

# TrustedMarket: 一种基于信任度量理论的智能终端可信软件市场模型

平柳琼

(上海民航职业技术学院计算机教研室 上海 200232)

**摘要** 针对智能终端应用软件市场对上架应用软件审核不严格、第三方软件市场存在大量对合法软件“重新打包”的恶意软件等问题,设计了一种基于信任度量机制的理论建立的可信应用软件市场模型——TrustedMarket。针对智能终端自身计算能力、电量和网络流量受限,运行环境复杂的特点,提出了关系成熟度、忠诚度和推荐服务质量的观念用于描述智能终端对外提供的推荐信任值;提出了针对不同配置智能终端分级分类存储信任值的思想;提出了新近特性描述函数用于计算历史忠诚度评价值的权重,较合理地解决了特定信任度量模型中信任值计算的难题。通过在 Android 平台上实现的 TrustedMarket 模型,验证了该模型可较好地解决当前应用软件市场不可信的问题。

**关键词** 智能终端,软件市场,信任度量,安卓

**中图法分类号** TP393 **文献标识码** A

## TrustedMarket: A Trusted Software Market Model Based on Trust Measurement Theory for Smart Terminal

PING Liu-qiong

(Computer Teaching and Research Section, Shanghai Civil Aviation College, Shanghai 200232, China)

**Abstract** Aiming at the problem that the applications in the software market are not strictly examined, and the third party software market includes a large number of legitimate repackaged software, TrustedMarket, a trusted application software market model based on trust measurement mechanism was designed. As the characteristics of smart terminal's own computing power, electricity power and network traffic are limited and the operating environment is complicated, the concept of relationship maturity, loyalty and recommended service quality was proposed to describe the recommended trust value provided by the smart terminal. A new feature description function was proposed to calculate the weight of historical loyalty evaluation value. The problem of trust value calculation in specific trust metric model is solved by all the above technologies. Through the implemented TrustedMarket model on Android platform, it is proved that the model can solve the problem that the current application software market is untrustworthy.

**Keywords** Smart terminal, Software market, Trust measurement, Android

目前,智能终端应用软件市场存在大量的安全问题,信任管理理论主要用于解决大型分布式计算系统中,评估服务请求者和服务提供者之间可信度和信誉的问题,它为了解决智能终端应用软件市场不可靠、不可信的问题提供了很好的思路。

移动互联网环境下的应用软件市场和智能终端构成了服务提供者和服务请求者的关系,而在移动互联网环境下,没有中心化的应用软件市场信誉信息可以使用,也无法获得某一应用软件市场的全部信息,一旦终端向有恶意破坏行为的服务提供者(应用软件市场)请求服务(下载和安装软件),就可能造成终端受到新的安全威胁,因此,产生了应用软件市场的可信性和风险问题。

本文首先介绍信息度量理论的发展和研究,接着对基于信任度量理论的智能终端可信软件市场模型 TrustedMarket 的各个要素进行形式化定义,然后对该模型中关系成熟度和忠诚度的计算、初始信任值指定和信任值计算等问题进行了深入研究,最后通过构建实验环境验证了文中提出的模型的有效性。

## 1 研究现状与相关工作

在“信任”相关的研究领域中,研究的主要内容包括信任的表示、信任的计算、信任的度量和评估以及信任管理的相关理论。其中,信任的度量和评估方法研究是信任相关研究的重点和热点问题。

1996年, Beth等<sup>[1]</sup>学者首先提出了信任量化的概念和方法。在 Beth等学者提出的信任度评估模型中,将实体完成任务的情况定义为经验(Experience),根据所完成任务的成功和失败情况,经验被分类为肯定经验(Positive Experience)和否定经验(Negative Experience)。若成功完成任务则增加肯定经验记数,若任务失败则增加否定经验记数。信任度评估模型中的经验通常由推荐(Recommend)获得,事实上,推荐经验本身的可信问题同样也是信任问题。因此, Beth信任模型将信任分为直接信任(Direct Trust, DT)和推荐信任(Recommend Trust, RT)。

考虑到 Beth信任度计算模型中求简单算术平均值方法的不足,文献<sup>[2]</sup>中 Josang等学者引入了证据空间(Evidence

Space)和观点空间(Opinion Space)概念来定量描述信任关系,同时提出了一套主观逻辑(Subjective Logic)算子来进行信任度的推导和综合计算。

同时,其他学者也相继采用不同的方法来度量和推理信任关系。Rahman等<sup>[3]</sup>提出的信任度评估模型给出了信任度的传递协议和计算公式。MIT的Mui等<sup>[4]</sup>从社会学和进化论的角度给出了一个信任和信誉的计算模型。Aberer和Despotovic<sup>[5]</sup>共同提出了基于负面评价的反馈系统的信任模型。Xiong和Liu<sup>[6]</sup>提出了基于信誉的信任模型,将推荐信任的计算和信誉进行关联来获得实体节点的信誉。郭晶晶等<sup>[7]</sup>采用博弈论的思想为节点间的间接信任信息的获取建立了博弈模型,提出了惩罚机制并给出了节点的效用函数。林伟等<sup>[8]</sup>针对对等网络存在的信任缺陷,借助私有云平台在计算与存储过程中的高效性、安全性等特点,提出一种私有云协助的对等网络信任度量模型。蒋黎明等<sup>[9]</sup>提出一种稳定性增强的组信任模型SEGTM,以动态组构造与管理为基础,划分同组及跨组节点间的信任关系并给出了各自的度量方法,较好地解决了信任模型因信任网络拓扑动态改变而难以有效维护信任关系度量的准确性问题。李建等<sup>[10]</sup>提出了基于信任度量的软件下载的服务模型,设计了软件下载的服务流程,研究了软件下载的服务协议,分析了协议的安全性,比较了不同软件下载方案的安全性。Zheng Yan等<sup>[11]</sup>讨论了物联网环境下信任管理的相关问题。龚洁中<sup>[12]</sup>介绍了智能移动终端技术的发展特点,以及对于安全研究的需求,重点介绍了信任管理的基本概念、特点及模型分类,讨论了在智能移动终端环境中应用不同信任管理模型以及需要注意的问题。

