DOI:10.16526/j.cnki.11-4762/tp.2015.04.070

文章编号：1671-4598（2015）04-1404-03　　中图分类号：TP319　　文献标识码：A

基于模糊逻辑的物联网访问控制框架研究

马雪松[1,2]，路俊维[1,2]

（1.燕山大学 信息技术学院，河北 秦皇岛　066004；2.邢台职业技术学院 现代教育中心，河北 邢台　054035）

摘要：访问控制协议是网络中资源安全访问与共享的重要研究内容，为了提高物联网中访问控制协议的可扩展性和能源利用率，提出了一种基于模糊逻辑的访问控制协议；首先通过模糊的信任值对设备间的访问控制权限进行定义；其次，基于经验、知识和推荐的语言模型及其成员函数定义进行信任值的计算；最后提出了一种物联网访问控制框架；通过模拟实验表明，随着网络节点个数的增加，平均能量消耗逐渐增大，提出的方法在相同的网络环境下其平均能量消耗小于经典的访问控制方法，而且提出的方法在节点规模增大的情况下，平均能量消耗的增加率逐渐减小，这些表明了提出的方法与传统的访问控制协议相比，可扩展性好，能量利用率高，因而更适用于物联网环境下的访问控制。

关键词：物联网；访问控制；信任度；模糊逻辑

Research of Access Control Protocol for Internet of Things Based on Fuzzy Logic

Ma Xuesong[1,2], Lu Junwei[1,2]

(1. School of Information Technology, Yanshan University, Qinhuangdao　066004, China;
2. Modern Education Centre, Xingtai Polytechnic College, Xingtai　054035, China)

Abstract: Access control protocol is one of the most important research issues in secure resource access and sharing in Internet of Things. In order to improve the scalability and power usage of access control protocol, this paper proposes a fuzzy logic based access control protocol. Firstly, defined access control ability between devices by fuzzy trust score. Secondly, computed the trust score based on linguistic model containing experience, knowledge and recommendation and related membership functions. Finally, with the increasing number of network nodes, the average energy consumption increases gradually, the proposed method in the same network environment the average energy consumption is less than the classical method of access control, and the proposed method nodes in the case of larger scale, the average energy consumption rate decreases, proposed an access control framework for Internet of Things. Simulation experiments show that, compared with the classic access control protocol, the proposed approach has better scalability and higher power usage, and thus is better suitable for access control in environment of Internet of Things.

Keywords: internet of things; access control; trust; fuzzy logic

0　引言

物联网是由各种大量的带自配置能力的嵌入式设备所构成的无线传感器网络，这些设备包括射频识别（radio frequency identification，RFID）标签，PDA，以及传感器节点等[1]。在物联网中，人们周围存在着大量的计算设备，这些设备的资源是有限的，往往通过电池进行供电。此外，这些设备通过无线方式进行相互间的通信。物联网将现实世界与信息世界联系起来，向用户提供与环境相关的服务与应用。物联网将处于不同地理位置的用户、设备以及应用服务进行无缝的连接。然而，物联网在本质上是分布式的，其信任管理，访问控制和身份识别都面临着严峻的挑战。如果没有有效的身份识别和访问控制协议，普适网络带来的便利将变得十分有限[2]。

本文应用经验、知识和推荐等因素，计算出它们的模糊值，并将这些模糊值作为信息值的计算结果。在物联网中，可信的设备是对被访问资源进行授权的设备，因此访问控制需要可扩展的信任管理模型和框架。本文提出一种基于模糊方法的可信访问控制框架。该框架包括设备间进行通信交互的经验、知识和推荐组件，通过这些组件计算出信任值，并根据信任值进行访问控制的映射。

1　相关工作

Blaze 等人[3]提出了基于授权委托的信任管理，该方法包含“Policy Maker”和“Key Note”，其中授权委托与公钥相绑定，设备间基于相互的信任关系识别出彼此的授权证书。Josang[4]基于主观逻辑提出了信任管理模型。该模型用一系列主观逻辑操作符来进行信任值的计算和推到。然而，由于物联网中资源有限，缺少集中式服务器以及网络拓扑的动态变化使得授权委托很难应用于物联网中。Sun 等人[5]应用熵函数来表示节点间的信任关系，该方法可以动态地计算出加点间的信任关系。但是由于物联网的规模巨大，该方法的性能很低，并且灵活性差。Bhargav－Spantzel 等人[6]研究了如何将联邦身份管理系统和信任协商相结合来更好的保护用户信息。

