DOI:10.16208/j.issn1000-7024.2013.11.023

物联网中基于网关的跨域信任模型

马满福[1,2]，张 龙[1,2+]

（1. 西北师范大学 计算机科学与工程学院，甘肃 兰州 730070；
2. 甘肃省物联网工程研究中心，甘肃 兰州 730070）

摘 要：针对物联网环境下实体间的跨域信任问题，引入网关技术，提出基于网关的跨域信任模型。将域间节点历史交易纪录存储于网关中，提高对域间节点信任度的计算和存储能力；引入节点信任因子、历史因子，结合上下文环境变化对节点信任度值进行计算；提出节点跨域信任算法，并给出了模型详细流程。实验结果表明，模型具有良好的网络动态适应性以及较高的域间节点交互成功率，降低了物联网环境的变化对跨域节点信任评估准确性的影响。

关键词：物联网；多信任域；UTM 模型；网关；信任计算
中图法分类号：TP393 **文献标识号**：A **文章编号**：1000-7024（2013）11-3829-06

Inter-domain trust model based on gateway of IOT

MA Man-fu[1,2], ZHANG Long[1,2+]

(1. College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China;
2. Gansu IoT Research Center, Lanzhou 730070, China)

Abstract: The trust relationship inter-domain is restricted by difference of inner-domain model in Internet of Things, based on the UTM, a new IOT inter-domain trust model is proposed which implements trust value conversion among domains by gateway. In this model, the history scheduling record is stored on gateway by the strong computing and storage capacity. With the trust factor, history factor and context, the node trust value is computed, and then the trust algorithm of inner-domain is described. Finally, the process step of trust model is given. The experiments show that the model is efficient on SSP when IOT full load and stabilization, reduce the passive affect of veracity inter-domain trust value.

Key words: Internet of things; multi trust domain; UTM model; gateway; trust computing

0 引 言

随着物联网技术的迅速发展，逐渐形成了大规模、异构化、动态化的分布式物联网环境。对处于物联网环境中的诸多实体，如何跨越单信任域的限制，在多个信任域之间实现信息交互和资源共享显得十分重要。目前，国内外对于物联网跨域信任问题的研究仍处于起步阶段，还存在着诸多问题。George[1]等人提出基于半环代数理论的节点信任模型，将信任问题定义为有向图 $G(V,E)$ 的路径问题，然而该模型忽视了节点信任值的初始化问题。Claudiu[2]等人提出一种 P2P 环境下的动态信任模型，通过引入网络中节点的近期、长期信任度以及推荐信任度等参数来反映域间节点的信任度，然而该模型仅根据邻居节点的推荐来计算信任值，得到的只是局部信任度，影响了对节点信任评估的准确性。还有一些学者根据具体物联网应用背景提出跨域信任关系模型[3,4]，虽然能够解决某些具体类型物联网环境下的应用问题，但是局限性较大。

本文参考普适网络[5,6]、P2P 网络[7,8]信任模型，将网关技术引入物联网信任管理模型中，提出物联网新型多信任域网关的设计与实现方法。所提出的方法便于域间路由信息维护，提升了域间节点的交互以及通信能力；将域间节点历史交易纪录存储于网关中，提高了对域间节点信任度的计算和存储能力；同时，充分考虑影响信任度量化的各个因素，并结合上下文环境变化对节点信任度值进行计算与更新，有效提高了信任模型可信决策的准确性与动态适应能力。

收稿日期：2013-05-02；修订日期：2013-07-06
基金项目：国家自然科学基金项目（71263045）；甘肃省科技支撑基金项目（1204FKCA162）
作者简介：马满福（1968-），男，甘肃甘谷人，副教授，研究方向为计算机系统结构、移动计算；+通讯作者：张龙（1987-），男，河南商丘人，硕士研究生，研究方向为物联网、分布式与并行计算。E-mail：zhanglongstyle@163.com

