基于博弈的物联网终端陌生节点信任评估模型及算法

苏照力[1] 蒋文保[1] 邱启迪[2]

（1.北京信息科技大学信息管理学院 北京 100192；2.中国科学技术大学 安徽合肥 230027）

【摘 要】物联网技术作为一种新兴应用技术快速地发展，其对推动能源、科技、医疗、教育等方面具有战略意义。物联网应用环境下的安全和信任问题，受到国内外专家的广泛的重视。在研究基于现有的物联网安全领域理论研究成果的基础之上，结合物联网应用层陌生节点的信任评估模型，并引入博弈论在信任评估模型的应用，提出了一种基于博弈的物联网终端陌生节点信任评估模型及算法。该模型在对应用终端和网络层的信息交互通过博弈达到均衡状态，并及时进行反馈和更新系统记录，此信誉管理中介站对于各个应用节点的信誉管理更加动态且高效。

【关键词】物联网；博弈；利益模型；信任模型

【中图分类号】TP393.0

【文献标识码】A

Apply the Game Theory to Trust Evaluation Model &Algorithm of Unknown Node in IOT Terminal

Su Zhao-li[1] Jiang Wen-bao[2] Qiu Qi-di[2]

（1.Beijing Information Science & Technology University Beijing 100192；

2.University of Science and Technology of China AnhuiHefei 230027）

【Abstract】IoT as a new application of technology , it is important to promote energy, science and technology, health care, education and so on.Domestic and foreign experts pay the extensive attention to the security and trust issues of IoT environment. Based on the existing research results of the theory of the security of the IoT, this paper combines the trust evaluation model of the unknown nodes in the application layer of the IoT and introduces the application of the game theory in the trust evaluation model, and proposes a game- Trust evaluation model for unfamiliar terminal. In this model, the information exchange between the terminal application and the layer network come to balanced by the game-Trust evaluation, and update system records in time. This intermediary station of reputation management make each application node's reputation management more efficient.

【Keywords】lot; game; interest-model; trust-model

1 引言

物联网技术的兴起又一次推动了计算机技术的创新发展，物联网应用越来越贴近人们的日常生活。随着人们对隐私信息保护意识的增强，对数据信息的读取者的身份认证成为物联网中信任管理的重点问题。信任管理的目的是提出一个开放的、分布的和动态特

性的安全决策框架适用于开放式应用系统。在信任管理中组织管理应用实体对下属传输层采集数据的基站的安全授权问题,是保证信息安全传输、存储的主要方面。但当前对于应用层所下属的可信任基站,能够控制保证授权交互的安全可靠和访问权限的有效性,其他应用实体所属的陌生来访基站进行交互请求时,现在尚缺乏统一的信任管理机制来很好地实现信任评估与安全管理。

物联网应用和传统的网络存在一些差异,首先,物联网的终端比传统互联网接入终端更加复杂多样,且物联网的终端之间是相互通信或相互控制的。在其获得授权控制之前,需要对其安全信任等级进行博弈评估,而后再根据评估结果进行分配控制级别。其次,在不同的行业物联网具有领域专业性,如环境智能监测、汽车电子智能设备等,它们所收集的的数据来自不同的感知传感器,存在较大的差异,因此物联网是由许多异构网络和多样化的终端设备组成的网络,而异构网络[1]所面临协同能力和协作安全的问题。在此系统中引入博弈论的模型,系统通过感知设备获取用户的基本信息,并根据对该用户的历史服务记录进行利益和信誉度的博弈评估,以保证交互过程的安全。

2 国内外研究现状

1996 年,M.Blaze 等人首次将信任模型的研究与分布式系统的研究领域相结合,并且提出了这个“信任管理”Trust Management 的新概念 [1]。A.Adbul-Rahman 等人[3]提出了一种量化的数学模型,用以度量实体的信任。文献[4]中证书认证应用信任模型中,应用中介站同所有的应用实体系统相联系,处在中心节点,并且同相关联的应用之间建立起相对等的信任关系。