Adjei 等人[7]讨论了如何应用信任管理来保护用户的身份隐私，但是并没有给出具体的解决方案。Liu 等人[8]对异构网络中的信任控制进行了理论分析，但是并没有解决设备的资源受限问题。在文献［9］中，作者定义了普适计算中不同的信任属性，这种信任属性是高层次的信任关系，但是没有给出性能的度量标准。无线通信中的信任管理模型的详细描述可参见

收稿日期：2014-08-09；　修回日期：2014-09-02。

基金项目：国家科技支撑计划项目（2009BAH501）。

作者简介：马雪松（1978-），男，山东淄博人，讲师，主要从事传感器技术及计算机网络等方向的研究。

路俊维（1974-），女，陕西杨凌人，硕士，副教授，主要从事计算机应用技术等方向的研究。

综述文章[10-11]。不同的用户或系统往往需要不同的用户级和系统级的信任模型，实际的物联网应用往往需要混合的信任模型。此外，物联网需要显示的信任模型来解决基于信任的访问控制。文献［12］应用模糊方法提出了一种基于信任的访问控制机制，并应用访问反馈进行访问控制，然而该方法却不适用于分布式结构的物联网。

上述模型采用信任来进行访问控制，它们都没有对信任进行很好地量化。为了对信任进行量化，本文将模糊方法用于信任的管理，该方法基于信任关系计算出上下文的信任值，从而实现了信任的量化。

2　访问控制模型

2.1　信任和访问控制

密钥保护可以从某种程度提高信任等级并实现访问控制，但是在物联网中该方法增加了额外的时间和能量消耗。采用模糊方法进行信任管理可以很容易地集成到基于效用的决策制定，同时该方法可以灵活地与附加组件相结合。本文将访问控制与信任关系相结合，其定义为公式（1）：

$$Level\_of\_Access\_Control(i \to j) \propto Trust(i \to j) \quad (1)$$

公式（1）表明从设备 i 访问设备 j 时，其访问控制水平与设备 i 对 j 的信任度成正比。访问控制与信任是紧密相关的，设备间的访问控制水平依赖于它们之间的信任水平。

本文应用设备间的信任关系进行访问控制的决策，依据设备的经验、知识和推荐进行上下文依赖的信任关系计算。此外，基于成员关系函数设计了一种新的语义，并依据该语义对信任关系进行量化。令模糊集合 A，其成员关系函数为 μ_A：$X \to [0, 1]$。在大多数模糊技术应用中，需要将模糊值转换为明确值，这个过程叫作去模糊化。Center－of－Gravity（COG）方法[13]是最重要的去模糊化方法之一。公式（2）和（3）分别为连续和离散样式的去模糊化公式：

$$COG(A) = \frac{\int_X \mu_A(x) x \mathrm{d}x}{\int_X \mu_A(x) \mathrm{d}x} \quad (2)$$

$$COG(A) = \frac{\sum_{q=1}^{N_q} \mu_A(x) x}{\sum_{q=1}^{N_q} \mu_A(x)} \quad (3)$$

信任是一种主观的基于上下文的值，它表示设备对其它设备行为的不确定预测。物联网是一种不确定环境，通过模糊方法计算信任值更适合于设备行为的量化和评估，以及访问控制规则的指定。信任管理系统负责管理设备对其它设备的授权，这种授权通过经验、知识和推荐来度量。为了实现该管理方法，本文基于收集到的信息，以及 Mamdani 模式的模糊规则实现信任计算。在该模型中，语言值经验、知识和推荐是模糊的，模型的输出是一个模糊集合。为了对该模型进行验证，信任的模糊值可以通过去模糊化方法转换为确定的值。Mamdani 模式是一种模糊关系模型，其中的每个规则都通过一个 if－then 关系来表示。Mamdani 类型的 if－then 模糊规则可以记为：

$$\text{if} \quad x_1 = A_{1r} \wedge x_2 = A_{2r} \wedge \cdots \wedge x_n = A_{nr}, \quad \text{then} \quad Y = B_r \quad (4)$$