学者们对信任关系的定义、信任度的计算和评估的研究成果为本文提出基于信任机制的智能终端可信软件市场模型提供了很好的研究基础,其中,对信任关系、节点和交互关系的定义,对信任模型中节点成熟度和忠诚度、信任级别的计算等关键问题的研究都可以为新的信任模型的建立提供参考和借鉴。

## 2 可信软件市场模型 TrustedMarket

### 2.1 TrustedMarket 模型中的重要概念

在研究智能终端可信软件市场问题前,首先需要对智能终端可信软件市场模型 TrustedMarket 中的若干重要概念进行描述,明确其定义和指代。这些重要的概念包括节点、服务节点、客户节点、关系成熟度、忠诚度、推荐信任值和信任值等。

**定义 1(节点, Nodes)** 节点是指参与应用软件发布和下载、安装的设备。节点的地位和作用并不是完全对等的,根据节点在环境中的地位和作用,将节点分为服务节点(Service Nodes)和客户节点(Client Nodes)。

**定义 2(服务节, Service Nodes)** 服务节点是指提供应用软件上传、发布和提供用户下载功能的节点。服务节点主要是指各类提供应用软件在线查询、下载功能的应用软件市场服务程序。

**定义 3(客户节点, Client Nodes)** 客户节点是指向服务节点申请提供服务的节点。客户节点主要是指从应用软件市场中查询、下载和安装应用软件的各类智能终端上安装的应用软件市场客户端程序。

**定义 4(关系成熟度, Relationship Maturity)** 大量智能终端用户之间的熟悉程度是不一样的,为了对终端之间的信任关系进行定量描述,首先需要对关系的熟悉程度进行定量描述。关系成熟度是对节点间的熟悉程度的定量描述。假设  $RM(node_i, node_j)$  表示节点  $node_i$  和节点  $node_j$  之间的关系成熟度,那么  $RM(node_i, node_j) \in [0, 1]$ , 并且  $RM(node_i, node_j)$  随着交往的次数递增。

本文引入了关系成熟度的概念,主要用于在移动互联网环境中提高节点之间信任度评估的效率。基本的出发点是基于推荐节点被使用来产生推荐信任度的频度。日常生活中,人与人之间的交往会随着交往次数的增多变得越来越熟悉。同样,在大规模移动互联网的分布式环境下的信任评价系统中,同样定义节点通过交互增加各自的熟悉程度。

**定义 5(忠诚度, Loyalty)** 智能终端所在的移动互联网是一个大型分布式环境,海量的终端用户本身的“可靠性”千差万别,部分用户甚至对外提供虚假信息。忠诚度用来定量描述一个客户节点对外提供推荐信任信息的“可靠程度”。假设  $W_{loyalty}(node_i)$  表示节点  $node_i$  的忠诚度,那么  $W_{loyalty}(node_i) \in [0, 1]$ , 并且  $W_{loyalty}(node_i)$  的初始值为 0.5。

**定义 6(推荐信任值, Recommend Trust Value, RTV)** 推荐信任值是一个客户节点对另一个客户节点提供的对某一请求服务节点的定量信任程度表示。RTV 是一个四元组  $\{node_i, node_j, node_s, c\}$ , 其中,  $node_i$  表示请求服务的客户节点,  $node_j$  表示提供推荐信任值的客户节点,  $node_s$  表示提供服务的节点,  $c$  表示服务的上下文环境,  $c \in \{Total, Software\}$ 。

**定义 7(客户节点和客户节点之间的通信, Communication between Client Nodes)** 客户节点在需要下载安装软件时,通过和邻居客户节点的通信来获得服务节点的推荐信任度量值。客户节点和客户节点之间的通信主要包括以下 3 种类型:

- 1) *GetRTV*( $node_i, c$ ): 请求获得在上下文环境  $c$  下, 服务节点  $node_s$  的推荐信任值;
- 2) *SetMaturity*: 通信完成后对关系成熟度进行设置;
- 3) *RecommendationEvaluate*: 对邻居客户节点提供的推荐信任服务进行评价。

**定义 8(客户节点和服务节点之间的通信, Communication between Client Node<sub>s</sub> and Service Node<sub>s</sub>)** 客户节点在下载安装软件时,需要和服务节点通信,通信的类型主要包括以下 3 种:

- 1) *QueryState*( $node_s$ ): 查询服务节点  $node_s$  的状态, 包括是否可提供服务、可提供哪些服务等;
- 2) *GetService*: 客户节点使用服务节点提供的服务, 本模型中主要是客户节点从服务节点处下载安装应用软件;
- 3) *SetOpinionExperience*: 服务结束后, 客户节点给出对该服务节点的自身经验(Opinion Experience)。

考虑到在移动互联网环境下,没有一个统一的可信第三方对服务节点进行信任评价,本节提出了一种基于主观信任的信任度评价模型,并将该模型应用到智能终端和应用软件市场的交互的信任度评价过程中。

**定义 9(信任值, Trust Value, TV)** 在 TrustedMarket 模型中,假设每个客户节点只与所有的邻居客户节点建立信任关系,对某一服务节点信任值的计算基于之前的自身经验

(Opinion Experience)和邻居客户节点的推荐信任值。TV 计算方法的表述如下:

$$TV(node_i, node_s, c, t) = \sum_{t=0}^t OE(node_i, node_s) + \sum_{k=m}^n RTV(node_k, node_s) \quad (1)$$