近年来,在信息安全的相关研究中也广泛应用到博弈论,博弈的相关理论可以提供决策分析理论支持。文献[5]提出了一种基于博弈论的网络安全态势评估方法。把攻击和防御的对抗比作成二者随机博弈问题,利用信誉管理对网络站点的评估来确定博弈参数,评估结果可以通过攻防博弈的纳什均衡来量化,但该博弈参数的确定方法存在较强的主观性。文献[6]在对防御和共谋行为的识别方面的研究较为全面,制定了不同的奖惩措施来针对不同场景下恶意服务在选择策的略,并且对每种措施组合做了详细的收益分析,并提供了使系统达到帕累托最优状态的条件,为基于博弈论的信任评估研究提供基础。Isaac Agudo 等人[7]提出将安全机制和激励机制结合起来的基于 VCG 机制的改进协议,为防止节点在路径选择阶段的作弊行为选出最佳路径,为保证信息在数据转发阶段可靠传输引入加密机制。

文献[8]提出了一种非标准博弈框架,运用贝叶斯网络来推断系统可能的状态,对多个层级进行建模,进而对复杂的分布式拒绝服务攻击攻防场景进行评估,但该方法只能对特定的分布式拒绝服务攻击场景进行评估,适用面较窄。

针对物联网环境的特点,在前人的研究基础上[9]针对模型算法中存在的不足,为物联网终端应用的信任评估模型设计了一种基于博弈的陌生节点信任度评估模型。陌生网络站点向其他应用终端发出交互授权请求,应用实体将通过第三方信誉管理中介站来验证其所属应用的信誉,并根据此交互授权所获的收益进行评估,运用博弈收益算法综合计算做出决策。信誉管理中介站对陌生网络节点的交互结果和行为做出评估管理,并且反馈更新应用实体的信誉。

3 基于博弈的陌生节点信誉评估模型

在基于信誉的信任评估模型中,信任是主体对客体特定行为的主观预判,根据经验记录随着客体行为的变化而不断矫正。此模型是参照人在社会中的信任关系,根据对方的信誉来判断他的可信度,它并未依照实体间的固定关系,而是将信任视为经验的积累和表达,并将信任进行分级和量化,它现在广泛应用于 P2P 环境下各种分布式应用(如 Kazaa)、电子商务(如阿里巴巴和亚马逊网上商城等)和在线社区等领域,成为近年来研究的热点。

当应用实体授权网络站点时,看作两个终端之间的博弈,响应实体终端将选择对自己受益更大的一方来作为授权方。在物联网分布式应用中,可按地理区域划分,形成可管理的单元,其中单元内由一个第三方的信誉管理中介站集中管理所下属的普通应用终

端的信誉。根据单元内终端的交互报告，管理终端的信誉；隶属普通应用实体参考信誉管理中介站所发布的终端实体的信誉值，决定是否对该网络站点进行授权。在应用实体对陌生节点信誉评估过程中，应用实体将优先保证自身交互安全的自私性原则，当网络站点同标签进行交互时，通过验证终端所属的授权请求，通过验证后，对于进行交互的陌生网络站点交互具有两种策略：授权或拒绝。

形成可管理的单元甲内普通应用实体的信誉由一个信任管理应用实体 P 集中管理，P 根据单元内整体的信誉报告，维护应用实体的信誉；普通应用实体参考 P 发布的应用实体的信誉值，决定是否对该交互请求进行授权。如图 1 所示。

