物联网环境下的信任机制研究

刘文懋[1)] 殷丽华[2)] 方滨兴[1)] 张宏莉[1)]

[1)] (哈尔滨工业大学计算机科学与技术学院 哈尔滨 150001)

[2)] (中国科学院计算技术研究所信息智能与信息安全研究中心 北京 100190)

摘 要 物联网环境下的信任机制是一个亟待研究的重要课题,文中提出物联网环境下层次化的信任架构,满足了不同主体的信任需求,隔离了机构信誉和阅读器信任.使用基于证据理论的方法推导动态运动阅读器的信任,因较短的标签通信距离使恶意事件检测效率较差,文中提出可验证缓存前次交互摘要的方法,有效检测出恶意的终端阅读器.在稳定的机构层,使用信誉机制维护机构信任.层间信任交互构成了"现象可信-行为可信-节点可信-机构可信-授权可信"的环流,使得信任得到快速收敛和反馈.实验表明,可验证缓存前次交互信息的方法有效解决了证据理论方法中因物体RFID通信距离短无法被邻居节点检测到的缺陷,层次化的信任机制具有较强的汇聚信任的能力,并有较快的收敛速度.

关键词 物联网;信任机制;证据理论;可验证缓存前次交互摘要;层次模型

中图法分类号 TP393 **DOI号:** 10.3724/SP.J.1016.2012.00846

A Hierarchical Trust Model for the Internet of Things

LIU Wen-Mao[1)] YIN Li-Hua[2)] FANG Bin-Xing[1)] ZHANG Hong-Li[1)]

[1)] (*School of Computer Science and Technology, Harbin Institute of Technology, Harbin* 150001)

[2)] (*Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100190)

Abstract The role of the trust model in the Internet of Things (IoT) represents an important domain which is not yet well studied. In this paper, we propose a hierarchical trust model to meet heterogeneous subject trust requirement and isolate organization trust and reader trust, in which the following processes can take place: A verifiable caching interaction digest (VCID) schema is introduced for the purposes of monitoring object-reader interaction, an improved evidence theory is employed to deduce unstable reader-reader trust, and a long-term reputation mechanism is used to manage indirect trust of organizations. A cross-layer trust loop flow is established through the following levels of trust: phenomenon, event, node, organization and authorizing. Within this flow, the reader trust from the lower layer converges up towards the organization reputation on the upper layer by way of supervisor readers quickly. With simulations analyzing the impact of abnormal node ratio, node density, and tag communication range on the organization trust, the hierarchical trust model can effectively detect malicious organizations from their node behaviors and has demonstrated good convergence in the distributed IoT environment.

Keywords Internet of Things; trust model; evidence theory; verifiable caching interaction digest schema; hierarchical architecture

---

收稿日期: 2011-08-30; **最终修改稿收到日期:** 2011-09-19. **本课题得到国家自然科学基金**(61100181,61173145)、**国家"八六三"高技术研究发展计划项目基金**(2011AA010705)**和国家"九七三"重点基础研究发展规划项目基金**(2011CB302605)**资助.****刘文懋,男,**1983**年生,博士研究生,主要研究方向为物联网和网络安全.** E-mail: liuwenmao@software.ict.ac.cn. **殷丽华,女,**1973**年生,博士,主要研究方向为网络安全.方滨兴,男,**1960**年生,博士,教授,博士生导师,中国工程院院士,主要研究领域为物联网和网络安全.张宏莉,女,**1973**年生,博士,教授,博士生导师,主要研究领域为网络信息安全、网络计算.**

1 引　言

物联网将现实中的物体通过虚拟的互联网连接起来,智能化的终端催生了大量新应用,其中重要的有组织协作、人员跟踪和物流定位等. 在上述应用中,物体通过 RFID 阅读器组成的接入网与应用服务器通信,为了保证交互是安全和可靠的,阅读器必须是可信节点,即机构需对与其标签交互的阅读器动态授权. 但由于物联网环境复杂,而阅读器也不稳定,机构无法直接推断未知阅读器的信任度,物联网中的信任授权问题尚未得到很好解决.

解决动态授权问题的前提是在机构、阅读器和标签间建立可靠的信任机制,然而物联网应用种类众多,互联网和阅读器网络环境存在较大差异,机构和阅读器有不同的信任特征,现在还没有一种方法可直接应用于物联网.

对此本文提出了一种层次化的信任机制,分离了异构环境中主体的不同信任需求. 根据证据理论的不足提出了一种可验证的缓存交互摘要方案(Verifiable Caching Interaction Digest schema, VCID) ; 在信任架构中构建了"现象可信-行为可信-节点可信-机构可信-授权可信"的环流,将阅读器信任和机构信誉很好地整合. 实验表明,提出的 VCID 方法比证据理论更能有效地检测出恶意的终端节点; 此外,层次化的信任架构具有很好的信任收敛性.

本文第 2 节介绍相关的工作; 第 3 节简要介绍物联网的应用模型; 第 4 节提出一种层次化的信任机制; 第 5 节分析影响信任机制的模型参数及所提信任机制的性能; 第 6 节进行简要总结.

2 相关工作

从众多信任相关的研究可知,信任[1]是一个主观模糊的概念,取决于主体、客体、环境和交互的因素,没有一种单一模型可以精确刻画主体的信任度,尽管已有一些工作尝试在不同网络中从理论上统一定义主体间的信任[2],但未给出具体的信任计算模型.