1 多信任域互信问题

1.1 问题描述

物联网中存在众多的信任域，这主要是由不同信任域的管理策略和具体应用环境之间的差异造成的。图 1 为具有多信任域的物联网部署图。

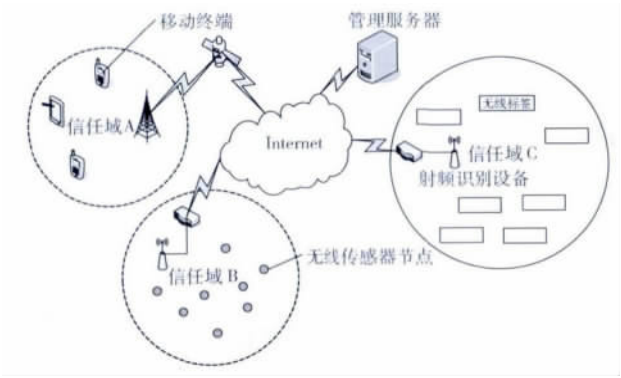

图 1 具有多信任域的物联网部署

在多信任域之间共享资源的情况下，物联网中资源的调度存在着域内调度和域间调度，因而产生了域内和域间两种信任关系。对于域内信任，实体处于同一信任域之中，受同一安全策略管理，这种信任关系当前已经进行了较为深入的研究[9,10]。本文着重于域间信任关系的讨论，在这种关系中，实体存在于多个信任域内，每个信任域都有着相对独立的安全管理策略，跨域关系实体间的信任值计算也缺乏标准，而且涉及到关系实体所处信任域的上下文环境、信任语义和信任值计算方法等问题。

1.2 UTM 模型

为解决物联网中的跨域信任问题，文献［11］提出了一种通用信任管理模型（universal trust management model，UTM），该模型负责在分布式系统中跨越多信任域实现实体间的信任关联[12]。UTM 模型既可以作为一个独立的信任模型来使用，也能在异构的信任域间提供实体信任的语义转换，模型结构如图 2 所示。

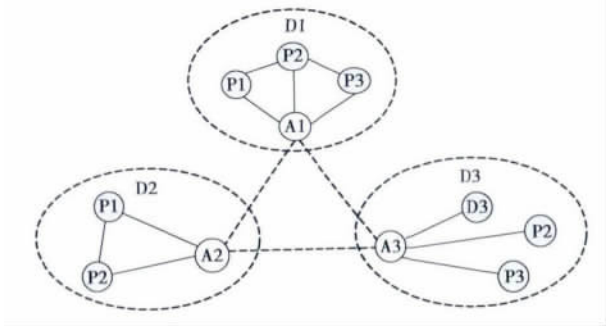

图 2 UTM 模型

UTM 模型中不同信任域间采用集中式信任管理，每个信任域都由代理来负责域内节点的信任度计算，同时代理担当“桥接”任务，实现与相邻信任域的连接。代理中存储着域内节点历史交易记录，当节点提出跨域服务请求时，代理根据历史交易记录对相关节点的信任度进行计算。然而，该模型还具有以下不足：

（1）该模型将不同信任域节点间的交易历史纪录存储于代理中，这就要求代理必须具有较高的存储能力和计算能力。然而，在实际物联网环境中所有节点均在计算能力、存储能力和能量水平上受限。

（2）缺乏路由信息支持，域间的相互通信需要发送大量的数据包，如果网络规模比较大，通信开销将会十分巨大。

（3）可信决策准确性与动态适应能力较低，不适合大规模动态的物联网网络环境。

2 多信任域网关设计

2.1 信任管理模型

针对 UTM 模型的不足，提出基于网关的跨域信任管理模型（GB-UTM，gateway based-UTM），该信任模型在 UTM 模型的基础上，在多信任域间设置了网关。网关的主要功能为：①存储相邻信任域的节点交易历史纪录；②维护信任域之间的路由信息；③查询节点历史交易记录，并根据查询结果进行信任值计算。GB-UTM 模型结构如图 3 所示。

