转移到新的状态 s_k ,动作序列函数 $F_s(s_i \times A) \rightarrow s_j$ 表示实体在运行一个动作序列后的状态变迁。

定义 3 算法参数 $\varepsilon, MinPts, MinDs$ 。其中: ε 表示聚类半径, $MinPts$ 表示密度阈值, $MinDs$ 表示最小偏移距离。

算法 1 对抽象的用户行为进行处理,在行为状态理论^[9]基础上先计算出单个行为的信任熵 R ,之后通过信任熵大小,及其他参数定义用户行为距离,并将用户行为证据输入算法,实现行为预期的提取。在算法中使用到的各个参数: B 为分析的数据对象即行为证据集合;半径 ε 以及密度阈值 $MinPts$ 是簇的分类标准,通过这两个参数对簇类进行选取; N, K 为算法中所使用到的临时变量。算法的输出结果为聚类得到的簇 C ,以及离群点集合 P 。算法 1 使用聚类的方法对用户行为数据集合进行分析,具体过程就是从集合中任意一点开始,使用函数找寻其全部 ε 邻近点,如果某个点的 ε 邻近点的个数大于事先设定的密度阈值,则认为这个点包括其 ε 邻近点都属于一个簇。算法 1 流程如下。

算法 1 DBSCAN($B, \varepsilon, MinPts, MinDs$)

```

1) begin
2)   Init_Cluster( $C$ ); // 对簇进行初始化
3)   for each unvisited point  $p$  in  $B$ 
4)     Mark  $p$  as visited; // 对任一个点进行访问,并标记
5)      $N = \text{get\_Neighbours}(p, \varepsilon)$ ; // 获取全部邻近点
6)      $K = \text{get\_Neighbours}(p, MinDs)$ ;
7)     if  $K! = 0$  then
8)       mark  $p$  as  $P$ ; // 标记点  $p$  为  $P$ 
9)     end if
10)    else
11)       $C = \text{nextcluster}$ ; // 找到一个簇,并记录
12)      Expand_Cluster( $p, N, C, \varepsilon, MinPts$ ); // 簇拓展算法
13)    end if
14)  end for
15) end // 算法结束

```

对这个簇使用簇拓展算法也就是算法 2 进行拓展。

算法 2 Expand_Cluster($p, N, C, \varepsilon, MinPts$)(簇拓展算法)。

```

1) Add p to cluster C;           // 把点 p 加入簇 C
2) for each point p' in N    // 从任意邻近点中开始拓展簇
3)   Mark p' as visited
4)   N' = get_Neighbours(p', ε);
5)   if sizeof(N') >= MinPts
6)     then N = N + N'      // 对符合要求的簇进行拓展
7)   end if
8)   if p' is not member of any cluster
9)     add p' to cluster C;
          // 若点 p 无法拓展, 则继续算法
10)  end if
11) end for
12) end                         // 算法结束

```

算法 2 对得到的簇进行拓展, 从已得到的簇中的任意一点开始拓展这个簇, 对任意一点 p , 寻找其 ϵ 邻近点, 如果发现直到没有办法找到簇中任意一点的新的邻近点时结束算法。不断重复算法 2, 直到遍历完 B 中全部的元素后结束。

可以看出, 算法对于簇的定义基于两个参数: ϵ 和 $MinPts$ 。对于任意的一点, 所有与其距离为 ϵ 的点均是 ϵ 邻近点。如果 ϵ 邻近点的数量不少于 $MinPts$, 那么这些点(包括点)都是数据集的一部分, 属于同一个簇, 算法可以对集合中的高密度部分进行提取。因此使用上述算法对用户行为证据集合进行聚类, 筛选出高密度行为簇, 以此构建行为预期。算法根据密度的区别筛选出可信的行为, 此外算法可以根据行为的偏差分离出离群点。离群点是“与数据集中其他数据有很大不同的数据”。分离离群点可以有效分离同用户常见行为差距过大的行为, 而这些行为可以作为降低用户可信度的依据。因此参数选取合适时, 使用基于密度的聚类可以快速提取出用户行为中高相似、高密度、高可信的行为数据, 同时也分离了不可信、离群、可疑的行为。