其中：A_{ir} 表示第 r 个规则的第 i 个（$i=1, \cdots, n$）输入变量的语言标签，B_r 表示该规则的输出变量。每个 A_{ir} 和 B_r 分别用成员函数 μ_{ir} 和 γ_r 来表示，系统的模糊输出用如下公式来表示：

$$F(y) = \bigcup_{r=1}^{R}((\bigcap_{i=1}^{N} \mu_{ir}(x_i)) \cap \gamma_r) \quad (5)$$

2.2　计算经验、知识和推荐值

文献［14］表明，信任值在相同的上下文中与经验、知识和推荐 3 个部分相关。在上下文‘c’中，设备 A 对设备 B 的信任与先前的交互记录 V_k（$k=1, \cdots, n$）相关。如果交互成功，那么交互记录数加 1；如果交互失败，那么交互记录数减 1。基于先前的成功的和失败的交互记录，k 个交互的经验值的计算为公式（6）：

$$(EX)^c = \frac{\sum_{k=1}^{n} v_k}{\sum_{k=1}^{n} |v_k|}, \quad (EX)^c \in [-1, 1] \quad (6)$$

在公式（6）中，经验值 $(EX)^c$ 用确定的值来表示，本文应用 Good，Average 和 Bad 这 3 个语义来表示。由于模糊逻辑表达了自然语言中的模糊性，本文采用模糊逻辑实现上述目的。在文献［13］中，Zadeh 引入了成员函数。成员度的取值在 0 和 1 之间，其中 0 表示非成员关系，1 表示完全成员关系。为了计算经验值，用语言标签 $(EX)^c$ 来表示成员度。

语言变量的定义如表 1 所示，其中 $L(EX)$、$L(KN)$ 和 $L(RC)$ 分别为经验、知识和推荐语言变量。语言变量经验值的成员函数的图形表示为图 1 所示。

表 1　语言变量定义表

$L(EX)$	$L(KN)$	$L(RC)$	取值范围	模糊区域
Bad	Insufficient	Negative	(－1，－0.5)	(－1，－1) (－0.5，－0.1)
Average	Less	Neutral	(－0.1，0.25)	(－0.25，－0.1) (0.25，0.5)
Good	Complete	High	(0.5，1)	(0.25，0.5) (1，1)

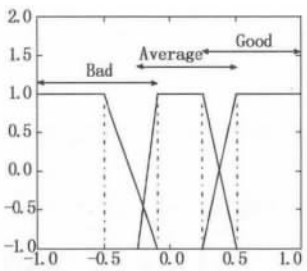

图 1　经验的成员函数示意图

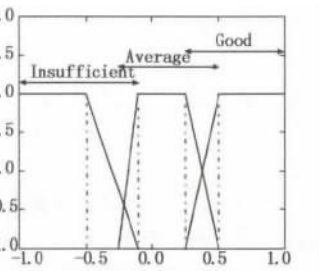

图 2　知识的成员函数示意图

在高级别的信任关系中，设备 A 需要知道 B 的所有知识，知识不充分将会影响设备的信任值。在上下文 c 中，准确的知识包括直接知识和间接知识，其计算公式如式（7）所示：

$$(KN)^c = W_d \cdot d + W_r \cdot r \quad (7)$$

其中：d，$r \in [-1, 1]$，W_d 和 W_r 分别为直接知识和间接知识的权重，W_d，$W_r \in [0, 1]$，并且 $W_d + W_r = 1$。知识语言变量的定义见表 1，成员函数如图 2 所示。

信任评估的第 3 个特征是推荐，其计算公式如式（8）所示：

$$(RC)^c = \frac{\sum_{i=1}^{n} w_i \cdot rc_i}{\sum_{i=1}^{n} rc_i} \tag{8}$$

其中：$rc_i \in [-1, 1]$ 为第 i 个设备的推荐值，$w_i \in [0, 1]$ 为该设备的权重。推荐语言变量的定义见表 1，其成员函数如图 3 所示。