通常互联网中的机构是商业或政府机构,具有时间状态稳定且空间数量有限的特点,故可借鉴电子商务的信任管理. 通常电子商务的信任模型有两种: 一为基于身份的完全控制[3],即通过证书确认对方身份,并根据统一信任管理域中的策略进行授权,这种架构可直接管理网络中节点,计算较方便,但其身份和信任策略是固定的,不适合分布式环境; 二为基于信誉的信任管理[4],即主体在计算客体的信任度时,除使用自身经验外,还参考第三方对客体的评价. 在计算中可使用多种模型,如平均值[5]、贝叶斯系统[6]和向量机制[7]等. 信誉的建立和维护需要较长时间,符合机构稳定的特性,同时机制可通过协作,在分布式网络中快速检测出恶意节点,所以信誉体系可应用于互联网中的机构. 上述的计算模型中客体信誉的更新主要源于主体对于客体交互的反馈,但在物联网实际的应用中,机构间并无过多的交互,交互多发生在机构-阅读器和阅读器-标签中,机构信誉主要受其阅读器的行为的反馈,故使用信誉系统评估机构的信任时,需考虑相应机构下属阅读器的因素.

在阅读器网络中,存在大量节点增减或移动的现象,而基于身份的方法结构固定且计算开销较高,基于信誉的方法要求主体存活时间较长,均不适用于这种动态环境. 在 ad-hoc 网络的研究中,往往采用节点间协作,更新自己对各节点的信任值,最终推导出恶意节点. 所以阅读器主体在评估客体的信任值时,主要是考察其行为,故称为基于行为的信任[8]. 在具体的信任计算和节点状态推导过程中出现了各种模型,如文献[9]中使用的 D-S 证据理论,其根据与客体的交互,计算本地信任,并通过一个 TrustNet 网络结合其它节点对客体的本地信任进行合成,得到综合信任. 证据理论通常有较好的计算收敛性和可扩展性,但证据理论的 Dempster 合成存在冲突风险,因为正交合成考虑不同报告中的相同部分,如果有一个节点的报告与真实情况完全不同,合成结果也会受影响,特别是在有伪造报告节点的环境中,冲突尤为明显. 与证据理论类似,Song 等人[10]提出的基于贝叶斯决策理论模型的方法,其假设不具备模糊性,节点行为总是非是即否,在文献[11]中的实验表明这种确定性在快速变化的网络中,恶意事件报告率并不理想,且当信任阈值较小时,恶意事件误报率较高,且贝叶斯的先验概率及条件概率需要专家知识,往往很难确定. 此外,还有基于熵理论[12]的信任模型和基于云模型[13]的方法,都使用了不确定度描述信任,但如果主体和客体的信任路径过长,不确定度会被放大,故两者在多级信任链中收敛较慢; 基于半环代数理论的信任模型[14]也存在

同样的问题. 上述模型随着路径跳数增加,信任收敛速度变慢,可扩展性变差.

可见,每种信任模型也有不同的奖惩特性、收敛速度和可扩展能力,单一信任架构或信任计算模型并不能满足物联网中所有主体的信任需求. 本文的信任机制能满足不同主体的信任需求,同时有较快的信任收敛性及可扩展性.

3 物联网应用背景

信任架构和应用背景有密切的关系,本章主要介绍物联网具体的应用模型,指出模型中各主体的特点及其信任需求.

3.1 物联网应用模型

物联网现已在一些领域中使用,如物流公司在运输过程中读取物体上的编码,实时更新物体位置;智能手机使用 GPS 或移动基站获得当前位置,通过移动网络接入互联网,使用各种基于位置的服务(LBS),诸如此类. 物联网的应用众多,具体实现也不同,现以一类重要的物联网应用——物体或人员定位为例说明.

在定位应用中,家长可借助置于孩子身上的标签,通过服务器查询,实时获知孩子的位置以防止意外. 具体而言,机构在互联网中部署数据存储和查询服务,并在一些需监控的区域安放一定量的阅读器,阅读器间可通过 WIFI 相连,构成一个自主网络,并通过某些阅读器接入互联网;同时机构为每个孩子提供装有 RFID 标签的设备,这样当其运动到某个阅读器附近时,标签与阅读器交互,阅读器将时间、人员编号与标签信息通过阅读器网络传输到相关机构的服务器,后者将三元组保存;当家长登陆定位应用后,即可知自己孩子最近出现的位置(即阅读器编号所对应的范围).

针对物联网中快速移动、富信息和交易网络环境下的企业级应用,国际物品编码协会(EAN)和美国统一代码协会(UCC)两大标准化组织于 2003 年联合成立 EPCglobal 组织,已在开发对应的架构和标准;此外日本多家企业组成的泛在 ID 中心提出了泛在识别技术体系架构. 但这些标准化架构主要是针对商业级别的应用,没有考虑更一般化的应用. 尽管现在各物联网应用的模型尚未统一,但其主体通常都包含三类:机构、阅读器和物体,如图 1 所示. 机构包括商业组织和政府单位等,是物联网应用的发布和提供商. 机构在互联网中部署服务器,同时机构在各地理区域安装大量 RFID 阅读器,阅读器可读取附近的标签信息;物体上安装有 RFID 标签,故可与阅读器通信. 在本文中,"阅读器"和"节点"含义相同,"标签"和"物体"的含义相同,以下不作区分.