通过算法 1.2 得到了用户行为预期集合 C 以及用户可疑行为集合 P , 将 (C, P) 作为用户行为预期, 提交给信任评估者, 评估用户行为信任。

1.3 信任评估

信任评估就是验证用户实际行为集与行为预期接近程度的过程, 用户在网络中的行为与预期越接近, 则用户可信程度越高; 反之, 其可信度则越低。在实际应用中为有效管理用户信任, 需要对用户的信任度进行量化, 根据量化的结果对用户的信任分层分级管理, 对不同级别信任度的用户分配不同级别的权限, 并依据相应的安全策略进行管理。

定义 4 信任等级。

为实现基于信任的网络管理, 对实体信任进行量化并进行分级管理。信任值 T_i 越高则信任等级越高, 实体也越可信。信任等级如表 1。

表 1 信任等级

分类	信任等级 T_i	信任值	语义
恶意用户	T_1	[0.0, 0.2)	极不可信
	T_2	[0.2, 0.4)	不可信
善意用户	T_3	[0.4, 0.6)	临界可信
	T_4	[0.6, 0.8)	一般可信
	T_5	[0.8, 1.0)	可信

由定义 1 信任度计算以用户具体行为与行为预期的相符程度来表示。截取用户一段时间的行为数据集合作为当前行

为样本, 将样本集合与预期行为作比较, 考虑这两者之间的相似性。具体的评估流程如图 2 所示。

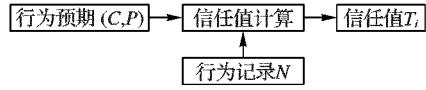


图 2 信任值计算

信任值使用 Jaccard 相似度^[13] 进行计算, Jaccard 相似度是指在两个集合中集合 A 与集合 B 交集元素在 A, B 两个集合并集中所占的比例, 称为两个集合的 Jaccard 相似系数, 使用 $J(A, B)$ 表示, 这里只要考虑用户行为记录窗口 N 中, 符合预期的行为数在行为窗口 N 中所占的比例用来表示行为的可信程度记为 $J_\theta(A, B)$, 基于预期 (C, P) 和行为窗口 N 的用户信任值可以写成:

$$T_i = J_\theta(N, C) - J_\theta(N, P) \quad (1)$$

用户行为越接近预期, 其行为的相似度越高。而行为越异常, 行为与预期相似度也越低, 因此其信任度就越低。这样通过比对用户行为预期与用户一段时间内的行为记录集合可以评估用户的信任度。但式(1)的缺陷在于用户近期所采取的超出预期的行为对信任的负面影响会被历史信任淡化。因此必须采取信任评估的惩罚机制, 模型构造了一个近期行为的小窗口 m , 并以此评估用户近期行为可信度。近期的不可信行为会快速影响整体信任。因此对式(1)进行改进后得到式(2):

$$T_i = J_\theta(N, C) - J_\theta(N, P) + J_\theta(m, C) - 1 \quad (2)$$

近期的不可信行为会迅速降低用户的信任, 同时, 信任的提高只能依靠长期的信任交往, 实现了慢升与快降^[8] 的结合, 对信任的评价更为合理。模型依据计算出的信任值 T_i 对用户进行管理, 通过查询表 1 对 T_i 进行量化并依靠事先定义的安全策略进行网络管理。

1.4 决策判定与信任更新

决策判定是根据信任评估对于用户行为的评估结果对用户进行决策管理的过程。信任更新是为了实现用户行为信任评估的时效性, 及时更新用户行为信任值, 更新信任预期, 实现对于网络用户动态管理的模块。用户行为可信的基本准则^[5] 要求信任评估必须考虑用户行为的时间特性, 即是近期用户行为的重要性与远期行为的衰减性。因此, 本文引入嵌套的滑动窗口以实现信任更新与预期重构。设窗口大小为 m , 窗口中仅保留 m 条用户行为记录, 作为用户的当前信任的评估样本。当出现新的行为记录, 将最旧的记录删除以此实现信任的更新。当记录指针 N 滑过窗口将指针重置并对用户的历史行为记录库进行一次完整更新, 并重构用户的行为预期, 保持信任值的时效性。更新机制如图 3 所示。