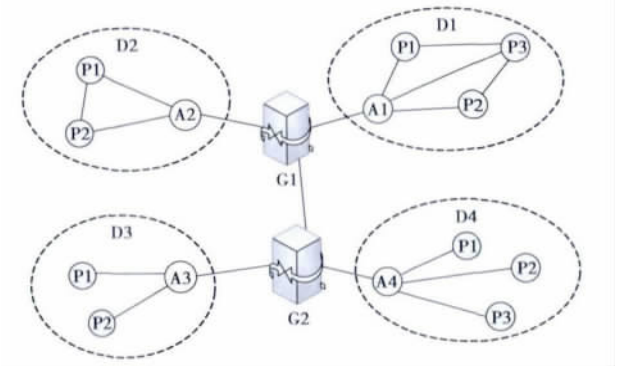

图 3 GB-UTM 模型

GB-UTM 模型中每个信任域均通过代理与网关相连，网关成为不同信任域之间沟通的桥梁，代理仅负责节点与相邻网关的通信。GB-UTM 模型中每个节点都有一个唯一的节点标识，节点标识的格式为：域 ID@域内节点 ID。例如，图 3 中域 D1 内的节点 P1 的标识为 D1@P1。在 GB-UTM 模型中网关为连接不同信任域的主要组件，用来维护各个信任域的历史交易记录，记录格式如图 4 所示。

网关为每个与其相连接的信任域建立一个历史交易记录表空间。由于网关的存储资源有限，不能无限的增加历史交易记录，并且信任度计算比较重视近期的交易历史记

请求节点ID	目标节点ID	信任度	交易时间戳	交易持续时间	成功数	失败数	计数器

图 4　历史交易记录格式

录，根据这些特征，在历史交易记录中加入一个计数器字段。当新增加一条历史交易记录时，网关给计数器设置一个正整数 n，n 的设置考虑到网关的存储空间与信任度计算的精度。网关每隔时间 t 对历史交易记录中的计数器字段执行“减 1”操作，并执行“定期清理”操作，清除计数器为零的历史交易记录。

2.2　信任度计算

物联网中信任的动态性就决定了信任是一个随着时间变化而演化的关系。Hassan 等人提出一种基于信任值向量的信任模型（Hassan's Model），该模型采用向量运算机制来计算实体信任值，并且具有信任关系动态性的特点[13]。因此本文参考 Hassan's Model 中的数学方法，来计算多信任域间实体的信任值。

Hassan's Model 引入了自信任因子、历史因子和时间因子，分别以 CF、PI 和 TE 表示。假设 P 对 Q 的信任度值 $t_{pq} \in [0,1]$，如果多信任域系统中有 n 个实体 $Q_1 Q_2 \ldots Q_n$，则第 i 个实体 Q_i 的信任度向量为 $\vec{Q}_i = (t_{Q_iQ_1}, t_{Q_iQ_2}, \ldots, t_{Q_iQ_n})$。当两个实体 Q_i 和 Q_j 初次交互时 $t_{Q_iQ_j} = null$，推荐的信任度如式(1)

$$PR_{Q_iQ_j} = \begin{cases} \vec{C}_{Q_iQ} \cdot \vec{C}_{QQ_j} / m; & S_{Q_i} \cap S_{Q_j} \neq \Phi \\ 0; & S_{Q_i} \cap S_{Q_j} = \Phi \end{cases} \tag{1}$$

其中，$\vec{C}_{Q_iQ} = (t_{Q_iQ_{k_1}}, t_{Q_iQ_{k_2}}, \ldots, t_{Q_iQ_{k_m}})$，$\vec{C}_{QQ_j} = (t_{Q_{k_1}Q_j}, t_{Q_{k_2}Q_j}, \ldots, t_{Q_{k_m}Q_j})$，$S_{Q_i}$ 与 S_{Q_j} 分别为所有满足 $t_{Q_iQ} \neq null$ 与 $t_{QQ_j} \neq null$ 的交互实体的集合，$m = |S_{Q_i} \cap S_{Q_j}|$ 为同 Q_i 与 Q_j 都具有交互历史的实体集合的基数。实体 Q_i 与实体 Q_j 的交互关系如图 5 所示。