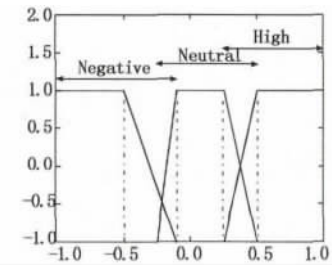

图 3 推荐的成员函数示意图

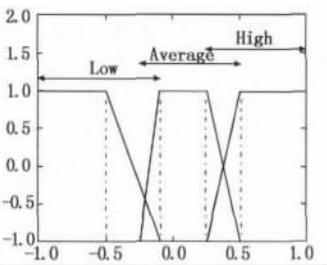

图 4 信任的成员函数示意图

基于经验、知识和推荐语言变量，本文定义的信任关系见表 2 所示，其等价的成员函数如图 4 所示。

表 2 模糊信任定义表

信任值	取值范围	模糊区域
Low	(−1, −0.5)	(−1, −1) (−0.5, −0.1)
Average	(−0.1, 0.25)	(−0.25, −0.1) (0.25, 0.5)
High	(0.5, 1)	(0.25, 0.5) (1, 1)

在信任关系的计算中，通过经验、知识和推荐语言变量进行模糊计算，其计算步骤如下：

1）利用成员函数分别计算出经验、知识和推荐的值，并将其作为输入，在 MATLAB 中应用 Mamdani 模糊推导系统计算信任值；

2）构建模糊规则库；

3）计算确定的和模糊的信任值。

2.3 信任管理框架

在普适计算环境下，有效的信任管理意味着高强度的访问控制，信任管理将产生一个功能系统。在该系统中，模糊信任值与是否允许访问相互映射，同时访问结果也伴随着信任度。本文提出的信任管理框架包含 3 层：

1）设备层：该层包含物联网中所有的设备以及设备间的通信。

2）请求层：该层主要负责收集经验、知识和推荐，并以此计算模糊信任值。

3）访问控制层：该层用于访问控制的决策，并在模糊信任值与访问权限间建立映射。

信任值与访问权限相映射以便提供对设备和知识的访问，基于模糊值的访问控制工作如下：假设设备的许可集合为 M，将设备 i 对设备 j 的信任分为 k 个间隔，即 $T = (T_1, T_2, \cdots, T_k)$，访问权限集合为 $AR = \{\phi, \{READ\}, \{READ, WRITE\}, \cdots, \{READ, WRITE, DELETE\}\}$。

集合 AR 的势为 k，其值与集合 T 的信任间隔的个数相等，并且每个 T_i 与 AR 中的一个元素相对应。如果模糊信任值 $T_1 = Low$，那么相应的 AR 元素为 ϕ；如果 $T_2 = Average$，那么相应的 AR 元素为 $\{READ\}$。

在分布式的物联网中，上述映射依赖于具体的上下文，并且信任间隔和访问控制之间的映射是变化的。当设备与其它设备通信时，经验、知识和推荐通过模糊方式得出，并据此计算出信任值。基于得到的模糊信任值，可以得到其它设备的可信性，并基于该可信性进行访问控制映射的管理。为了增强访问控制能力，可以增加访问控制框架中的语言项。例如，可以通过增加 Very Good，Very Bad，以及 Below Average 等语言项来增强访问控制的能力。随着物联网中设备数量的增加，系统中设备的访问控制功能并不会受到影响，因而该框架式可扩展的。此外，在具体的物联网上下文中，该框架中包含的语言项是可以增加或减少，因而该框架具有很好的灵活性。

3 仿真实验分析

本文应用 NS2 模拟器模拟了一个物联网的基本结构，并采用如下集合进行 T 和 AR 间的映射：$T = (Good, Average, Low)$，$AR = \{(Send, Receive, Forward, Drop), (Receive, Forward), (Receive)\}$。模拟环境及其参数设置如表 3 所示。

表 3 模拟环境及参数

模拟区域	800×800 mts
节点个数	100, 125, 150, 175, 200, 225, 250
传输功率	0.9 mW
接收功率	0.6 mW
初始能量	100 J
模拟时间	1 000 s
应用	温度传感器
应用速率	1 kbps
报文大小	512 bytes
模拟次数	3