其中,  $TV(node_i, node_s, c, t)$  表示在时刻  $t$  和上下文环境  $c$  下, 客户节点  $node_i$  对服务节点  $node_s$  的信任值。它是由自身对服务节点的历史经验和所有邻居客户节点的推荐信任值综合计算得到的。

通过正面和负面的行为对其进行评价。历史行为可形成自己对所有节点的“个人观点(Personal Opinion)”, 节点可以共享其对邻居节点的“观点”, 这种观点被其他节点获取并利用即成为“推荐信任值”。推荐信任在节点无法获得服务节点的“个人观点”时非常重要。

### 2.2 TrustedMarket 模型概貌

基于信任机制的 TrustedMarket 模型可分为两个独立的部分: 学习部分和信任实施部分, 学习部分负责收集信息并将这些信息转化为知识, 比如, 学习部分负责监控每一个邻居节点的行为; 信任实施部分定义了如何使用学习阶段的知识 and 邻居节点之间交换的信息来评价每一个邻居的信任级别。

在智能终端这种受限的环境中, 不光要考虑恶意行为的节点, 还要考虑由于自身资源受限产生的有“自私”行为的节点, 比如终端为了省电和节省网络流量费用, 不为邻居节点提供推荐信任信息服务。本文使用推荐服务质量(Recommend Service Quality, RSQ)表征一个客户节点在信任计算过程中为其他客户节点提供服务质量的定量评价。

TrustedMarket 模型概貌如图 1 所示。

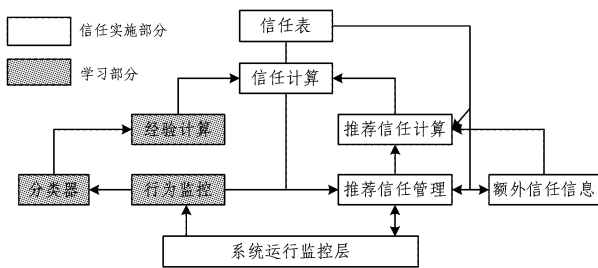


图 1 TrustedMarket 模型概貌

TrustedMarket 模型的学习部分依赖于 3 个基本模块: 行为监控模块、分类模块和经验计算模块。行为监控模块对邻居节点行为进行监控, 获取邻居节点对其他节点的服务质量; 行为监控模块也负责向推荐管理模块提供新加入的邻居节点的信息; 分类模块对行为监控模块提交的节点行为信息进行分析和归类, 将分类的信息送入经验计算模块; 经验计算模块通过分类器模块送来的部分信任值信息来计算邻居节点的信任级别。

信任实施阶段主要包括 5 个模块, 每个节点必须维持一个信息表, 表中包含每个邻居的推荐服务质量 RSQ。另外, 节点也可以存储其他邻居节点对某一邻居节点的 RSQ 信息。信任表中的每一个入口和一个时限(Timeout)关联, 当邻居节点从某节点的邻居中消失或 RSQ 超期, 则删除该入口信息, 同时所有与这个入口关联的推荐信息也应删除。在本文模型中, 每个节点还保存一张直接信任级别表和邻居成熟度表。直接信任级别表用于记录节点和服务节点历次交往中产生的“个人观点”信任评价信息, 邻居成熟度表用于记录与邻居节

点的交往历史信息, 用来评价邻居节点的“可信度”。

考虑到智能终端配置的差异, 本文定义了 3 种类型的信任信息存储类型: 基本型(Basic)、正常型(Normal)和高级型(Advanced)。运算能力差、存储容量低的终端节点使用基本操作, 它们只维护主信任表, 推荐信任交换协议也是可选的。运算能力和存储容量一般的终端节点使用正常操作, 保存了对其邻居节点的信任信息。运算能力强、存储容量大的终端使用高级操作, 它们维护主信任表、节点推荐信任表、节点成熟度表、节点忠诚度表和应用软件推荐信任表。节点保存的信息越多, 对服务节点信任级别的评估越准确。下文假设节点完整存放了所有信任信息。

推荐信任管理模块负责接收、发送和存储推荐信任信息。推荐信任管理模块和网络接口交互使用 CREP。推荐信任的接收包括两个动作, 其一是将推荐信任信息保存在 ATT(额外信任信息表)中并传递给推荐计算模块。推荐计算模块计算给定邻居节点的所有推荐信任信息, 并决定每一个邻居节点的忠诚度。忠诚度被传递到信任计算模块。信任计算模块基于忠诚度、直接信任信息和推荐信任信息评估节点的信任级别。信任计算模块在必要时也会请求推荐管理模块提供需要推荐的信任信息。本文模型只需要与邻居节点交互, 并且只存储邻居信息。对于计算能力、存储容量和电量受限的智能终端而言, 这是非常有用的设计。

### 2.3 关系成熟度和忠诚度的计算

如上文所述, 关系成熟度被定义为描述客户节点之间交互熟悉程度的定量描述, 当客户节点之间进行交互时, 节点之间的关系成熟度动态变化, 定义节点  $node_i$  和节点  $node_j$  之间的关系成熟度为  $RM(node_i, node_j)$ , 当  $node_i$  和  $node_j$  交互后,  $RM(node_i, node_j)$  递增, 本文定义  $RM(node_i, node_j)$  的初始值为 0, 每交互一次,  $RM(node_i, node_j)$  递增 0.01, 那么  $RM(node_i, node_j)$  的计算方法为:

$$RM(node_i, node_j, n) = \begin{cases} 0, & \text{initial} \\ RM(node_i, node_j, n-1) + 0.01, & \text{others} \end{cases} \quad (2)$$