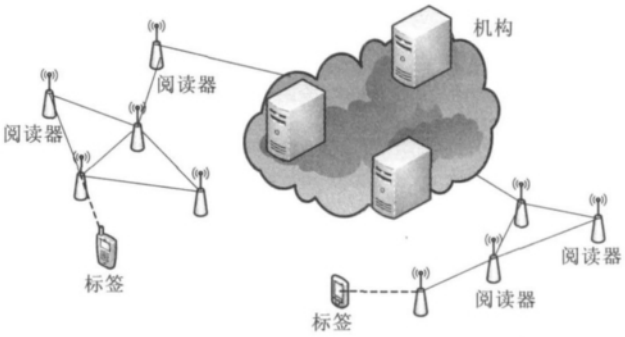

图 1 物联网的应用环境

3.2 主体的信任需求

对于一个物联网应用,其所涉及的各个环境有很大不同,环境中主体对信任的需求有较大差异. 在互联网中,机构数量较少,且状态长期稳定,故信任易管理. 而在阅读器环境中,由于成本和通信距离的限制,单个机构的阅读器部署远不能覆盖整个区域,所以多个机构的阅读器可互联组成阅读器网络,节点间是对等的;此外,节点随时可能新增、移动或失效,所以阅读器的信任缺乏全局性和稳定性. 在标签层面,就现有技术,无源 RFID 标签的运算性能较弱,故其信任机制设计受到较多限制.

阅读器可协作处理其他机构的标签,产生数据或指令的交互. 但由于机构和阅读器不在同一环境中,两者没有直接的信任关系,那么交互是否可获机构授权,则需一个分布式层次化的信任体系来解决.

4 物联网环境下的信任架构

在研究物联网环境的信任体系中,因各主体的规模、能力和稳定性不同,如果将所有信任关系置于一起讨论,会增加系统的复杂性,故可将信任体系分为三层:机构层、阅读器层和物体层,如图 2 所示. 在互联网的机构层使用长期的信誉处理机构的信任度,在阅读器层使用邻居监控节点的行为,在物体层使用缓存的交互信息检测节点与标签的交互. 同时,层与层之间也存在信任流传递,计算阅读器信任度可参考节点所属机构的信誉,而阅读器的行为也最终反馈为其所属机构的信誉值. 层次化的信任机制可简化物联网的信任交互复杂度,满足不同主体的信任需求.

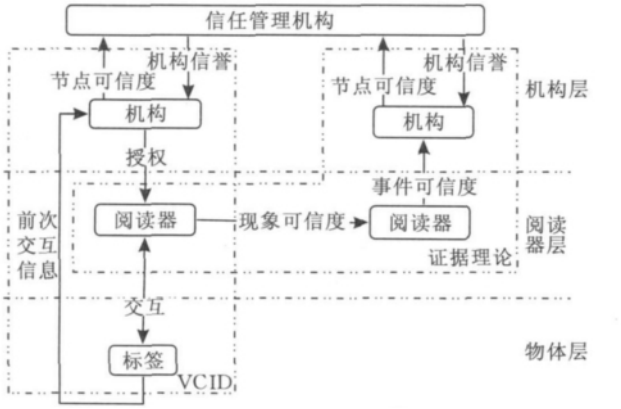

图 2　信任架构示意图

具体而言,机构的信誉受其阅读器的行为影响,阅读器的行为主要体现在与标签的交互中,即获授权的终端阅读器是否如实转发数据和执行命令,如表 1 所示,详细说明参见下两节.

表 1　阅读器信任的类型

信任类型	行为
授权信任 T_r	终端节点丢弃指令或数据 终端节点篡改指令或数据 终端节点重放或伪造指令或数据 终端节点自身信息正确性

4.1　阅读器信任

本节介绍基于证据理论推导阅读器信任的方法,并分析其缺陷,进而提出可验证缓存交互摘要的方法.

4.1.1　基于证据理论的信任推导

由于物联网中节点间的距离和通信并不可靠,节点对观察到的现象并不确定,同时分布式的环境缺乏专家知识,没有非常可靠的参数,所以借助证据理论进行信任推导,其要求比贝叶斯推导更松,容易得出一致的结论,它在处理"现象-行为-节点状态"的推导链中表现的性能较好,是一种有效的节点信任推导方法.

4.1.1.1　证据理论

证据理论(D-S theory)是一种不确定推理,它利用已有的知识和证据,推导假设的不确定度. 根据证据理论,判断阅读器的信任度,需要根据其行为进行分析. 用形式化表述,就是假设 H 为节点 r 不可信,支持这个假设的证据是节点 r 存在恶意行为,如 $B_1,B_2,\cdots,B_n$; 而判断这些恶意行为是否存在,同样需要根据 r 的邻居节点观察到的现象 $A_1,A_2,\cdots,A_m$ 进行推导,如此形成了一条"现象-行为-状态"的推导链.

4.1.1.2　恶意行为推导

表 2 中路由信任的每个类型可分为若干假设,然后定义推导出假设的现象与知识. 以"中间节点丢弃数据包"为例,分别定义了 4 个事件假设.

表 2　抛弃数据的推导规则

事件	事件假设	假设标记	知识(推导规则)	知识不确定度
终端节点丢弃数据包	节点未丢弃数据包,被邻居节点检测到	B_0	A_1 AND A_2 AND A_3 AND $A_5\rightarrow B_0$	CF_0
	节点未丢弃数据包,但未被邻居节点检测到	B_1	A_1 AND A_2 AND A_4 AND A_5 AND(A_6 OR A_8) $\rightarrow B_1$	CF_1
	节点丢弃数据包,因无法连接邻居节点	B_2	A_1 AND A_2 AND A_4 AND $A_9\rightarrow B_2$	CF_2
	节点恶意丢弃数据包	B_3	A_1 AND A_2 AND A_4 AND A_7 AND $A_5\rightarrow B_3$	CF_3

表 2 知识中的$\{A_i\}$是节点观测到的现象,具体如下:

A_1: T_n时刻,节点 N 收到数据包 P,且 P 的目的地为 N;

A_2: P 类型为数据,下一跳是标签 Q;

A_3: $[T_n,T_{n+1}]$ 间隔内,监控节点 X 收到节点 N 发出的数据包 C,目标为 Q;

A_4: $[T_n,T_{n+1}]$ 间隔内,X 未收到节点 N 发出的 C,目标为 Q;

A_5: C 与 P 的内容一致;

A_6: $[T_n,T_{n+1}]$ 间隔内,节点 N 运动较快;

A_7: $[T_n,T_{n+1}]$ 间隔内,节点 N 运动较慢;

A_8: 节点 N 和 X 距离较远;

A_9: $[T_n,T_{n+1}]$ 间隔内,节点 Q 运动较快.