在每个周期间隔，每个节点计算其与邻居节点之间的信任水平和访问权限。通过低信任度的设备来避免额外的通信开销，并以此来保证高的剩余能量。为了测试可扩展性，通过调整节点个数来观察平均能量消耗和平均剩余能耗。平均能量消耗的计算为所有节点的能耗之和与节点个数的比值，平均剩余能量为所有节点剩余能量的总和与节点个数的比值。

传统的基本物联网结构如图 5 所示。

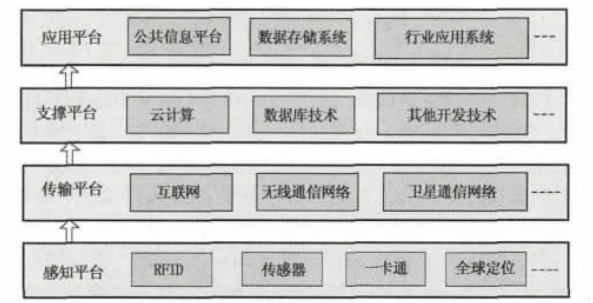

图 5 基本物联网结构图

平均能量消耗的模拟结果如图 6 所示。从图 6 可以看出，随着网络节点个数的增加，平均能量消耗逐渐增大，并且本文方法的平均能量消耗要远小于经典的访问控制方法，这表明本文提出的方法在相同的网络环境下其平均能量消耗小于经典的访问控制方法。此外，本文提出的方法在节点规模增大的情况下，平均能量消耗的增加率逐渐减小。这表明当增加网络规模

（下转第 1417 页）

[2] 邸　巍．基于视觉的全天候驾驶员疲劳与精神分散状态监测方法研究［D］．长春：吉林大学，2010.
[3] 陶　芬．全天候疲劳驾驶监测系统的研究及实现［D］．南京：南京理工大学，2009.
[4] 魏秀金．红外条件下驾驶员疲劳检测研究［D］．杭州：浙江理工大学，2011.
[5] 王江波，李绍文．基于 AdaBoost 算法和模板匹配的人眼定位［J］．计算机测量与控制，2012，20（5）：1347-1349，1353.
[6] 谢秀珍，唐　琎，陈守明，等．一种在红外图像中定位人眼的方法［J］．计算机工程与应用，2011，47（5）：202-205.
[7] 郝明刚，董秀成，黄亚勤．一种精确的人眼瞳孔定位算法［J］．计算机工程，2012，38（8）：141-143.
[8] 熊池亮．基于 Adaboost 算法的驾驶员疲劳检测［D］．成都：电子科技大学，2012.
[9] Viola P，Jones M. Rapid object detection using a boosted cascade of simple features［A］. Proc IEEE Conference Computer Vision and Pattern Recognition［C］. 2001，1：511-518.
[10] Lienhart R，Maydt J. An extended set of Haar-like features for rapid object detection［A］. IEEE International Conference on Image Processing［C］. 2002，1：900-903.
[11] Lienhart R，Kuranov A，Pisarevesky V. Empirical analysis of detection cascades of boosted classifiers for rapid object detection［A］. Proceedings of the DAGM-symposium［C］. 2003：297-304.
[12] Xu Y，Zhong A，Yang J A，et al. Bimodal biometrics based on a representation and recognition approach［J］. Optical Engineering，2011，50（3）：037202.
[13] Li S Z，Chu R F，Liao S C，et al. Illumination invariant face recognition using near-infrared images［J］. IEEE Transactions on Pattern Analysis and Machine Intelligence，2007，29（4）：627-639.
[14] Garcia I，Bronte S，Bergasa L M，et al. Vision-based drowsiness detector for real driving conditions［A］. IEEE Intelligent Vehicles Symposium［C］. 2012：618-623.
[15] 陈明初．基于人眼状态的驾驶员疲劳检测技术研究［D］．重庆：重庆大学，2012.