忠诚度  $W_{loyalty}$  用于描述节点对外提供推荐信息的“可靠程度”,  $W_{loyalty}$  取决于它是否存在恶意推荐行为、拒绝推荐行为, 以及推荐信息是否对请求节点有效等因素。本文定义节点  $node_i$  和节点  $node_j$  之间交互完毕并给对方一个忠诚度评价  $E_{loyalty}(node_i, node_j, n)$ , 其中  $node_i$  和  $node_j$  表示此次交互的节点名称,  $n$  表示第  $n$  次交互,  $-1 \leq E_{loyalty}(node_i, node_j, n) \leq 1$ , 当节点  $node_i$  认为节点  $node_j$  存在恶意推荐行为, 拒绝推荐或推荐的信息虽然没有恶意, 但是对自己的信任评价没有帮助, 则评价  $E_{loyalty}(node_i, node_j, n)$  为负数, 否则为正数。定义  $v$  的计算方法如下:

$$E_{loyalty}(node_i, node_j, n) = \begin{cases} [-1, -0.6], & \text{malicion usrecommend} \\ [-0.6, -0.3], & \text{avoid recommend} \\ [-0.3, 0], & \text{no effect} \\ [0, 0.3], & \text{micro help} \\ [0.3, 0.6], & \text{normal help} \\ [0.6, 1], & \text{large help} \end{cases} \quad (3)$$

为了计算对邻居客户节点的忠诚度, 本文需要搜集当前客户节点对邻居节点的所有忠诚度评价, 并定义一个忠诚度

评价权重函数来评估每一个历史忠诚度评价对总忠诚度评价的贡献度。可以借用 FIRE 模型中的新近特性描述函数用于计算历史忠诚度评价的权重。新近特性函数可对新近的忠诚度评价赋予更大的权重,定义如下:

$$W_r(E_k) = e^{-\Delta t(E_k)/\lambda} \quad (4)$$

其中,  $W_r(E_k)$  是忠诚度评价  $e_k$  的权重,  $\Delta t(E_k)$  表示当前时间与忠诚度评价  $E_k$  产生的时间之差。假设之前节点  $node_i$  和节点  $node_j$  共有  $n$  次交互,发生的时间分别为  $t_k (t_k \in I \wedge t_k \in [1, n])$ ,则在节点  $node_i$  和节点  $node_j$  发生第  $n+1$  次交易时,节点  $node_j$  对节点  $node_i$  的忠诚度  $W_{Total\ loyalty}$  的计算方法为:

$$\begin{aligned} W_{Total\ loyalty} &= \frac{1}{n} \sum_{m=1}^n E_{loyalty}(node_i, node_j, m, v) \cdot W_r(E_m) \\ &= \frac{1}{n} \sum_{m=1}^n E_{loyalty}(node_i, node_j, m, v) \cdot e^{-\Delta t(E_m)/\lambda} \end{aligned} \quad (5)$$

上述忠诚度  $W_{Total\ loyalty}$  的计算方法中引入了新近特性函数,离当前时间越久的忠诚度评价对本次忠诚度评价的贡献越小,可以较公平地体现之前历次忠诚度评价对本次忠诚度计算的影响。

#### 2.4 初始信任值的指定

在 TrustedMarket 模型中,本文将信任值的计算分为两个阶段:初始化阶段(Initial phase)和信任值计算阶段(Trust value calculate phase)。在初始化阶段,需要为每一个节点制定一个信任值<sup>[14-15]</sup>。

当客户节点  $node_i$  首次请求邻居节点  $node_j$  提供某服务节点  $node_s$  推荐信任值时,节点  $node_i$  为节点  $node_j$  指定一个初始推荐信任值  $RTV_{init}(node_j, node_s)$ 。初始信任值指定的策略通常分为保守策略和乐观策略<sup>[12]</sup>。在保守策略中,客体节点  $node_i$  不信任任何陌生节点,并且认为所有的新邻居节点都可能对自己存在恶意行为,这种情况下就为初始推荐信任值  $RTV_{init}(node_j, node_s)$  指定一个较低的值。相反地,乐观策略认为在没有证据证明存在恶意行为前,所有的陌生节点和新邻居节点都是“可信的”,这样就为所有的初始推荐信任值  $RTV_{init}(node_j, node_s)$  指定一个较高的值。

考虑到智能终端对隐私信息、电量消耗和资费的敏感性,TrustedMarket 模型中基于保守策略对所有的节点的信任值进行初始化指定。为了更精确地指定节点  $node_i$  为节点  $node_j$  的初始信任值,本文同时引入邻居节点  $node_j$  对请求服务节点  $node_s$  的推荐信任值信息。综合考虑以上因素,TrustedMarket 模型对节点初始化信任值  $RTV_{init}(node_j, node_s)$  的计算方法如下:

$$RTV_{init}(node_i, node_j, node_s) = (1 - \eta)F(node_i) + \eta R(node_j) \quad (6)$$

其中,  $\eta$  表示其他邻居节点对节点  $node_j$  的推荐信任值所占的权重,  $F(node_i)$  表示基于保守策略所设置的节点  $node_i$  对节点  $node_j$  的初始信任值。在基于智能终端的 TrustedMarket 模型中,  $F(node_i)$  通常设置为 0.3 以下。

#### 2.5 信任值的计算

在 TrustedMarket 模型中,服务节点的信任值由请求服务的客户节点的直接信任值和其所有邻居客户节点的推荐信任值综合计算而成。假设客户节点  $node_i$  对服务节点  $node_s$  的总信任值为  $T_{node_i}(node_s)$ , Virendra 和 Jadliwala 等<sup>[13]</sup> 提出