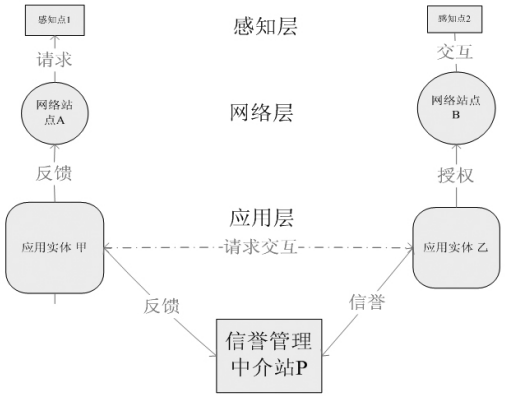

图 1 信誉管理框架

当应用实体接收到陌生网络节点的授权请求时，首先向信誉管理中介站发送消息，通过其向该节点所属应用提供的信誉以及该节点的信誉度和自己联通交互数据的收益，决定是否联通授权。如果交互行为的大部分历史信誉度较好，并且交互所获得的收益越大，那么将增大成功交互授权请求的可能性。因此，本文基于博弈收益和历史信誉提出陌生节点信誉度评估函数，且运用此函数于设计博弈授权交互算法，信誉度评估函数如下：

$$Auth(n)=Trust(n-1)\times Benefit \quad (1)$$

其中，网络站点的历史信誉度表示为 Trust(n−1)，而 Benefit 是指在本轮博弈中决策授权网络中心进行数据交互协作所能带来的收益。

本文设计提出的信誉度，是从终端自身的理性偏好出发，并且每一个应用实体的网络中心交互组织都保存了邻居节点的信誉度，同时又采用信誉管理中介站存储节点信誉，因此本模型的算法具有独立性、分布式、自动执行的特点，体现出该算法更适用于自私理性的物联网无线网络。在设计详细博弈授权算法前，首先介绍本文前面提出的两个用于信任度评估的模型：信誉度模型与利益模型。

3.1 信誉度模型

本文在研究节点历史行为的统计基础上，设计了基于信誉度模型的评估方法。在本模型中，将采取直接评估的原则对邻居节点的信誉度的评估，减少节点重复交互的开销，通过交互的历史博弈行为记录直接进行评估，进而得出信誉度。如此可以避免自私网络中，间接评估带来的不真实性。同时通过直接博弈决策也回避了由此带来的授权决策错误以及决策信誉效率降低等风险问题。每个应用终端都保存着邻居网络站点的历史交互记录，如表 1 所示。

表 1 历史博弈交互记录

历史博弈记录	第 i 轮	第 i−2 轮	第 i−2 轮	…	第 2 轮	第 1 轮
	授权	拒绝	授权	…	授权	拒绝

表 1 是近 i 次授权博弈的交互记录，其中也记录有邻居节点的行为。本文将记录每轮的博弈行为，Auth(i)表示第 i 轮邻居节点交互的行为。

$$Auth(i)=\begin{cases}0, \text{拒绝}\\ 1, \text{授权}\end{cases}$$

根据交互的历史行为授权记录，邻居节点的信誉度可计算为：

$$Trust=(\sum_{i=1}^{n} Auth_i/n)\times 100\%$$

本文中交互协作节点的信誉度可以当做博弈决策授权的一个标准，来防止协作交互应用的自私行为。如果交互双方在上一轮博弈中都不合作，那么交互双方

都可以采取降低其信誉度的方式来惩罚对手的恶意行为。由于节点无法得知何时退出博弈,所以必须要考虑当前的决策行为对后续博弈的影响程度,以及对自身信誉的影响。同时交互者也可通过改善自己的行为,进而改善和提高自身的信誉度,不会因为偶尔的不合作行为,失去与其他节点交互合作的机会。这种信誉度模型的设计理念既符合自然界人类的博弈决策理念,又体现了博弈授权过程的宽容性和学习性。

3.2 利益模型

在应用实体的授权博弈中,收益结果会根据交互节点的不同决定而不同。在物联网应用中的两个协作节点甲和乙,它们是授权应用博弈的参与者,即响应终端的网络站点甲和陌生终端的请求网络站点乙,二者各自有两个策略: 交互和拒绝。 根据授权博弈中的不同策略, 设计博弈所得收益的矩阵,如表 2 所示。