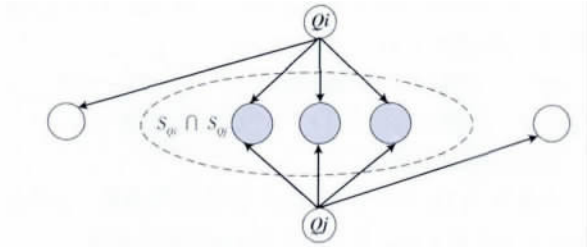

图 5　实体交互关系

$CF_{Q_iQ_j} \in [0,1]$ 用来表示 Q_i 对 Q_j 的信任因子，也就是Q_i 通过中间实体对 Q_j 的信心（confidence）。如果 Q_i 和 Q_j 的社交网络中具有共同的社交群体，即 $S_{Q_i} \cap S_{Q_j} \neq \Phi$，那么 Q_i 对 Q_j 的信任因子 $CF_{Q_iQ_j}$ 可以通过式(2)进行推导

$$\begin{cases} f(x) = 1 - \dfrac{1}{x+\alpha} \\ CF_{Q_iQ_j} = \dfrac{1}{2}[f(m) + f(I_{Q_i})] \end{cases} \tag{2}$$

式中：I_{Q_i} ——Q_i 与 $S_{Q_i} \cap S_{Q_j}$ 集合中各元素的交互数，从函数 $f(x)$ 中可以看出交互实体的信任因子与交互网络中的实体数和交互数存在着正向关系。

除了考虑信任因子外，实体间的信任度推导还与历史因子紧密相关，历史因子体现了实体间的历史交易记录对信任度的影响。在计算时，以历史交易成功数和交易失败数作为历史因子的推导参数，设 $SI_{Q_iQ_j}$ 与 $UI_{Q_iQ_j}$ 分别为 Q_i 与 Q_j 的历史交易成功数与失败数，那么历史因子 $PI_{Q_iQ_j}$ 可以通过式（3）进行推导

$$\begin{cases} h_{Q_iQ_j} = \max\{\bar{\omega}_1 SI_{Q_iQ_j} - \bar{\omega}_2 UI_{Q_iQ_j}, 0\} \\ PI_{Q_iQ_j} = 1 - \dfrac{1}{h_{Q_iQ_j}+1} \end{cases} \tag{3}$$

式中：$\bar{\omega}_1$、$\bar{\omega}_2$ ——权重，体现了对历史交易成功的奖励和对交易失败的惩罚。

信任度计算还具有时间相关性的特点，即在信任度计算中最近的交易具有最大的权重。任意两个交易实体 A、B 间都有一个时间戳，该时间戳记录着两个实体间最近交易的时间，记作 τ_{AB}。设实体 Q_i 期望在时间 τ 与 Q_j 进行交易，时间域值为 $\Delta\tau$，那么时间因子 $TE_{Q_iQ_j}$ 可以根据式（4）进行推导

$$TE_{Q_iQ_j} = \frac{m}{\sum_{i=1}^{m} (\tau - \tau_{Q_iQ_k})/\Delta\tau} \tag{4}$$

物联网多信任域中实体的信任度随着时间和上下文环境的变化而动态变化，在综合考虑自信任因子 CF、历史因子 PI 和时间因子 TE 的情况下，实体 Q_i 对 Q_j 的信任度根据式(5) 进行计算和更新

$$t_{Q_iQ_j} = \frac{\bar{\omega}_1 (PR_{Q_iQ_j}) \left(\dfrac{CF_{Q_iQ_j} + TE_{Q_iQ_j}}{2} \right) + \bar{\omega}_2 (PI_{Q_iQ_j})}{\bar{\omega}_1 + \bar{\omega}_2} \tag{5}$$

2.3　信任算法

由章节 2.2 可知，要计算域间节点 Q_r 对 Q_d 的信任度，首先需要得到节点 Q_r 与 Q_d 的公共社交群体集合 S。公共社交群体集合 S 通过对历史交易信息集合的计算得到，在请求节点所在域的网关和目标节点所在域的网关执行搜索算法1。