使用以下公式计算  $T_{node_i}(node_s)$ :

$$T_{node_i}(node_s) = (1 - \alpha)Q_{node_i}(node_s) + \alpha R_{node_i}(node_s) \quad (7)$$

其中,  $\alpha (\alpha \in [0, 1])$  表示推荐信任值  $R_{node_i}(node_s)$  ( $R_{node_i}(node_s) \in [0, 1]$ ) 在总信任值  $T_{node_i}(node_s)$  中的权重,  $Q_{node_i}(node_s)$  ( $Q_{node_i}(node_s) \in [0, 1]$ ) 表示客户节点  $node_i$  对服务节点  $node_s$  的直接信任值。

##### 1) 直接信任值 $Q_{node_i}(node_s)$ 的计算

在 TrustedMarket 模型中,客户节点  $node_i$  对服务节点  $node_s$  的直接信任值  $Q_{node_i}(node_s)$  由两部分组成:对节点  $node_s$  的总体信任值  $Q_{node_i}(node_s, total)$  和特定上下文环境  $Context$  的信任值  $Q_{node_i}(node_s, context)$  (如下载某个软件时,对该软件的信任值)。  $Q_{node_i}(node_s)$  的计算方法为:

$$Q_{node_i}(node_s) = (1 - \beta)Q_{node_i}(node_s, total) + \beta Q_{node_i}(node_s, context) \quad (8)$$

其中,  $\beta (\beta \in [0, 1])$  表示总体信任值  $Q_{node_i}(node_s, total)$  ( $Q_{node_i}(node_s, total) \in [0, 1]$ ) 在  $Q_{node_i}(node_s)$  中的权重。

总体信任值  $Q_{node_i}(node_s, total)$  取决于客户节点  $node_i$  和服务节点  $node_s$  在每次交互过程中形成的直接信任评价价值  $TV(node_i, node_s, n)$  和信任值产生时间与当前时间的差值。为了公正评价之前各次直接信任值在总体信任值  $Q_{node_i}(node_s, total)$  中所占的权重,同样引入新近特性函数的概念。总体信任值  $Q_{node_i}(node_s, total)$  的计算方法如下:

$$\begin{aligned} Q_{node_i}(node_s, total) &= \frac{1}{n} \sum_{m=1}^n TV(node_i, node_s, m) \cdot W_r(TV_m) \\ &= \frac{1}{n} \sum_{m=1}^n TV(node_i, node_s, m) \cdot e^{-\Delta t(TV_m)/\lambda} \end{aligned} \quad (9)$$

特定上下文环境信任值  $Q_{node_i}(node_s, context)$  取决于客户节点  $node_i$  和服务节点  $node_s$  在特定上下文环境  $context$  下,每次交互过程中形成的直接信任评价价值  $TV(node_i, node_s, n, context)$  和信任值产生时间与当前时间的差值。为了公正评价之前各次直接信任值在特定上下文环境信任值  $Q_{node_i}(node_s, context)$  中所占的权重,同样引入新近特性函数的概念。特定上下文环境信任值  $Q_{node_i}(node_s, context)$  的计算方法如下:

$$\begin{aligned} Q_{node_i}(node_s, context) &= \frac{1}{n} \sum_{m=1}^n TV(node_i, node_s, m, context) \cdot W_r(TV_m) \\ &= \frac{1}{n} \sum_{m=1}^n TV(node_i, node_s, m, context) \cdot e^{-\Delta t(TV_m)/\lambda} \end{aligned} \quad (10)$$

##### 2) 推荐信任值 $R_{node_i}(node_s)$ 的计算

推荐信任值  $R_{node_i}(node_s)$  的获取主要通过客户推荐交换协议(CREP)进行。在智能终端中,由于其运算能力和电量都是受限的,为了计算  $R_{node_i}(node_s)$ ,本文定义一个邻居推荐信任值的阈值  $\tau_r$ ,定义一个客户节点  $node_i$  的邻居节点的子集  $K_{node_i}$ ,集合  $K_{node_i}$  中的元素  $k_i$  满足  $\forall k_i (k_i \in K_{node_i} \wedge k_i \leq \tau_r)$ 。本文只对集合  $K_{node_i}$  中的元素计算其对客户节点  $node_i$  的推荐信任值<sup>[14]</sup>。

推荐信任值  $R_{node_i}(node_s)$  取决于  $K_{node_i}$  中元素  $k_j$  和节点  $node_i$  的关系成熟度  $RM(k_j, node_i)$ 、节点  $k_j$  的忠诚度、节点  $k_j$  对节点  $node_s$  的总体推荐信任值  $R_{k_j}(node_s, Total)$  和节点  $k_j$  对节点  $node_s$  的特定上下文环境的推荐信任值  $R_{k_j}(node_s, context)$ 。推荐信任值  $R_{node_i}(node_s)$  的计算方法为:

$$R_{node_i}(node_i) = (1-\gamma)R_{node_i}(node_s, total) + \gamma R_{node_i}(node_s, context) \quad (11)$$

其中,  $\gamma(\gamma \in [0, 1])$  表示总体推荐信任值  $R_{node_i}(node_s, total)$  ( $R_{node_i}(node_s, total) \in [0, 1]$ ) 在  $R_{node_i}(node_i)$  中的权重。