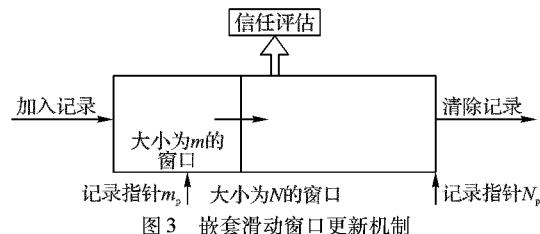
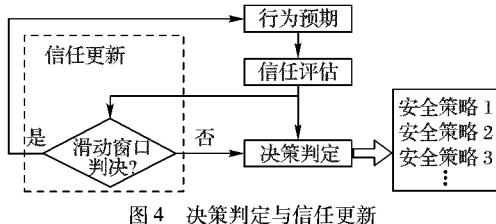


图 3 嵌套滑动窗口更新机制

决策判定实现了对可信用户与不可信用户的区分。根据评估得到的信任度决定是否将用户进行安全隔离, 同时根据可信程度分配用户服务权限, 当用户行为记录指针 m_p 滑过事先约定的窗口 m 时, 重新评估信任以进行信任更新。当指针

N_p 滑过窗口 N 时对用户行为预期进行重构,以实现对于用户信任的动态管理。模型根据评估的信任对用户进行管理,当用户信任过低时,对用户进行隔离,保证网络的整体信任度。决策判定的过程如图 4。



决策者依据信任评估的结果进行决策,对善意与恶意用户采用预先定义的不同的安全策略,对不同信任等级的善意用户依据事先定义的安全策略进行权限分配,完成基于信任的用户管理。

2 模型实现与实验分析

2.1 实验环境的搭建

搭建虚拟局域网进行实验,验证模型的功能。实验平台的网络环境如表 2 所示。

表 2 虚拟网络配置信息

虚拟机 ID	内存/MB	操作系统	IP 地址
终端 1	512	Windows XP	192.168.68.35
终端 2	512	Windows XP	192.168.68.36
终端 3	512	Ubuntu12.04	192.168.68.37
终端 4	512	Ubuntu12.04	192.168.68.38
终端 5	1224	Windows server 2003	192.168.68.254
终端 6	1224	Windows server 2003	192.168.68.1

实验将评估模型部署在网关服务器中,对用户进行数据使用定义 1 中的抽象描述表示,对用户的行为数据整理后进行聚类分析,通过聚类分析得到行为预期,并依预期进行信任评估。参数的选取如表 3 所示。

表 3 实验参数设置

类型	参数	数值
算法参数	聚类半径 ϵ	3
	密度阈值 $MinPts$	15
	最小距离 $MinDs$	7
实验参数	时间窗口 N 大小	100
	小窗口 m 大小	15

2.2 功能测试实验

功能测试主要验证模型功能,即从正常用户中区分出恶意用户的能力,以及对正常用户实施恶意行为时迅速响应的能力。在实验参数条件下,采集各实验终端的数据进行分析,对实验终端分组进行对比实验,在终端 2、4 中运行木马代码,采集各终端行为数据。采集并抽象其行为数据输入模型,连续进行 50 次实验。最终结果如图 5 所示。

图 5 中:横坐标为实验次数,纵坐标为用户信任评估值 T 。由图 5 的区分实验可以看出模型对用户的信任评估存在较好的区分度。善意与恶意的终端用户的信任值计算结果有明显差别,说明模型在网络环境中能够识别、区分恶意、不可信用户并将之安全隔离。本节功能测试表明对于不同系统用户都