表 2 博弈利益

甲 / 乙	交互	拒绝
交互	Q,Q	S,T
拒绝	T,S	P,P

表 2 中的参数的意义是: 交互协作双方节点进行交互博弈时, 其中一个进行正常交互联通接受了对方的信息,但另一个拒绝交互,舍弃了对方的信息,则交互节点获得的收益是 S,而拒绝节点得到的收益是 T; 如果双方都进行正常的交互联通交换了对方的数据,双方收益都为 Q; 如果双方都拒绝交互, 舍弃交互彼此的数据,那么彼此所获得的利益都为 P。其中 T>Q>P>S,其中 2Q>T+S。在博弈的利益矩阵中,两个博弈的节点都拒绝交互舍弃信息的状态,形成矩阵的纳什均衡状态,如果两个博弈节点都合作进行正常交互并按照指令,接收信息的时形成帕累托最优状态。仅仅依照收益矩阵, 所有网络节点的参加者都能够推测出,如果在某一轮所进行的博弈中选择拒绝合作并拒接对方信息,那么本次博弈获益为 T,但是在今后该节点需要与另一节点进行交互时,有可能会遭到对方的拒绝,其请求信息会被拒绝,则它获得收益为 S,则在这两轮博弈后该节点的总收益变为 T+S; 如果双方从开始时就相互协作, 那么在两轮博弈后的获益便是 2Q。根据经济学原理可知 2Q>T+S, 在经过多次重复的博弈的过程中, 博弈的结果将衡趋近于帕累托最优状态, 物联网应用的网络节点也将根据收益最大的原则,选择相互合作、正常交互的策略安全执行指令并转发数据,以获得更高的信誉度。

4 基于博弈的陌生节点信誉评估算法

当响应方应用实体接收到协作网络站点的上一次交互行为的反馈信誉信息时, 运用基于博弈的陌生节点信誉评估算法, 即授权博弈评估对请求方的陌生网络节点,根据评估结果决策是否交互,应用实体是否对其授权。邻居节点选择协作节点时倾向选择前一次信誉度较好的节点协作交互, 以获取更高的利益和信誉值。基于网络站点的自私利益最大和信誉值获益最大原则, 如果网络节点在合作交互时获得较高的信誉等级,那么它获得授权,成功交互合作的可能性会更大。

4.1 应用实体信誉等级的划分

应用实体的信誉可以说是影响交互的一个非常重要的方面,信誉越高可信任也就越高,数据信息交互的安全可靠几率也就越高。

(1)评分原则

作为应用实体甲方, 对方应用实体乙进行交互主要看应用实体的信誉等级,应用甲所属网络站点是否安全执行指令、按照指令正确转发数据等。作为应用实体乙方, 其应用的信誉也是信用度的高度表现,真实客观的评价不仅可以在信誉管理中介站提升信誉度,也可以为其他更多的应用实体提供参考。信誉管理中介站为单元内应用终端提供安全评估服务,应用每交互一次,信誉管理中介站就会对交互对象作一次信用评价。

(2)积分标准

评价是参照电子商务(淘宝网)的卖家信用评分原

则，分为“好、中、差”三种，分别对应加一分、不加分和减一分相应的奖惩措施。

应用终端的信誉等级：

所积分数	等级图标	信誉等级
4分-10分	♥	一星
11分-40分	♥♥	二星
41分-90分	♥♥♥	三星
91分-150分	♥♥♥♥	四星
151分-250分	♥♥♥♥♥	五星

图 2 信誉等级图

4.2 陌生网络站点授权

当请求交互的网络基站所属终端为非信誉管理中介站所管辖内终端时，响应终端实体则将会通过信誉管理中介站来判断终端的信任度，并且根据陌生网络节点所属的应用实体提供的历史交易记录信息来进行信任度评估，进而判断是否符合安全交互信誉阈值范围。陌生网络基站授权交互说明如下：