总体推荐信任值  $R_{node_i}(node_s, total)$  取决于客户节点  $node_i$  的邻居节点  $k_j$  和服务节点  $node_s$  每次交互过程中形成的推荐信任评价价值  $RTV(k_j, node_s, n)$ 、关系成熟度  $RM(k_j, node_i, m)$ 、忠诚度  $W_{loyalty}(k_j, node_i, m)$  和推荐信任值产生时间与当前时间的差值。为了公正评价之前各次推荐信任值在总体推荐信任值  $R_{node_i}(node_s, total)$  中所占的权重, 同样引入新近特性函数的概念。总体推荐信任值  $R_{node_i}(node_s, total)$  的计算方法如下:

$$\begin{aligned} Q_{node_i}(node_s, total) &= \frac{1}{|K_{node_i}|} \sum_{k_j \in K_{node_i}} RTV(k_j, node_s, m) \cdot W_{loyalty}(k_j, node_i, m) \cdot RM(k_j, node_i, m) \cdot W_r(RTV_{k_j}) \\ &= \frac{1}{|K_{node_i}|} \sum_{k_j \in K_{node_i}} RTV(k_j, node_s, m) \cdot W_{loyalty}(k_j, node_i, m) \cdot RM(k_j, node_i, m) \cdot e^{-\Delta t(RTV_{k_j})/\lambda} \end{aligned} \quad (12)$$

特定上下文环境推荐信任值  $R_{node_i}(node_s, context)$  取决于客户节点  $node_i$  的邻居节点  $k_j$  和服务节点  $node_s$  在特定上下文环境  $context$  下, 每次交互过程中形成的推荐信任评价价值  $RTV(k_j, node_s, m, context)$ 、关系成熟度  $RM(k_j, node_i, m, context)$ 、忠诚度  $W_{loyalty}(k_j, node_i, m, context)$  和推荐信任值产生时间与当前时间的差值。为了公正评价之前各次推荐信任值在特定上下文环境信任值  $R_{node_i}(node_s, context)$  中所占的权重, 同样引入新近特性函数的概念。特定上下文环境推荐信任值  $R_{node_i}(node_s, context)$  的计算方法如下:

$$\begin{aligned} R_{node_i}(node_s, context) &= \frac{1}{|K_{node_i}|} \sum_{k_j \in K_{node_i}} RTV(k_j, node_s, m, context) \cdot W_{loyalty}(k_j, node_i, m, context) \cdot RM(k_j, node_i, m, context) \cdot W_r(RTV_{k_j}) \\ &= \frac{1}{|K_{node_i}|} \sum_{k_j \in K_{node_i}} RTV(k_j, node_s, m, context) \cdot W_{loyalty}(k_j, node_i, m, context) \cdot RM(k_j, node_i, m, context) \cdot e^{-\Delta t(RTV_{k_j})/\lambda} \end{aligned} \quad (13)$$

### 3 基于信任机制的可信软件市场模型在 Android 上的验证

基于信任度量理论的 TrustedMarket 模型为可信软件市场的研制提供了必要的理论支撑。为验证该模型的有效性, 本文在开源的 Android 操作系统平台下实现了 TrustedMarket 模型, 并在模拟器环境中进行了实验验证。

#### 3.1 实验环境设置

TrustedMarket 模型是一种移动互联网环境下的可行软件市场模型, 模型的验证需要大量的应用软件市场和智能终端的参与, 在现实的移动互联网环境中的验证需要对实际的应用软件市场服务器端软件和应用软件市场客户端软件进行改造, 实施的工作量较大。考虑到实验验证的方便性, 本文在实验室环境中, 使用“计算机+Android 模拟器”的模式搭建了如图 2 所示的实验环境。

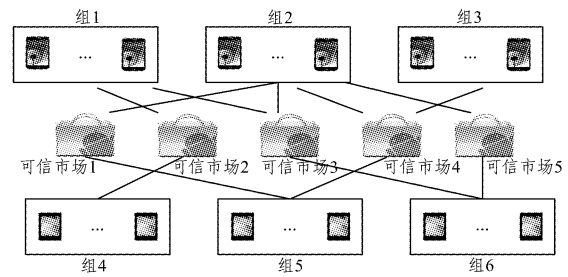


图 2 TrustedMarket 在 Android 下的实验环境设置

在图 2 的实验环境中, 本文使用了 5 台计算机安装 TrustedMarket 可信软件市场的服务端程序充当可信软件市场服务器, 使用 6 台计算机分别运行 Android 模拟器, 每台计算机上运行 5 个 Android 模拟器。为便于邻居节点的发现和推荐信任值的计算, 本文将同一台计算机上的 Android 模拟器设置运行在同一个子网下, 互为邻居节点。不同计算机上运行的 Android 模拟器不在同一个子网下, 不互为邻居节点。

#### 3.2 实验过程和分析

本文开发了 TrustedMarket 可信软件的服务端程序 TrustedMarket - Server 和客户端程序 TrustedMarket - Client, 在每一台充当应用软件服务器的计算机上部部署了 TrustedMarket - Server, 并各发布了 10 款应用软件, 如表 1 所列。在每一个 Android 模拟器上部部署了 TrustedMarket - Client, 并对所有服务节点的直接信任值进行了初始化。

表 1 可信软件市场上发布的软件列表

可信软件市场名称	发布的应用软件
可信软件市场 $TM_1$	$S_1, S_2, S_3, S_4, S_5, S_{11}, S_{12}, S_{13}, S_{14}, S_{15}$
可信软件市场 $TM_2$	$S_6, S_7, S_8, S_9, S_{10}, S_{11}, S_{12}, S_{13}, S_{14}, S_{15}$
可信软件市场 $TM_3$	$S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8, S_9, S_{10}$
可信软件市场 $TM_4$	$S_1, S_2, S_3, S_4, S_5, S_{16}, S_{17}, S_{18}, S_{19}, S_{20}$
可信软件市场 $TM_5$	$S_{11}, S_{12}, S_{13}, S_{14}, S_{15}, S_{16}, S_{17}, S_{18}, S_{19}, S_{20}$