算法 1：公共社交群体集合的分布式搜索算法

输入——请求节点 Q_r 的 ID：r_id

目标节点 Q_d 的 ID：d_id

历史交易记录表：TH

输出——Q_r 和 Q_d 的公共社交群体集合 S

Dest _id 指 TH 表中的目标节点 ID 字段；Requ _id 指 TH 表中的请求节点 ID 字段；

S1：=Φ //初始化请求节点 Q_r 的社交集合

S2：=Φ //初始化目标节点 Q_d 的社交集合

gate _id ：= get _gateID（r _id） //获取请求节点所在域的网关 ID

gid ：= get _rank（） //获取当前执行分布式程序的网关 ID

IF gate _id IS gid THEN //如果请求节点所在域的网关正是执行程序的网关

select Dest _id into S1 from TH where Requ _id = r _id //在 TH 表中查询 Q_r 的社交集合

S2 ：= recv（tag） //接收目标节点 Q_d 的社交集合；tag 指发送和接收的同步标志

S ：= Intersect（S1，S2） //集合交

Return S //输出公共社交群体集合 S

ELSE

select Requ _id into S2 from TH where Dest _id = d _id //在 TH 表中查询 Q_d 的社交集合

send（S2，gate _id，tag） //把 S2 发送给网关 gate _id；tag 指发送和接收的同步标志

END IF //分布式算法结束

根据算法 1 计算出节点 Q_r 与 Q_d 的公共社交群体集合 S 之后，就可以根据下面的算法 2 计算出 Q_d 对 Q_r 的信任度。

算法 2：目标节点 Q_d 对请求节点 Q_r 的信任度生成算法

输入——请求节点 Q_r 的 ID：r _id

目标节点 Q_d 的 ID：d _id

历史交易记录表：TH

公共社交群体集合：S

输出——Q_d 对 Q_r 的信任度值 trust _value

//分别推导出式(5) 中所需的 4 个参数：推荐信任度 $PR_{Q_rQ_d}$、自信任因子 $CF_{Q_rQ_d}$、历史因子 $PI_{Q_rQ_d}$、时间因子 $TE_{Q_rQ_d}$

// $PR_{Q_rQ_d}$ 的推导算法

m ：= | S |　　// m 为公共社交群体集合 S 的基数

For Q_i in S Loop //对 S 中所有节点进行循环

sum += $t_{Q_rQ_i} \cdot t_{Q_iQ_d}$　　// $t_{Q_rQ_i}$ 和 $t_{Q_iQ_d}$ 为 TH 表中的信任度字段值

End Loop

$PR_{Q_rQ_d}$ ：= sum / m //根据式（1）计算出参数 $PR_{Q_rQ_d}$

Return $PR_{Q_rQ_d}$

// $CF_{Q_rQ_d}$ 的推导算法

$f(x)$：$= 1 - \frac{1}{x+\alpha}$　　// f(x) 来自式(2)

I_{Q_r} ：= count（Q_r，S）　　// I_{Q_r} 为节点 Q_r 与 S 中各元素的交互数

$CF_{Q_rQ_d}$ ：= average［f(m)，f（I_{Q_r}）］ //根据式(2)求平均

Return $CF_{Q_rQ_d}$

// $PI_{Q_rQ_d}$ 的推导算法

$SI_{Q_rQ_d}$ ：= 0 //初始化节点 Q_r 与 Q_d 的历史交易成功数

$UI_{Q_rQ_d}$ ：= 0 //初始化节点 Q_r 与 Q_d 的历史交易失败数

（$SI_{Q_rQ_d}$，$UI_{Q_rQ_d}$）：= Find _Transaction _Vector（r _id，d _id，TH） //从 TH 表中查询节点 Q_r 与 Q_d 的历史交易成功数和失败数

IF（$SI_{Q_rQ_d}$，$UI_{Q_rQ_d}$）is Φ THEN //如果 Q_r 与 Q_d 之前没有过历史交易

$h_{Q_rQ_d}$ ：= 0

ELSE $h_{Q_rQ_d}$ ：= $\tilde{\omega}_1 \cdot SI_{Q_rQ_d} - \tilde{\omega}_2 \cdot UI_{Q_rQ_d}$ //根据式(3)计算