根据表 2 的假设设定相应的推导规则,由节点观测到的现象推导出假设的可能性. 如当节点 X 在 T 时刻收到目的地为节点 N、类型为命令且对象为标签 T 的数据包,而在下一时刻没有观测到节点 N 发送相应命令,且发现标签 T 近期运动速度较快,则推断可能是因为标签运动速度过快导致节点没有发送命令. B_2的概率分配函数为

$$m(B_2)=\min\{CER(A_1),CER(A_2),CER(A_4),CER(A_9)\}CF_2.$$

$CER(A_i)$ 为各现象的不确定度,该事件的信任函数和似然函数分别为

$$Bel(B_2)=m(B_2),$$

$$Pl(B_2)=1-Bel(\neg B_2)=m(B_2)+m(D),$$

其中 $D=\{B_i\}$.

其它事件的推导类似,限于篇幅不作赘述,表 3 为其它事件列表.

表 3 阅读器网络的事件列表

假设类型	假设	标记
终端节点篡改数据包事件	节点未修改数据包	B_4
	节点未修改数据包,但网络传输错误	B_5
	节点工作异常,转发时修改数据包	B_6
	节点恶意修改数据包内容	B_7
终端节点伪造或重放数据包	节点未重放数据包,因前后两个数据包内容一致	B_8
	节点将数据包重放,转发到非目的机构	B_9

当邻居发现节点 R 异常事件后,需要向机构汇报. 由于一个事件可能被多个节点捕获,机构 O_A 定时检查,找到所有关于该事件的报告$\{T_{\text{event}}\}$,正交计算每个事件的综合信任度

$$m(B_i)=m_{X_1}(B_i)\oplus m_{X_2}(B_i)\oplus\cdots\oplus m_{X_n}(B_i),$$

$$T'_{\text{event}}=(m(B_i),B(B_i),P(B_i)),$$

并计算 B_i 不确定度 $CER(B_i)=Bel(B_i)+\dfrac{Pl(B_i)}{|D|}$.

4.1.2 基于可验证缓存交互摘要的信任评估

使用证据理论的前提是节点间的协作,邻居节点能够检测到物体与阅读器交互. 然而,物体与终端阅读器间采用 RFID 通信,距离较短,可能无法被其它节点获知; 此外阅读器分布过稀也可能导致检测效率低. 本文提出的可验证的前次交互摘要缓存的方法,在物体层保留终端节点使用授权的证据,在机构层验证物体提供的前次交互摘要,完成对授权的审核,避免了阅读器分布和标签通信距离的影响.

机构在获得阅读器的授权请求时,通过其所在机构的信誉判断是否允许预授权; 在通过授权后,为防止被滥用,机构需监控后续交互,具体过程为: 物体在交互时需缓存交互相关信息,在下次交互时提交给机构,这样机构就能确定该交互是否合理. 故可验证的缓存前次交互摘要方法包含 3 个步骤: 机构对交互的预授权、标签缓存交互摘要及机构对授权的审核.

机构对交互的预授权过程如图 3 所示. 阅读器 $R=R_{n-1}$ 发现标签 T 后,发送 TAG_HEADER_REQ 请求; T 则响应 TAG_HEADER_REP,包括编号 T、所属机构 O 等信息; R 随后向机构 O 发送授权请求 AUTH_REQ,当 O 确认 R 可信后通过授权,返回 AUTH_REP; R 获得授权后向 T 出示授权凭证; 最后 T 可与 R 进行数据或指令交互.

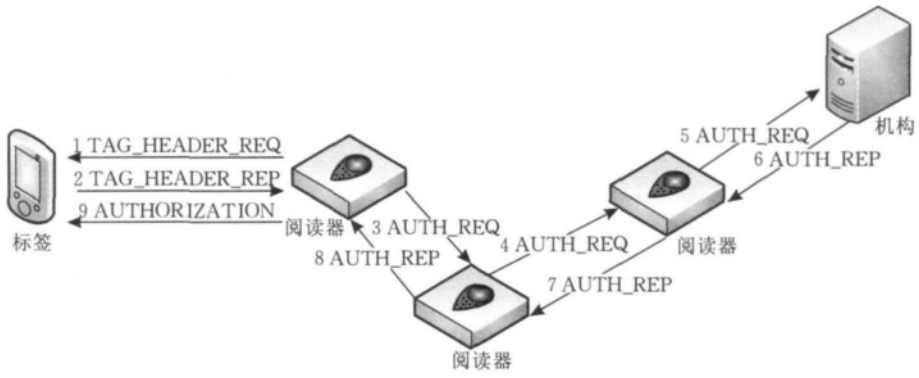

图 3 动态授权示意图

接着在时刻 T_{n-1},T 与 R_{n-1} 交互后,T 记录 $(R_{n-1},T_{n-1},op_{n-1})$,其中 op_{n-1} 为交互的操作类型等摘要. 在下个时刻 T_n,当 T 经过终端阅读器 R_n 并向机构 O 发送数据包 D 时,T 在数据包中添加时刻 T_{n-1} 的交互信息. 数据包变为 $M=(cert_T,rs_T,seq,R_{n-1},T_{n-1},op_{n-1},D,h)$,其中 $h=\text{hash}(cert_T,seq,R_{n-1},T_{n-1},op_{n-1},rs_T)$ 是字段组合的散列值,以保证 M 的完整性,$cert_T$ 为 T 的证书,rs_T 为 T 的随机数,seq 为 D 的序列号. 当 R_n 接收到 M 后,转发 $M=(cert_T,rs_T,seq,R_{n-1},T_{n-1},op_{n-1},D,h,cert_{R_n},rs_{R_n},h')$,其中 $h'=\text{hash}(cert_{R_n},rs_{R_n},h)$,$cert_{R_n}$ 和 rs_{R_n} 分别为 R_n 的证书和随机数. 故 M' 中包含了 R_n 的签名,中间阅读器在路由时会校验 h 和 h',如失败则拒绝转发,否则一直转发到 O.