能达到良好的效果。由于感染了恶意代码的用户终端的网络行为会迥异于正常的用户,模型能够通过信任评估放大这种差别达到识别恶意用户,并将恶意终端隔离的目的。

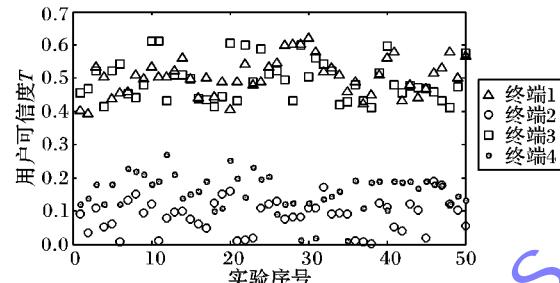


图 5 用户区分实验结果

2.3 时间特性测试

本实验分为两部分:第一部分对可信用户长期接入评估系统,考察时间对信任评估的影响;第二部分考察在善意用户接入时,突发恶意行为对模型信任评估的影响。

为验证模型对用户长期接入时的信任评估情况,定时查看模型对正常接入的用户信任评估情况,实验终端的接入时长与信任度的分布如图 6 所示。

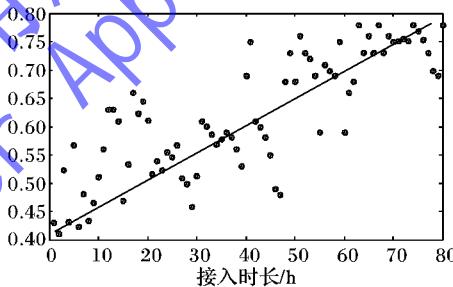


图 6 用户信任随时间的变化分布

为验证系统在实时评估中对用户恶意行为的识别能力,在终端用户正常接入时突然引入恶意行为,终端用户接入时长与信任度分布如图 7 所示。

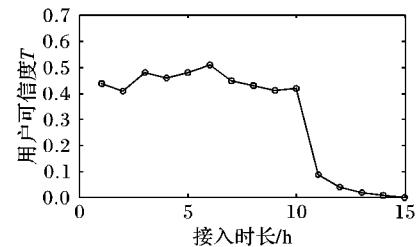


图 7 用户出现恶意行为时的信任变化

图 6、7 中:横坐标为用户接入网络中的时长,单位为 h (hour);纵坐标是对应时间点的用户信任度值,反映了数据分布趋势。实验显示:当可信用户长期接入时,用户的信任度缓慢提升,经过 80 h 的接入后系统对信任的评估趋于稳定。同时恶意行为响应实验显示:模型对用户突然出现的恶意行为可以快速反应,当用户出现恶意行为时,模型对用户的信任评估会迅速下降,用户被迅速隔离出网络。

综合 2.2 和 2.3 节的实验结果得出结论,模型可以通过信任评估从而区分正常用户与恶意用户,同时对正常的用户可以快速达到稳定的信任度,并对恶意行为反应迅速,能实现提高网络安全可信的目的。

2.4 性能测试实验

为了测试模型性能,实验选取传统信任模型中较有代表

性的基于 DS 证据的 GTET 信任模型^[8]以及基于模糊理论的 GIFT 模型^[14]计算信任值。DS 证据理论与模糊理论是比较有代表性的传统信任理论,而 GTET 和 GIFT 都是较新的较有代表性的信任模型,均能够定量地描述终端信任,实现对信任的评估,因此通过对三个信任模型进行比较实验来评估终端信任,分析本模型的性能。

实验使用三种模型同时对实验终端进行信任评估,主要对信任评估的准确性进行分析,通过对大量行为样本的信任评估,计算信任评估值的标准差进行实验分析。标准差的值越小则信任评估的准确度越高。每次实验取 10 次信任评估结果,计算结果之间的标准差,10 次实验结果如图 8 所示。