END IF

$PI_{Q_rQ_d}$ ：= $h_{Q_rQ_d}$ /（$h_{Q_rQ_d}$ +1） //根据式(3)求出 $PI_{Q_rQ_d}$

Return $PI_{Q_rQ_d}$

// $TE_{Q_rQ_d}$ 的推导算法

For i in 1... m Loop //根据公共社交群体集合 S 的基数进行循环

sum += $(\tau - \tau_{Q_iQ_k})/\Delta\tau$ //根据式（4）计算：τ 为 TH 表中的交易时间戳字段值

End Loop

$TE_{Q_rQ_d}$：=m/sum //根据式(4) 计算出 $TE_{Q_rQ_d}$

Return $TE_{Q_rQ_d}$

//将以上计算出的 4 个参数值代入式(5)，计算出 Q_d 对 Q_r 的信任度值 trust _value

trust _value：= Compute（$PR_{Q_rQ_d}$，$CF_{Q_rQ_d}$，$PI_{Q_rQ_d}$，$TE_{Q_rQ_d}$） //将参数代入式（5）计算信任度值

Return trust _value

节点 Q_r 与 Q_d 根据计算出的信任度进行交易，交易结束之后，网关对历史交易记录表 TH 进行及时更新。

2.4 详细流程

下面以图 6 中节点 D4@P1 调用 D1@P1 为例，介绍 GB-UTM 模型的详细工作流程。

（1）D4@P1 发送 requst _resource（ID，D1@P1，Context）请求与 D1@P1 的交互。

（2）网关 G1 发送 requst _analysis（D4@P1）到网关 G2 请求分析 D4@P1 的相关历史交易记录，以得到 D4@P1

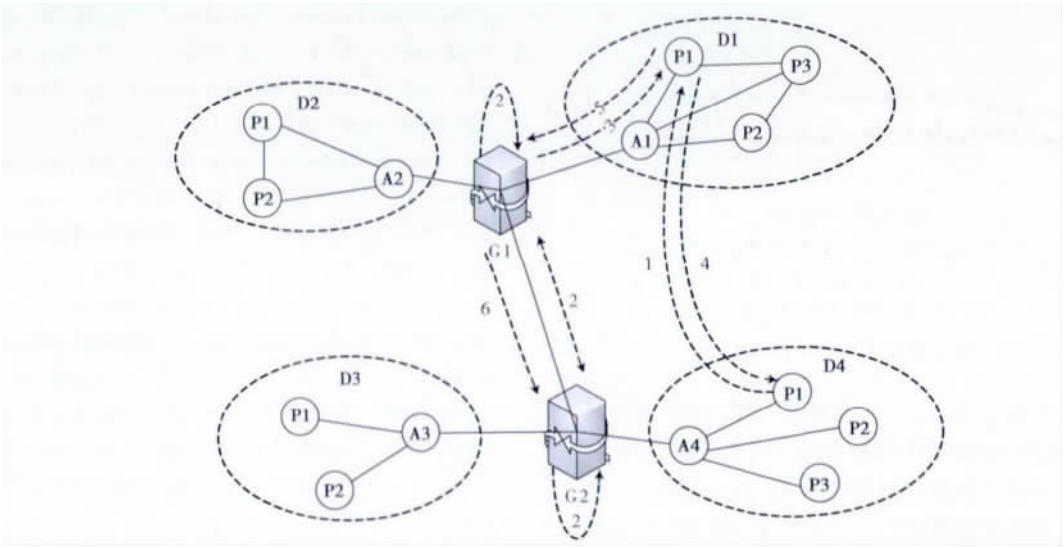

图 6　GB-UTM 工作流程

的社交集合 S1，G2 将分析结果 response _analysis（S1）发送给 G1。G1 对 D1@P1 的相关历史交易记录进行分析，得到 D1@P1 的社交集合 S2，然后 G1 将 S1 与 S2 进行集合交操作，得到公共社交群体集合 S。G1 根据 S 和历史交易记录计算得到信任因子、历史因子和时间因子，最后将这些参数代入式(5)，计算得出 D1@P1 对 D4@P1 的信任度。