（1）当陌生网络节点向应用实体发出交互请求，应用实体甲接到请求响应，判断出非可信应用所属的网络站点，向信誉管理中介站发出信息，信誉管理中介站检查其所属应用实体，并向该应用即非会员应用实体，发出请求验证消息。

（2）响应应用实体接收到信誉管理中介站的消息时，根据其通讯的历史记录来评估应用甲的信誉等级。

（3）双方应用通过博弈决策判断应用实体的信誉等级，选择信誉等级较为安全的应用实体来进行交互。

4.3 信誉中介站的信任反馈

信誉管理中介站是连接各应用实体之间的桥梁，为各应用之间的信任交互提供了安全的交互平台，并且记录各应用实体间的实际交互行为，根据应用间行为记录更新并保存各应用的信誉度和信誉等级。当应用交互结束后，接收应用实体状态的反馈报告，并定期检查更新应用的信誉，并引入惩罚因子管理应用实体的信誉值[10]。如下信誉管理中介站检查流程：

1、将应用实体的状态报告进行列表管理，列表包括交互双方交互信息对应节点 T={A，R(A)，n}

2、信誉管理中介站统计 T 的正确、节点故障、执行错误的报告数量，得出综合值作为 T 的最终考核结果，并列出所有节点的考核结果 Tm{A，R(A)}。

3、根据 A 所在应用对 Tm 进行散列，每个应用实体 agt 对应列表 Tagt={{A，R(A)}|A=agt}

4、统计标记每个 Tagt 的正确执行指令 right、执行报错 error、节点故障 faulty 报告数。

5、计算更新应用最终信誉值：Vtru=max {V-f*(error+faulty)}，f 是节点故障的惩罚因子

6、Intermediary Center 公布{Vtru}，如图 3 所示。

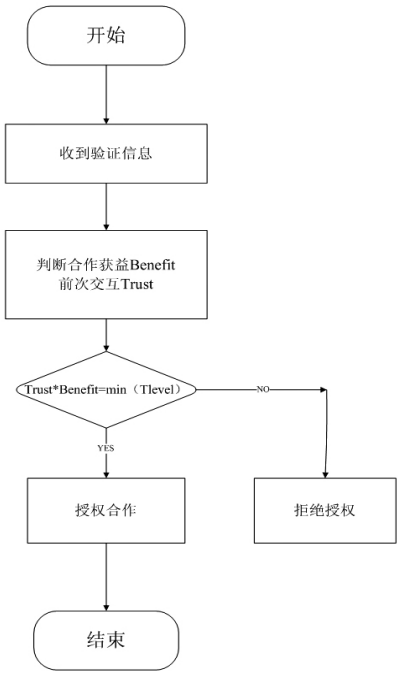

图 3 博弈评估工作流程图

在合作授权博弈决策的过程中，接受交互合作的终端对请求实体的信誉度评估如公式(1) 所示。接着应用实体将根据系统的信誉度阈值 TLevel 来判断是否合作，授权网络站点进行进一步的数据交互。如果陌生网络站点的信誉度大于应用实体设定的最小合作授权阈值，应用则接收网络站点的授权请求，授权交互请求进行合作数据交互，否则拒绝授权并且反馈更新其应用的信誉值。

应用实体博弈评估做出授权交互决策之后，还会受到信任模型的初始值和收敛性的影响，导致应用实体对陌生网络站点的不合理授权决策，此时就需要采用信誉反馈及时修正决策的错误。信誉管理中介站从感知节点提供的交互记录获得更新节点行为信誉度，并反馈到其所属应用实体的信誉值。如果某一个授权节点出现故障或恶意交互时，该节点会反馈异常信息到信誉管理中介站（Trust Management Intermediary Center），信誉管理中介站就会调整降低该节点的信誉等级和信誉值，如果其信誉值低于最低信誉等级时，那么应用有权撤销对其授权。