最后,机构 O 为每个 T 维护一个散列表 $C=\{seq\rightarrow(M'-D)\}$; 同时 O 使用散列表 $B=\{R\rightarrow\{c\}\}$ 保存检测到的恶意授权节点信息,c 为每个异常事件的确信度. 当机构 O 收到 M' 后,检查是否有针对授权的恶意行为,如图 4 所示.

可验证缓存交互信息的方法保证机构能完成授权信任,说明如下:

(1) 由于中间节点进行数据包完整性检查,如果机构 O 对 h' 检查成功,则可保证 M' 从 R_n 发出后没有被修改,否则中间节点会抛弃校验失败的数据包,故可保证路由安全.

(2) 机构 O 校验 h,可保证 R_n 未篡改 M,故当标

```
if h′≠hash(cert_{R_n}, rs_{R_n}, h) ‖valid(cert_T) == false
    return
seq_max = max(seq, seq_max)
seq_min = min(seq, seq_min)
C[seq] = (cert_T, rs_T, seq, R_{n-1}, T_{n-1}, op_{n-1}, h)
if (currentTime % checkTimeout = 0)
    foreach (cert_T, rs_T, seq, R_{i-1}, T_{i-1}, op_{n-1}, h) ∈ values(C) and
            seq_min ≤ seq ≤ seq_max
        if (h ≠ hash(cert_T, seq, R_{n-1}, T_{n-1}, op_{n-1}, rs_T))
            B[R_n].add(c_1)
        else if (seq - 1 ∉ keys(C))
            B[R_{n-1}].add(c_2)
        else if (op_{n-1} is invalid)
            B[R_{n-1}].add(c_3)
        endif
    endforeach
endif
```

图 4　机构检查摘要过程

签数据经阅读器网络时,其完整性得到保证. 另 T 在数据包中添加随机数 rs_T 和时间戳 T_{n-1},可保证 R_n 无法重放或伪造 M.

(3) 阅读器与 T 交互前获得授权,路由的路径是通的,若机构在 C 中找不到 $seq-1$ 的键,则说明机构最终没有收到前次交互的数据包,很可能被 R_{n-1} 抛弃数据包,则 O 可标记 R_{n-1} 发生了一次恶意行为.

(4) 通过检验前一时刻的操作摘要 op_{n-1},机构可审核阅读器是否合理地使用授权,未进行非法操作.

然而这种方法存在漏报的风险,即相继交互的阅读器均为恶意节点或因网络变化发生数据包丢失的情况,则机构只知道发生数据包丢失事件,却无法获知阅读器的编号. 但由于 VCID 只根据确认的恶意事件降低机构的信誉,不会影响正常机构,所以是可接受的. 此外对授权的验证可设计为异或运算,这样能满足标签的计算能力.

可验证缓存交互摘要的方法需要保存摘要信息,一方面,标签在交互时会保存本次交互的摘要,而在下次交互时上传并舍弃,故只需保存一个摘要即可;另一方面,服务器需要保存时刻 $check\_timeout$ 内所有标签上传的摘要,尽管对于单个标签的存储和检查开销较小,但如果对于大规模的应用,可能需要使用并行存储和计算,事实上物联网的云计算研究已经有大量工作,本文不再赘述.

4.2　机构信任

在对阅读器授权前,需考察该阅读器所在机构的信任. 机构信任是稳定的,可由第三方机构对其信誉值的评价来获得,主要在机构层实现. 考虑到机构的数量远远小于阅读器和标签的数量,同时机构往往存在实体,是稳定可朔的,故提出基于信任管理机构的信任管理.

4.2.1　基于簇的信任管理

在分布式应用中,可按地理区域划分,形成可管理的单元簇. 簇内由一个信任管理机构 G 集中管理普通机构的信誉,G 根据簇内机构的报告,维护机构信誉; 普通机构参考 G 发布的机构信誉值,决定是否对该机构阅读器进行授权.

4.2.2　机构层的信任汇聚

机构 O_A 定期检查证据理论中的事件或 VCID 中的交互验证事件,当正交计算后发现节点 R 状态异常时,向 G 报告. 流程如图 5 所示.