（3）G1 将计算得到的信任度发送 send _trust（D1@P1，D4@P1，trust _value）到 D1@P1。

（4）D1@P1 与 D4@P1 进行交互。

（5）交互结束后，D1@P1 将交互结果发送给网关 G1，G1 随后更新本地历史交易记录。

（6）G1 发送 requst _update（RECORD，G2）请求 G2 更新历史交易记录。

3　仿真与分析

3.1　仿真设置

本文采用 OMNeT ++对物联网环境进行模拟仿真，来验证 GB-UTM 模型的可行性和效率。实验中部署两个信任域 A、B，每个信任域各有 500 个节点和一个相邻网关。将式(3) 中的参数 ω_1 、ω_2 分别设值为 0.8 和 0.2，以显示对失败交易的惩罚和对良好交易的激励。为提高仿真实验的准确性，设置实验运行次数为 2000，并将信任域中的节点分为目标节点、请求节点两种类型，且这两种身份相互独立、互不影响。本文采用网络节点交互成功率（swap success percent，SSP）作为衡量信任模型性能的指标，在动态变化的物联网环境中，拥有较高 SSP 的信任模型才具有较高的可信决策准确性与良好的网络动态适应性。下面给出 SSP 的计算公式

$$SSP = \frac{P_q(t)}{Q_{total}(t)} \tag{6}$$

式中：$Q_{total}(t)$ ——在 t 时刻系统中节点总的交互次数，$P_q(t)$ ——在 t 时刻系统侦听到的节点交互成功次数。考虑到节点交互网络的动态性，实验中设置以下参数：①服务请求频繁度（service request frequency，SRF，$0 \leqslant SRF \leqslant 1$），SRF 值越大，表示信任域中节点的服务请求越频繁；②社群节点动态频度（society dynamical frequency，SDF，$0 \leqslant SDF \leqslant 1$），表示网络中有 $SDF \times N$（N 表示域内节点总数）个节点具有不稳定性，它们可随时加入或离开所属信任域。

3.2　结果分析

将 GB-UTM 信任模型与原 UTM 信任模型进行对比试验，仿真结果如图 7、图 8 所示，分别显示在不同网络状态下，两种信任模型中节点交互成功率的差异。

图 7 所示的仿真实验中，实验参数 SRF、SDF 均为 0.2，表明此时的物联网网络环境相对稳定，信任域中节点的服务请求频度较低，且大多数节点不能随意离开。实验结果表明，在网络状态稳定的情况下，GB-UTM 模型和 UTM 模型均有较高的 SSP 值，且 GB-UTM 模型的 SSP 值更高，说明 GB-UTM 模型可以为系统提供更加稳定的服务。

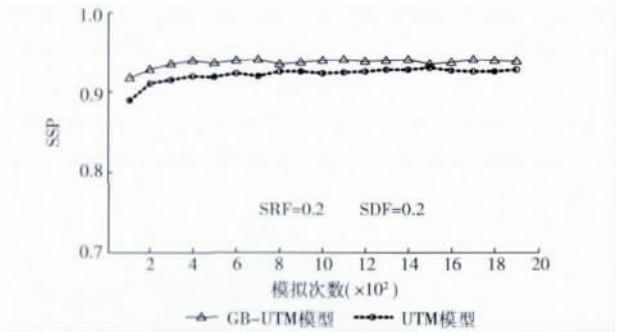

图 7　稳定状态下的系统

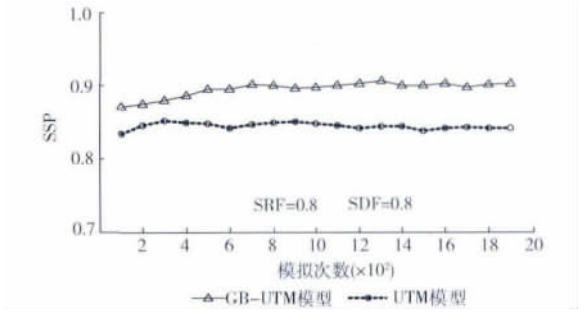

图 8 动态繁忙状态下的系统

图 8 所示的仿真实验中，实验参数 SRF、SDF 均提高为 0.8，表明此时的物联网网络环境处于高度动态且繁忙的情况，信任域中节点的服务请求频度高，网络开销大。从图 8 可知，在网络状态繁忙且节点交互业务量增加的情况下，GB-UTM 模型的 SSP 值能够平均维持在 90% 的水平，而 UTM 模型的 SSP 值仅维持在 83% 的水平，明显低于 GB-UTM 模型。实验结果表明，随着物联网网络负载以及网络动态属性的增加，GB-UTM 模型的可信决策准确性有了较大提高，而且具有更好的网络动态适应性，降低了网络环境的变化对跨域节点信任评估准确性的影响。