（上接第 1406 页）

时，本文方法引入的额外能耗少，因此具有较好的可扩展性。在本文提出的方法中，每个节点计算其它节点的经验、知识和推荐值。该计算是通过邻居节点间通信的方式进行，并且基于信任的方式进行访问控制，因此避免了低信任值的节点间的额外通信开销。

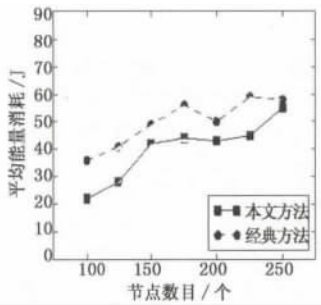

图 6　平均能量消耗对比图

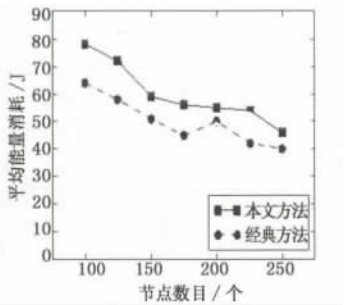

图 7　平均剩余能量对比图

图 7 为两种访问控制方法的平均剩余能量对比图。从该图可以看出，本文提出的方法的剩余能量明显高于经典的访问控制方法，并且能量利用率高，适用于物联网环境下设备间的访问控制。

4　结束语

访问控制是设备间进行资源共享的重要研究内容。在物联网中，往往存在着大量的能源有限设备。为了提高物联网中访问控制协议的可扩展性和能源利用率，本文提出了一种包含经验、知识和推荐的模糊逻辑访问控制协议。该方法应用自然语言中的模糊语义模型进行设备间信任值的计算，从而减少了低信任值设备间的信息传输。模拟实验表明，本文提出的方法与经典的访问控制协议相比，可扩展性好，能量利用率高，因而更适用于物联网环境下的访问控制。

参考文献：

[1] Atzori L，Iera A，Morabito G. The internet of things：a survey［J］. Computer Networks. 2010，54（15）：2787-2805.
[2] Gan G，Lu Z Y，Jiang J. Internet of things security analysis［A］. International Conference on Internet Technology and Applications［C］. 2011：101-110.
[3] Blaze M，Feigenbaum J，Lacy J. Decentralized trust management［A］. Proceedings of the IEEE Symposium on Research in Security and Privacy［J］. 2009：301-307.
[4] Josang A. Logic for uncertain probabilities［J］. International Journal of Uncertainty，Fuzziness，Knowledge-Based Systems，2001，9（3）：279-311.
[5] Sun Y L，Yu W，Han Z，et al. Information theoretic framework of trust modeling and evaluation for Ad-hoc networks［J］. IEEE Journal of Selected Areas in Communications，2006，24（2）：305-319.
[6] Bhargav-Spantzel A，Squicciarini A. Bertino E. Trust negotiation in identity management［J］. IEEE Security and Privacy Journal，2007，5（2）：55-63.
[7] Adjei J K，Olesen H. Keeping identity private［J］. IEEE Vehicular Technology Magazine，2011，6（3）：70-79.
[8] Liu Y，Wang K. Trust control in heterogeneous networks for internet of things［A］. International Conference on Computer Application and System Modeling（ICCASM）［C］. 2010，1：632-636.
[9] Trcek，D. Trust management in the pervasive computing era［J］. IEEE Journal of Security & Privacy，2011，9（4）：52-55.
[10] Yu H，Shen Z Q，Miao C Y，et al. A survey of trust and reputation management systems［J］. Proceedings of the IEEE Wireless Communications，2010，98（10）：78-82.
[11] Esch J. Prolog to a survey of trust and reputation management systems in wireless communications［J］. Proceedings of the IEEE，2010，98（10）：1752-1754.
[12] Ma S N，He J S，Shuai X B，et al. Access control mechanism based on trust quantification［A］. IEEE Second International Conference on Social Computing（SocialCom-2010）［C］. 2010：1032-1037.
[13] 陈　峰，荣晓慧，邓　攀，等．设备协同技术及其系统软件研究综述［J］．电子学报，2011，39（2）：440-447.
[14] Lei J Y，Cui G H，et al. Trust calculation and delivery control in Trust-Based access control［J］. Journal of Natural Sciences，2008，13（6）：765-768.