1. 对 T_R 每个节点状态,设定信任阈值 $\{B_i^2\}$、似然阈值 $\{P_i^2\}$、授权异常阈值 t 和最大授权异常阈值 c
2. 将所有交互报告按报告节点聚合,得到 $L=\{R\rightarrow(\{T_{event}\},\{c\})\}$
   while $R\in L.keys$ do
3. 根据表 4 计算节点 R 的状态假设: $T_R=(m(C_i),B(C_i),P(C_i))$
4. 如果存在 $0\le i\le 3$,使得 $B(C_i)>B_i, P(C_i)>P_i$,确认 R 的状态 $C(R)=C_i$
5. 计算授权异常次数 $A'=\{\forall c_i\in\{c\}\mid c_i>C_0\}$, $count=|A'|$
6. 如果 $count>c$, $C(R)=C_0$
7. 如 R 异常则将 $(R,C(R),1)$ 添加到 E
   endwhile
8. O_A 向 G 发送节点异常报告 E

图 5　机构检查流程

表 4　节点状态的推导规则

节点状态	知识(推导规则)	假设标记	知识不确定度
节点恶意	B_3 OR B_7 OR $B_{13}\rightarrow C_0$	C_0	CF_0'
节点正常	B_0 AND B_1 AND B_4 AND B_5 AND $B_{10}\rightarrow C_1$	C_1	CF_1'
节点故障	B_6 OR $B_{11}\rightarrow C_2$	C_2	CF_2'
环境故障	B_2 OR $B_{12}\rightarrow C_3$	C_3	CF_3'

4.2.3　信任管理机构的信任管理

信任管理机构缓存接收到的机构的节点状态报告,并定时检查. 具体步骤如图 6 所示.

1. 将机构的报告按照节点散列,每个节点 $node$ 对应一个列表 $L_{node}=\{(R,C(R),n)\mid R=node\}$
2. 对 L_{node} 统计正常、节点故障、环境异常和节点恶意的报告数,将最大值的类型作为 R 的最终状态类型,最终生成所有节点状态列表 $L_0=\{(R,C(R))\}$
3. 根据 R 所在机构对 L_0 进行散列,每个机构 org 对应一个列表 $L_{org}=\{(R,C(R))\mid R\in org\}$
4. 对每个 L_{org} 统计正常报告、节点故障、环境异常和节点恶意的报告数,记为 $normal, nfaulty, efaulty, nmal$.
5. 计算更新遗忘机构恶意事件后的信誉值
   $T=\min(T_0-(1-T_{n-1})f, T_0)$
   f 为遗忘因子, T_0 为初始信誉, T_{n-1} 为前一时刻机构的信誉,获得机构的最终信誉值:
   $T_n=\max(T-P_{faulty}(nfaulty+efaulty)-P_{mal}\cdot nmal, 0)$
   P_{faulty} 是节点故障的惩罚因子, P_{mal} 是节点恶意的惩罚因子
6. G 公布 $\{T_n\}$

图 6　信任管理机构检查流程

4.3 机构-阅读器间信任传递

4.3.1 动态授权阅读器

当阅读器 R_n 需要对标签进行交互前，需获得标签所属机构 O_A 的授权. R_n 向 O_A 发送授权请求，O_A 收到阅读器 R_n 的请求后，计算阅读器 R_n 的信任度:

$$T(R_n) = \alpha T_{O_A}(R_n, O_B) + (1-\alpha) T_G(O_B),$$

其中 $T_{O_A}(R_n, O_B)$ 为直接信任，基于以往交互的经验，$T_G(O_B)$ 为间接信任，即 R_n 所在的机构 O_B 的信誉，可从信任管理机构 G 获得，α 是比重调节因子. 如 $T(R_n)$ 小于阈值 $T_{\min}$，则拒绝授权; 否则通过.

4.3.2 信任反馈

受信任模型的初始值和收敛性的影响，机构对节点的授权可能并不合理，信任反馈就成为修正错误的重要手段，机构从标签提供的交互摘要获得节点行为可信度，更新该节点授权，并反馈到其所在机构的信誉值. 如某授权节点存在故障或恶意行为时，节点报告到达机构 O，O 调低该节点的信任值 $T_n(R) = \delta T_{n-1}(R)$，如果 $T_n(R) < T_{\min}$，则机构撤销该授权.

5 实验结果

实验使用模拟进行验证，环境如图 7 所示. 其中的点以 O 开头为物体，以 R 开头为阅读器，颜色代表其所属机构，节点间的线表示两者在通信. 模拟采用事件驱动. 下面实验中如不附说明，则环境中的阅读器网络面积为 $1200 \times 900\ m^2$，阅读器节点数量为 80，通信距离为 200 m，标签的通信距离为 60 m，模拟时间为 200 s. 以下分析不稳定阅读器对恶意事件发生的影响，以及析标签通信距离对事件检测的影响，并对比证据理论和 VCID 的收敛效率性能.