为验证 TrustedMarket 系统的有效性, 本文假设组 1 的终端  $C_5$  要下载安装软件  $S_5$ 。下载安装流程如下:

- 1) 查找发布软件  $S_5$  的软件市场。查找后发现  $TM_1, TM_3, TM_4$  市场发布了软件  $S_5$ ;
- 2) 分别计算对  $TM_1, TM_3, TM_4$  市场的直接信任值  $Q_{TM_1}, Q_{TM_3}, Q_{TM_4}$ , 如有需要则初始化直接信任值;
- 3) 在邻居节点中查找对  $TM_1, TM_3, TM_4$  市场的推荐信任值  $R_{TM_1}, R_{TM_3}, R_{TM_4}$ , 如有需要则初始化推荐信任值;
- 4) 综合直接信任值  $Q_{TM_1}, Q_{TM_3}, Q_{TM_4}$  和推荐信任值  $R_{TM_1}, R_{TM_3}, R_{TM_4}$  得到总信任值  $T_{TM_1}, T_{TM_3}, T_{TM_4}$ ;
- 5) 比较计算得到的总信任值  $T_{TM_1}, T_{TM_3}, T_{TM_4}$ , 找到最大的信任值, 并从该市场下载安装软件;
- 6) 对推荐节点  $C_2, C_3, C_4$  的关系成熟度、忠诚度进行更新, 对  $TM_1, TM_3, TM_4$  的直接信任值进行更新。

从上述实验过程可以看出, TrustedMarket 模型在 Android 操作系统平台上得到实现后, 可显著提高通过应用软件市场下载安装软件过程的可靠性和安全性, 较好地解决了目前智能终端应用软件市场“不可信”、下载安装应用市场发布的恶意软件带来的安全威胁问题。

**结束语** 本文介绍了基于信任度量理论的可信软件市场模型 TrustedMarket。首先回顾了信任度量理论的发展与研究现状, 详细比较了 Beth 模型和 Josang 模型的特点。然后

(下转第 418 页)

二分K-means算法在6个节点下的规模增长性约为4个节点下的69%，且高斯混合算法在6个节点下的规模增长性约为4个节点下的68%，节点个数比例都近似于4/6，说明在该规模数据集下集群中节点的计算能力能得到充分利用。因而，对1GB以上规模的数据集进行聚类更适合集群结构。

**结束语** 通过对Spark中的3种代表性聚类算法即K-means、二分K-means和高斯混合聚类算法的性能进行比较，可以发现：1)当数据集规模小于500MB时，随着节点个数的增多，3种算法的加速比并没有呈现线性增长的趋势；而当数据集规模大于500MB时，3种算法的加速比均有了明显提高，且随着节点个数的增加，加速比近似于线性增长，因此，对500MB以上规模的数据集进行聚类适合采用集群结构来提高3种算法的运行效率。2)3种算法的可扩展性随着节点个数的增加而降低。当数据集规模大于500MB时，相对于K-means和高斯混合算法，二分K-means算法的可扩展性最低，因而，对于500MB以上规模数据集，K-means和高斯混合算法更适合在集群环境下运行。3)当数据集规模大于100MB时，高斯混合算法的规模增长性远高于K-means和二分K-means算法，这表明K-means和二分K-means算法对100MB以上规模的数据集的聚类效率更高。

### 参考文献

- [1] 陆嘉恒. Hadoop 实战[M]. 北京:机械工业出版社, 2012.
- [2] 周品. Hadoop 云计算实战[M]. 北京:清华大学出版社, 2012.
- [3] KONSTANTIN S. The Hadoop distributed file system [C]// The 26th Symposium on Mass Storage Systems and Technologies. IEEE, 2010; 1-10.
- [4] DEAN J, GHEMAWAT S. MapReduce: simplified data processing on large clusters[J]. Communications of the ACM, 2008, 51(1): 107-113.
- [5] DEAN J, GHEMAWAT S. MapReduce: a flexible data processing tool[J]. Communications of the ACM, 2010, 53(1): 72-77.
- [6] KARAU H. Fast Data Processing With Spark[M]. Birmingham: Packt Publishing Ltd, 2013.
- [7] ZAHARIA M, CHOWDHURY M, DAS T, et al. Fast and interactive analytics over Hadoop data with Spark[J]. USENIX, 2012, 37(4): 45-51.
- [8] 梁彦. 基于分布式平台 Spark 和 YARN 的数据挖掘算法的并行化研究[D]. 广州: 中山大学, 2014.
- [9] 唐振坤. 基于 Spark 的机器学习平台设计与实现[D]. 福州: 厦门大学, 2014.
- [10] 陈虹君. 基于 Spark 框架的聚类算法研究[J]. 电脑知识与技术, 2015, 11(4): 56-57, 60.
- [11] 王桂兰, 周国亮, 萨初日拉, 等. Spark 环境下的并行模糊 C 均值聚类算法[J]. 计算机应用, 2016, 36(2): 342-347.
- [12] 吴哲夫, 张彤, 肖鹰. 基于 Spark 平台的 K-means 聚类算法改进及并行化实现[J]. 互联网天地, 2016(1): 44-50.
- [13] 郭晶晶, 马建峰, 李琦, 等. 基于博弈论的移动自组织网络的信任管理方法[J]. 通信学报, 2014, 35(11): 50-58.
- [14] 林伟, 郑涵涵. 基于私有云信任度量的对等网络节点安全互联模型[J]. 电信科学, 2015, 31(1): 1-6.
- [15] 蒋黎明, 刘志明, 张琨, 等. 基于动态分组的开放分布系统信任度量与管理研究[J]. 通信学报, 2015, 36(1): 1-7.
- [16] 李建, 何永忠, 徐开勇. 基于信任度量的软件下载服务框架[J]. 武汉大学学报(自然科学版), 2008, 33(10): 1062-1066.
- [17] ZHENG Y, PENG Z, ATHANASIOS V. Vasilakos. A survey on trust management for Internet of Things[J]. Journal of Network and Computer Applications, 2014, 42(3): 124-134.
- [18] 龚洁中, 陈恭亮, 李建华. 智能移动终端的信任管理技术研究[J]. 中国电子科学研究院学报, 2011, 6(6): 567-570.
- [19] 林庆国, 刘宴兵. 一种基于信任的动态访问控制策略[J]. 重庆邮电大学学报(自然科学版), 2010, 22(4): 478-482.
- [20] VIRENDRA M, JADLIWALA M, CHANDRASEKARAN M, et al. Quantifying trust in mobile ad-hoc networks[C]// Proc. IEEE International Conf. on Integration Knowledge Intensive Multi-Agent Syst. Waltham, USA, Apr. 2005.
- [21] VELLOSO P B, LAUFER R P, CUNHA D D O. et al. Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model[J]. IEEE Transactions on Network and Service Management, 2010, 7(3): 172-185.
- [22] ABERER K, DESPOTOVIC Z. Managing Trust in a Peer-2-Peer Information System[C]// Proceedings of the Ninth International Conference on Information and Knowledge Management, 2001.
- [23] XIONG L, LIU L. Peer Trust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities [C] // Proceedings of 2003 IEEE Conference on E-Commerce, 2003.
- [24] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open network[C]// Proceedings of the European Symposium on Research in Security (ESORICS). Brighton: Springer-Verlag, 1994.
- [25] RD T, KNAPSKOG S J. A metric for trusted systems. Global IT Security[C]// Proceedings of the 21st National Security Conference. NSA, 1998; 87-91.
- [26] ABDUL-RAHMAN A, HAILES S. A distributed trust model [C]// Proceedings of the 1997 workshop on New Security Paradigm. NSPW, 1997.
- [27] MUI L, MOHTASHEMI M, HALBERSTADT A. A Computational Model of Trust and Reputation[C]// Proc. 35th Hawaii International Conference on System Sciences, 2002.