4 结束语

文章以物联网多信任域间实体互信问题为出发点，将网关概念引入到物联网信任模型中，取得了 3 个方面的研究进展：①将域间节点历史交易纪录存储与网关中，提高了对节点信任度的计算和存储能力；②网关的引入，便于维护域间路由信息，提升了域间节点的交互以及通信能力；③引入节点信任因子、历史因子，并结合时间和上下文变化对节点信任值进行计算与更新，提高了信任模型可信决策的准确性与动态适应能力。仿真实验表明，GB-UTM 模型比 UTM 模型具有更高的节点交互成功率，而且随着网络负载以及节点交互业务量的增加，GB-UTM 模型显示出更好的网络适应能力，降低了物联网环境的变化对跨域节点信任评估准确性的影响。

参考文献：

[1] Theodorakopoulos G，Baras JS. On trust models and trust evaluation metrics for ad-hoc networks [J]. IEEE Journal onSelected Areas in Communications，2006，24 (2)：318-328.

[2] Li Xiaoyong，Zhou Feng，Yang Xudong. A multi-dimensional trust evaluation model for large-scale P2P computing [J]. Journal of Parallel and Distributed Computing，2011，71 (6)：837-847.

[3] Jiang Liming，Xu Jian，Zhang Kun，et al. A new evidential trust model for open distributed systems [J]. Expert Systems with Applications，2012，39 (3)：3772-3782.

[4] LIU Yan. Research on trust control technologies in internet of things [J]. Process Automation Instrumentation，2011，32 (8)：60-63 (in Chinese). [刘艳. 物联网中可信控制技术研究 [J]. 自动化仪表，2011，32 (8)：60-63.]

[5] Mieso K Denko，Tao Sun，Isaac Woungang. Trust management in ubiquitous computing：A Bayesian approach [J]. Computer Communications，2011，34 (3)：398-406.

[6] Javier Lopez，Rodrigo Roman，Isaac Agudo，et al. Trust management systems for wireless sensor networks：Best practices [J]. Computer Communications，2010，33 (9)：1086-1093.

[7] Florina Almenárez，Andrés Marín. Trust management for multimedia P2P applications in autonomic networking [J]. Ad Hoc Networks，2011，9 (4)：687-697.

[8] Zhao Yulan，Jiang Chunfeng. Research of trust model in P2P file-sharing system [J]. Procedia Environmental Sciences，2012，12：1208-1212.

[9] Shaikh R A，Lee Y K，Lee S Y. Energy consumption analysis of reputation-based trust management schemes of wireless sensor networks [C] //Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication，2009：602-606.

[10] LIU Wenmao，YIN Lihua，FANG Binxing，et al. A hierarchical trust model for the internet of things [J]. Chinese Journal of Computers，2012，35 (5)：846-855 (in Chinese). [刘文懋，殷丽华，方滨兴，等. 物联网环境下的信任机制研究 [J]. 计算机学报，2012，35 (5)：846-855.]

[11] Lee A J，Yu Ting. Towards a dynamic composite model of trust [C] //Proceedings of the 14th Symposium on Access Control Models and Technologies，2009：217-226.

[12] ZHU Zhong，WU Guoxin. Survey of trust management in distri-buted multi trust domain [J]. Computer Science，2011，38 (4)：38-42 (in Chinese). [朱重，吴国新. 分布式多信任域信任管理技术研究综述 [J]. 计算机科学，2011，38 (4)：38-42.]

[13] LI Xiaoyong，GUI Xiaolin. Research on dynamic trust model for large scale distributed environment [J]. Journal of Software，2007，18 (6)：1510-1521 (in Chinese). [李小勇，桂小林. 大规模分布式环境下动态信任模型研究 [J]. 软件学报，2007，18 (6)：1510-1521.]