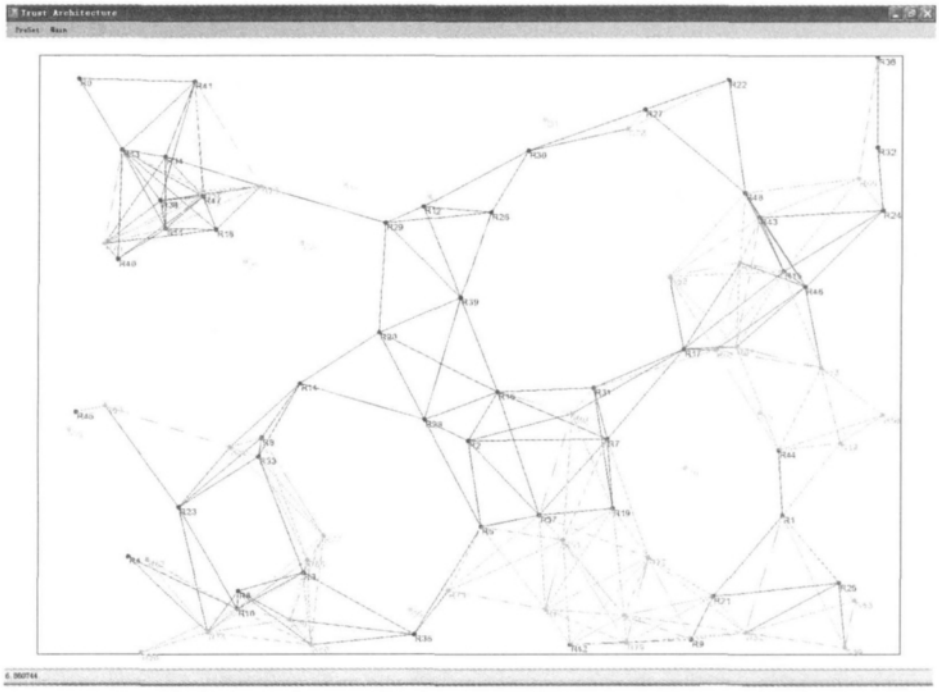

图 7 模拟环境

5.1 不稳定阅读器的影响

阅读器网络是动态的，不稳定节点会改变网络拓扑和交互时间，这些不稳定的因素会对恶意事件的识别产生影响. 设计使用基于证据理论方法的两个实验节点运动研究信任机构的性能. 第 1 个实验(图 8)中节点均静止不动，而第 2 个(图 9)中 30% 的节点以 10 m/s 的速度运动. 图中方点为发生的恶意事件，菱形点为检测到的恶意事件，如某时刻无恶意事件或未检测到的事件则不标，我们将某刻机构的信誉值乘 10，也标于图中比较.

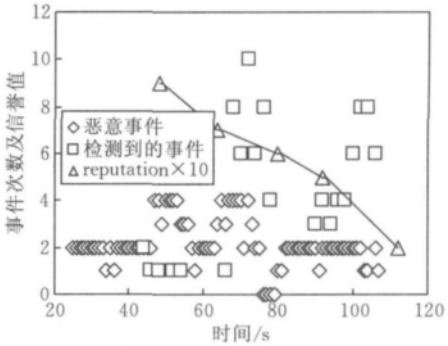

图 8 0% 运动节点环境中恶意事件与检测事件比较

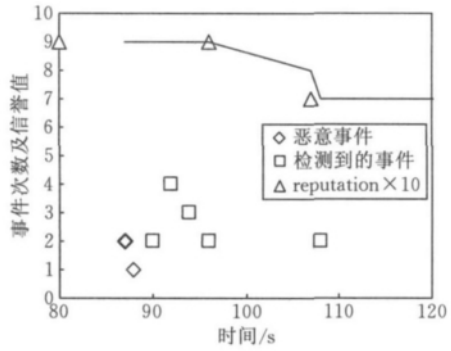

图 9　30% 运动节点环境中恶意事件与检测事件比较

可见,当恶意节点运动较快时,与标签的接触较少,恶意事件也少,当节点全部静止时,共有 242 个恶意事件,而当 30% 节点运动时,仅有 3 个. 可见节点运动对恶意事件的发生有很大影响. 但本实验中标签距离较长,故仅出现的 3 个恶意事件都被检测到,下个实验将分析标签通信距离对恶意事件检测的影响.

5.2　标签通信距离的影响

标签的通信距离对恶意事件检测率也有影响. 不同的 RFID 标签,如无源标签和有源标签的通信距离不同,标签的通信距离直接决定了能监听该标签与终端阅读器交互的邻居节点数量.

有 3 组实验,标签的通信距离分别为 30 m、60 m 和 90 m,机构的信誉变化参见图 10. 当标签的通信距离为 30 m 时,机构的信誉值没有变化,而标签的通信距离增加至 60 m 时,机构信誉值降低,在一段时间后没检测到恶意报告开始回升; 而当标签的通信距离增加到 90 m 时,机构信誉值迅速降低至最低值,一直不变.

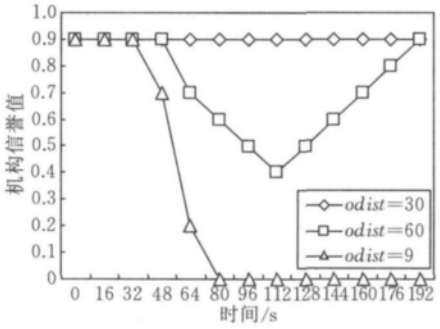

图 10　标签通信距离对机构信誉的影响

设标签通信距离为 $odist$,阅读器数量为 n,阅读器网络面积为 $S = w \cdot h$,每个标签平均遇到的阅读器数目为 $\overline{N} = \dfrac{odist^2 \cdot \pi \cdot n}{w \cdot h}$. 当 $odist = 30$ m 时,$\overline{N} = 0.21$,此时标签与阅读器时,很难遇到其它阅读器进行监控,可见证据理论在较短的标签通信距离条件下性能较差.

5.3　证据理论的收敛速度

对于层次化的信任机制,底层的节点恶意事件汇聚到顶层的机构信誉,信任收敛速度是重要的评价标准. 为了评估路由信任收敛性,我们将阅读器网络面积设为 800×600 m^2,其它不变,实验结果如图 11 所示.

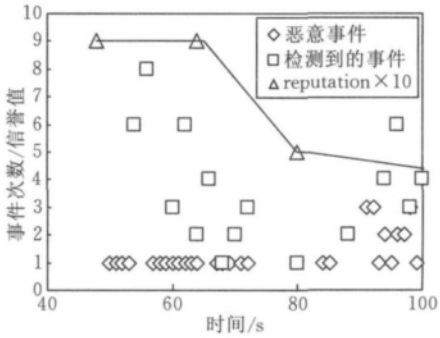

图 11　D-S 方法的收敛速度

机构的信誉初始值为 0.9,在 $t = 48$ s 前,无恶意事件,而后开始出现,如在 $t = 50$ s 后中连续出现 3 个丢弃事件,过了 $\Delta t = \max(recv\_timeout, check\_timeout)$ 后,即下个检查时刻或接收数据包超时的最大值,邻居节点检测到该恶意事件,故 $t = 55$ s 时,出现 6 个恶意事件报告,而下一秒有 8 个报告. 因为一个恶意事件可被多个节点捕获,故对应多个报告. 后恶意报告向上汇聚,但此时机构的信誉值还未得到更新,故当 $t = 64$ s 时,机构的信誉值还是 0.9. 信任管理机构的下个检查时刻 $t = 80$ s 后,恶意机构的信誉开始降低,并随报告增加继续降低. 可见信任层次结构可在较短的时间内,把底层的节点行为反馈到机构的信任上. 应用规模越大,节点也多,或节点的恶意行为越多,则信任反馈越快.