信任度评估模型的性能主要受其算法的收敛性和复杂程度的影响。在历史信誉模型和博弈收益模型基础上设计了基于博弈的信任度评估函数，并运用此函数设计博弈授权交互算法。当应用接收到陌生网络节点的授权请求时，通过信誉管理中介站收集到该节点所属终端的信誉以及该节点的信誉度，计算授权与该终端交互信息所得收益，进而决策是否交互授权。物联网应用的网络节点也将根据收益最大的原则，选择相互合作，正常交互的策略并且安全执行指令并且转发数据，以获得更高的信誉度。因此基于博弈的信任度评估算法是一种有效并且完备的算法。

5 结束语

本文首先对物联网终端的信任管理进行了分类，对于可信应用实体进行分级式信任管理，对于陌生网络站点交互行为进行基于博弈的信誉评估，对其已经授权的内部网络站点进行分析，设计一种信誉度模型和利益模型，采取自身安全收益最大原则对应用的网络站点信誉度进行信誉评估。在此基础上，即时反馈和更新应用实体和网络站点的交互行为，这就更加动态且更加高效地便于信誉管理中介站管理各应用终端上各节点的信誉度。

参考文献

[1] 董国钢，郑永昌，朱华，黎同根.异构环境下数据记录的复制与追加[J].微计算机信息. 2012(09).

[2] Song S, Hwang K, Macwan M, Fuzzy Trust Integration for Security Enforcement in Grid Computing [J], Network and Parallel Computing, 2004:9-21.

[3] Chenglin Miao, Liusheng Huang,Weijie Guo, Hongli Xu.A . Trustworthiness Evaluation Method for Wireless Sensor Nodes Based on D-S Evidence Theory. Wireless Algorithms, Systems, and Applications Lecture Notes in Computer Science Volume 7992, 2013: 163-174.

[4] Almenarez F, Marin A, Diaz D, Sanehez J. Developing a model for trust management in Pervasive devices. In: Bob Wemer, ed. Proc. of the 3rd IEEE Int'1 Workshop on Pervasive Computing and Communication Security (Persee2006).Washington: IEEE Computer Security Press, 2006:267-272.

[5] BaoTie, et al. Research on trustworthiness evaluation method for domain software based on actual evidence [J].Chinese Journal of Electronics,2011,20(2):195-199

[6] 陈建钧，张仕斌.基于云模型和信任链的信任评价模型研究[J].计算机应用研究, 2014,32:1-7.

[7] Isaac Agudo,Carmen Fernandez-Gago, Javier Lopez.A scale based trust model for multi-context environments.Computers and Mathematics With Applications .2010

[8] 潘春林，朱同林，刘寿强，等.基于理性博弈的 P2P 网络激励模型[J].计算机工程,2010,36(14): 79-81.

[9] 高逦，詹涛，汪芳.基于博弈论的 Ad Hoc 网络均衡路由协议[J].西北工业大学学报, 2014,32(2): 323-327.

[10] Wenbao Jiang,Qijing Li,Wenliang Chen. A multi-dimensional Evidence Based Trust Evaluation Model and Algorithm [J]. International Journal of Security and its Applications, Vol.9,No.5(2015),pp.123-132. (EI:20152500946940).

基金项目：

国家自然科学基金项目(NO:61540020)："基于多维证据的信任评估理论、模型与关键机制研究"。

作者简介：

苏照力(1992-)，男，汉族，山东菏泽人，北京信息科技大学，硕士研究生；主要研究方向和关注领域：信息安全。

蒋文保(1969-)，男，湖南人，毕业于清华大学，博士后，北京信息科技大学信息管理学院副院长，信息系统研究所副所长，教授，硕士生导师；主要研究方向和关注领域：网络与信息安全领域的科学研究、产品开发、教学和管理。

邱启迪(1995-)，男，中国科学技术大学，在读本科生；主要研究方向和关注领域：网络安全、密码学、信息隐写、图像加密与破译。