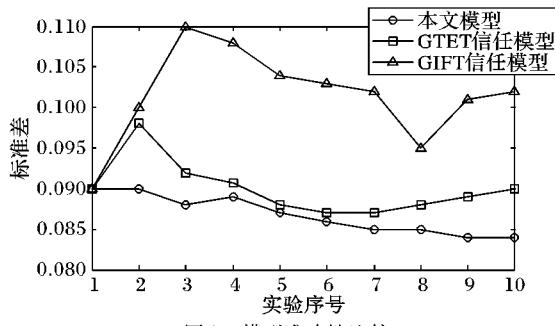


图 8 模型准确性比较

实验结果表明:三种模型对相同实体的信任评估准确度接近,其信任评估的准确度大约都在 0.1 左右,说明三种模型对于合法实体的信任评估都具有一定的准确度。其中:GIFT 通过直觉模糊理论刻画实体信任的模糊特性以确定实体的信任度,采用推荐信任的方法进行信任评估,但由于推荐信任链的不确定性,一旦出现恶意用户时偏差会被放大,对恶意策略的信誉评价容易出现较大的偏差,稳定性较差;GTET 的信任模型则是在证据理论的基础上通过图论的方法进行推理,对实体信任进行量化评估,借助实体信任证据消除模糊信任中的不确定性,准确性相对提高;而本文使用行为证据的方法,将用户的行为与状态关联起来,用行为预期的方式评估用户信任,虽然在少量样本及短期接入时与模糊理论的信任评估稳定性相比没有优势(如图 8 中实验 1),但是对长期及样本足够的用户准确度明显提升,并且其准确性随样本容量增加而增加,与基于模糊方法的模型相比具有一定的优势,适合作为长期的网络用户接入管理模型。

综上,可以得出结论,本文提出的模型完成了预期功能,对善意与恶意实体间有较高的区分度,并对行为的突变有较高的敏感度,能有效评估实体信任。对比实验结果表明,本文证明模型在信任评估的准确性上较传统模型有一定的提升。

3 结语

本文从行为预期的角度研究用户的信任,提出了一个新的基于聚类分析的网络管理模型。模型通过对用户历史行为证据的聚类分析从而发现其中的知识,找出用户固有的“性格特征”,作为行为预期来计算用户实际行为的可信程度并作为其信任度,通过对用户信任度进行量化分级,实现对用户信任分级的安全策略,同时将不符合信任要求的恶意用户进行安全隔离以提高网络可信度与安全性。实验结果表明,本模型可以正确评估用户的可信度,并对用户的恶意行为进行快速响应,达到了设计目的。同时与动态信任评估模型相比,

对信任评估的准确度有一定的提升,能更好地实现对可信网络中用户的实时管理。

参考文献:

- [1] 张焕国,陈璐,张立强.可信网络连接研究 [J].计算机学报,2010, 33(4): 706 - 717. (ZHANG H G, CHEN L, ZHANG L Q. Research on trusted network connection [J]. Chinese Journal of Computers, 2010, 33(4): 706 - 717.)
- [2] 沈昌祥,张焕国,王怀民,等.可信计算的研究与发展[J].中国科学:信息科学,2010,40(2):139 - 166. (SHEN C X, ZHANG H G, WANG H M, et al. Research and development of trusted computing [J]. Scientia Sinica: Information Sciences, 2010, 40(2): 139 - 166.)
- [3] 闫小侠.可信网络框架研究与设计[D].北京:北京工业大学,2014. (YAN X X. The trusted network framework research and design[D]. Beijing: Beijing University of Technology, 2014.)
- [4] 冯登国,秦宇,汪丹,等.可信计算技术研究[J].计算机研究与发展,2011,48(8):1322 - 1349. (FENG D G, QIN Y, WANG D, et al. Research on trusted computing technology[J]. Journal of Computer Research and Development, 2011, 48(8): 1322 - 1349.)
- [5] 林闯,田立勤,王元卓.可信网络中用户行为可信的研究[J].计算机研究与发展,2008,45(12):2033 - 2043. (LIN C, TIAN L Q, WANG Y Z. Research on user behavior trust in trustworthy network [J]. Journal of Computer Research and Development, 2008, 45(12): 2033 - 2043.)
- [6] 梁洪泉,吴巍.基于动态贝叶斯网络的可信度量模型研究[J].通信学报,2013,34(9):68 - 76. (LIANG H Q, WU W. Research of trust evaluation model based on dynamic Bayesian network [J]. Journal on Communications, 2013, 34(9): 68 - 76.)
- [7] FENG R, XU X, ZHOU X, et al. A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory [J]. Sensors, 2011, 11(2): 1345 - 1360.
- [8] 蒋黎明,张琨,徐建,等.一种基于图论方法的开放计算系统证据信任模型[J].计算机研究与发展,2013, 50 (5): 921 - 931. (JIANG L M, ZHANG K, XU J, et al. A new evidential trust model based on graph theory for open computing systems [J]. Journal of Computer Research and Development, 2013, 50(5): 921 - 931.)
- [9] 李道丰,杨义先,谷利泽,等.状态行为关联的可信网络动态信任计算研究[J].通信学报,2010,31(12):12 - 19. (LI D F, YANG Y X, GU L Z, et al. Study on dynamic trust metric of trusted network based on state and behavior associated [J]. Journal on Communications, 2010, 31(12): 12 - 19.)
- [10] 吴旭.基于增强稳定组模型的移动 P2P 网络信任评估方法[J].计算机学报,2014,37(10):2118 - 2127. (WU X. Enhanced stable group model-based trust evaluation scheme for mobile P2P networks [J]. Chinese Journal of Computers, 2014, 37(10): 2118 - 2127.)
- [11] 刘雪娇.数据挖掘中的动态聚类及增量研究 [D].哈尔滨:哈尔滨理工大学,2015. (LIU X J. Research on dynamic clustering and incremental in data mining [D]. Harbin : Harbin University of Science and Technology, 2015.)
- [12] HAN J, KAMBER M. Data Mining: Concepts and Techniques [M]. San Francisco, CA: Morgan Kaufmann, 2011: 13 - 18.
- [13] HAMERS L, HEMERYCK Y, HERWEYERS G. Similarity measures in scientometric research: the Jaccard index versus Salton cosine formula [J]. Information Processing & Management, 1989, 25 (3): 315 - 318.

(下转第 2458 页)

$L \cdot Adv_{DBDH,A}^{IND}$)。由于方案 IBBE 和方案 IBE 都是在随机预言机下 IND-sID-CPA 安全的,因此 $Adv_{IBBE,B}^{IND-sID-CPA}$ 和 $Adv_{IBE,A}^{IND-sID-CPA}$ 都可以忽略。此外,又由于 DBDH 假设成立,因此 $Adv_{DBDH,A}^{IND}$ 也可以忽略。综上所述, $Adv_{MCAPRE,A}^{IND}$ 必定可以忽略。换句话说,方案 MCAPRE 是在随机预言机下 IND-sID-CPA 安全的。

4 结语

本文充分利用基于身份的广播加密、基于身份的加密和基于身份的广播代理重加密的优点,提出了更实用的多条件型、非对称代理重加密方案。该方案充分考虑到目前移动设备计算能力一般这个劣势,根据条件,有选择地将复杂的基于身份的 IBBE 密文高效地转换成相对简单的 IBE 密文,更加利于移动设备的解密,便于移动设备高效快捷地访问云端的信息。但是,当条件增多时,方案的原始密文长度、重加密密文长度相应地都会增大,同时接收方在解密时也会增加配对运算的次数,但配对运算相对于指数运算比较耗时,因此为了使移动设备的解密速度更快,今后应该研究原始密文长度、重加密密文长度都不会随着条件个数的增加而线性增长的多条件型非对称代理重加密方案,而且也应该在减少接收方解密时的配对运算次数方面下功夫。

参考文献:

- [1] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography [C]// Proceedings of Advances in Cryptology — European Cryptology Conference '98, LNCS 1403. Berlin: Springer, 1998: 127 – 144.
- [2] BOLDYREVA A, FISCHLIN M, PALACIO A, et al. A closer look at PKI: security and efficiency [C]// PKC '07: Proceedings of the 10th International Conference on Practice and Theory in Public-Key Cryptography. Berlin: Springer, 2007: 458 – 475.
- [3] WANG L, WANG L, MAMBO M, et al. Identity-based proxy cryptosystems with revocability and hierarchical confidentialities [C]// SORIANO M, QING S, LÓPEZ J. Information and Communications Security, LNCS 6476. Berlin: Springer, 2010: 383 – 400.
- [4] CHU C K, WENG J, CHOW S S M, et al. Conditional proxy broadcast re-encryption [C]// Proceedings of the 2009 Information Security and Privacy, LNCS 5594. Berlin: Springer, 2009: 327 – 342.
- [5] XU P, JIAO T, WU Q, et al. Conditional identity-based broadcast proxy re-encryption and its application to cloud e-mail [J]. IEEE Transactions on Computers, 2016, 65(1): 66 – 79.
- [6] SHAO J, WEI G, LING Y, et al. Identity-based conditional proxy re-encryption [C]// Proceedings of the 2011 IEEE International Conference on Communications. Piscataway, NJ: IEEE, 2011: 1 – 137.)
- [7] LIANG K, LIU Z, TAN X, et al. A CCA-secure identity-based conditional proxy re-encryption without random oracles [C]// ICISC '12: Proceedings of the 15th International Conference on Information Security and Cryptology, LNCS 7839. Berlin: Springer, 2013: 231 – 246.
- [8] LIANG K, HUANG Q, SCHLEGEL R, et al. A conditional proxy broadcast re-encryption scheme supporting timed-release [C]// ISPEC 2013: Proceedings of the International Conference on Information Security Practice and Experience, LNCS 7863. Berlin: Springer, 2013: 132 – 146.
- [9] LIANG K, CHU C K, TAN X, et al. Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertext [J]. Theoretical Computer Science, 2014, 539(9): 87 – 105.
- [10] LI J, ZHAO X, ZHANG Y. Certificate-based Conditional Proxy Re-encryption [M]// AU M H, CARMINATI B, KOU C C J. Network and System Security, LNCS 8792. Berlin: Springer, 2014: 299 – 310.
- [11] DELERABLÉE C. Identity-based broadcast encryption with constant size ciphertexts and private keys [C]// Proceedings of the 2007 Annual International Conference on the Theory and Application of Cryptology and Information Security, LNCS 4833. Berlin: Springer, 2007: 200 – 215.
- [12] DENG H, WU Q, QIN B, et al. Asymmetric cross-cryptosystem re-encryption applicable to efficient and secure mobile access to outsourced data [C]// ASIA CCS '15: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2015: 393 – 404.
- [13] BONEH D, BOYEN X. Efficient selective-id secure identity-based encryption without random oracles [C]// EUROCRYPT 2004: Proceedings of the 2004 European Cryptology Conference, LNCS 3027. Berlin: Springer, 2004: 223 – 238.

Background

This work is partially supported by the National Natural Science Foundation of China (61272492, 61572521).

HAO Wei, born in 1990, M. S. candidate. His research interests include proxy re-encryption cryptosystem.

YANG Xiaoyuan, born in 1959, M. S., professor. His research interests include cryptography, information security.

WANG Xuan, born in 1981, Ph. D. candidate, associate professor. His research interests include cryptography, information security.

WU Liqiang, born in 1986, M. S., lecturer. His research interests include lattice-based cryptography, provable security.

(上接第 2451 页)

- [14] 王群, 戴秀岳, 杨莉. 一种基于直觉模糊理论的 P2P 动态信任模型 [J]. 计算机工程, 2014, 40(8): 133 – 137. (WANG Q, DAI X Y, YANG L. A P2P dynamic trust model based on intuitionistic fuzzy theory [J]. Computer Engineering, 2014, 40(8): 133 – 137.)

Background

This work is partially supported by the National Natural Science Foundation of China (61402530), the Natural Science Foundation of Shaanxi

Province (2014JQ8301).

XIE Hong'an, born in 1992, M. S. candidate. His research interests include network security, trusted computing.

LI Dong, born in 1993, M. S. candidate. His research interests include information technology.

SU Yang, born in 1975, Ph. D. , professor. His research interests include network security, trusted computing.

YANG Kai, born in 1985, Ph. D. , lecturer. His research interests include network security.