(上接第 389 页)

引出了 TrustedMarket 可信软件市场模型,对模型中的节点、服务节点、关系成熟度、忠诚度、推荐信任值等重要概念进行了定义,并详细研究了模型中关系成熟度和忠诚度的计算、初始信任值指定和信任值计算的关键技术。介绍了 TrustedMarket 模型在 Android 操作系统平台的智能终端上进行实验验证的过程。讨论了实验环境设置、实验详细过程等问题,最后对实验结论进行了深入分析。实验过程和结果分析指出,TrustedMarket 模型具有较高的可用性,可解决目前智能终端应用软件市场“不可信”的问题。

下一步,可以基于本文提出的可信软件市场模型构建安全性要求高的专用领域 Android 可信软件市场,保证专用领域 Android 智能终端应用软件来源可信。

### 参考文献

- [1] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open network[C]// Proceedings of the European Symposium on Research in Security (ESORICS). Brighton: Springer-Verlag, 1994.
- [2] RD T, KNAPSKOG S J. A metric for trusted systems. Global IT Security[C]// Proceedings of the 21st National Security Conference. NSA, 1998; 87-91.
- [3] ABDUL-RAHMAN A, HAILES S. A distributed trust model [C]// Proceedings of the 1997 workshop on New Security Paradigm. NSPW, 1997.
- [4] MUI L, MOHTASHEMI M, HALBERSTADT A. A Computational Model of Trust and Reputation[C]// Proc. 35th Hawaii International Conference on System Sciences, 2002.
- [5] ABERER K, DESPOTOVIC Z. Managing Trust in a Peer-2-Peer Information System[C]// Proceedings of the Ninth International Conference on Information and Knowledge Management, 2001.
- [6] XIONG L, LIU L. Peer Trust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities [C] // Proceedings of 2003 IEEE Conference on E-Commerce, 2003.
- [7] 郭晶晶, 马建峰, 李琦, 等. 基于博弈论的移动自组织网络的信任管理方法[J]. 通信学报, 2014, 35(11): 50-58.
- [8] 林伟, 郑涵涵. 基于私有云信任度量的对等网络节点安全互联模型[J]. 电信科学, 2015, 31(1): 1-6.
- [9] 蒋黎明, 刘志明, 张琨, 等. 基于动态分组的开放分布系统信任度量与管理研究[J]. 通信学报, 2015, 36(1): 1-7.
- [10] 李建, 何永忠, 徐开勇. 基于信任度量的软件下载服务框架[J]. 武汉大学学报(自然科学版), 2008, 33(10): 1062-1066.
- [11] ZHENG Y, PENG Z, ATHANASIOS V. Vasilakos. A survey on trust management for Internet of Things[J]. Journal of Network and Computer Applications, 2014, 42(3): 124-134.
- [12] 龚洁中, 陈恭亮, 李建华. 智能移动终端的信任管理技术研究[J]. 中国电子科学研究院学报, 2011, 6(6): 567-570.
- [13] 林庆国, 刘宴兵. 一种基于信任的动态访问控制策略[J]. 重庆邮电大学学报(自然科学版), 2010, 22(4): 478-482.
- [14] VIRENDRA M, JADLIWALA M, CHANDRASEKARAN M, et al. Quantifying trust in mobile ad-hoc networks[C]// Proc. IEEE International Conf. on Integration Knowledge Intensive Multi-Agent Syst. Waltham, USA, Apr. 2005.
- [15] VELLOSO P B, LAUFER R P, CUNHA D D O. et al. Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model[J]. IEEE Transactions on Network and Service Management, 2010, 7(3): 172-185.