5.4　VCID 的收敛速度

在授权信任中,使用缓存前次交互摘要的方式检测恶意终端节点,这种方法即便在阅读器密度不大的环境中,也能有效地检测出恶意节点. 我们设计了 3 组实验,第 1 和第 2 组分别使用证据理论和贝叶斯决策,通过节点检测邻居节点对标签的行为,推导恶意事件; 第 3 组采用验证缓存交互信息的方法. 每组均选取 40、60 和 80 个节点,一共 9 个实验,结果如图 12 所示.

在采用证据理论的实验中,由于节点间较稀疏,无法检测到恶意事件,所以当节点数为 40 和 60 时,恶意机构的信誉始终不变,当节点数为 80 时,信誉值才开始下降; 采用贝叶斯决策的结果与证据理论类似,但是检测成功率降低,这与文献 [11] 的实验

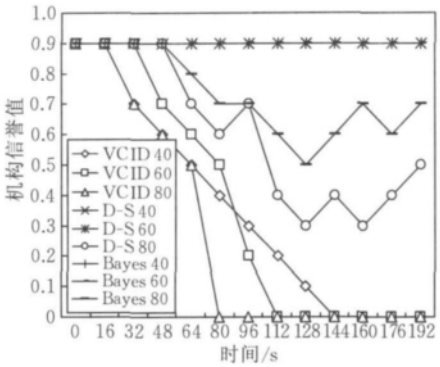

图 12 VCID 的收敛速度

结果一致. 其它如云模型和基于熵模型的方法也都是通过捕获邻居节点的行为来调整节点的信任度，在检测阅读器-标签的交互中会受标签短距通信的限制，故对机构信誉的影响与这两组实验结果相似.

相反，在使用 VCID 的实验中，即使节点数为 40，也能及时检测到恶意事件. 此后随着密度增加，恶意节点接触标签的次数增加，恶意机构的信誉值下降更快. 可见采用验证缓存前次交互信息的方法有较快的收敛速度，不受节点部署的影响.

6 结论和进一步研究

本文首先分析了物联网中应用的特点与不同主体的信任需求，然后提出了一种层次化的信任机制，分离机构信誉和阅读器信任. 之后根据阅读器特点提出了改进的证据理论方法，可推导阅读器的路由信任. 但实验表明当标签通信距离较短的条件下，当使用现有的信任模型时，邻居节点很难监控到终端节点与标签的交互; 本文提出了一种新的可验证缓存前次交互摘要的方法，交互的摘要被物体保存，并在下次交互时被机构验证，从而实现了阅读器的授权信任. 此外，阅读器的行为信任汇聚到机构的信誉中; 机构也通过信誉参考对节点的授权，建立了“现象可信度-行为可信度-节点可信度-机构可信度”的信任流. 该信任模型具有较快的收敛性和可扩展性，适合分布式、大规模的物联网应用.

实验表明了证据理论和 VCID 方法都适用于不稳定的阅读器网络，但在通信距离较近的标签-终端阅读器环境中，VCID 明显有更优的性能. 本文层次化的架构使阅读器信任收敛较快，有很好的性能.

本文讨论了终端节点与标签交互中的授权信任，但没涉及中间节点在路由数据包时的信任，在今后研究中，我们将研究结合授权信任和路由信任的信任架构.

参 考 文 献

[1] McKnight D H, Chervany N L. What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. International Journal of Electronic Commerce, 2001, 6(2): 35-59

[2] Carbone M, Nielsen M, Sassone V. A formal model for trust in dynamic networks//Proceedings of the Software Engineering and Formal Methods Conference. Brisbane, Australia, 2003: 54-61

[3] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management//Proceedings of the 1996 IEEE Symposium on Security and Privacy, 1996: 164-173

[4] Resnick P, Kuwabara K, Zeckhauser R, Friedman E. Reputation systems. Communications of the ACM, 2000, 43(12): 45-48

[5] Resnick P. Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system. The Economics of the Internet and E-Commerce, Advances in Applied Microeconomics, 2002, 11: 127-157

[6] Josang A. The beta reputation system//Proceedings of the 15th Bled Electronic Commerce Conference. Beld, Slovenia, 2002: 1-14

[7] Jameel H, Kalim U, Sajjad A. A trust model for ubiquitous systems based on vectors of trust values//Proceedings of the 7th IEEE International Symposium on Multimedia (ISM'05). Irvine, USA, 2005: 674-679

[8] Huang L, Li L, Tan Q. Behavior-based trust in wireless sensor network//Proceedings of the Advanced Web and Network Technologies, and Applications Conference. Berlin, Germany, 2006: 214-223

[9] Yu B. An evidential model of distributed reputation management//Proceedings of the 1st International Joint Conference on Autonomous Agents and Multiagent Systems. Bologna, Italy, 2002: 294-301

[10] Song S, Hwang K, Macwan M. Fuzzy trust integration for security enforcement in grid computing//Proceedings of the IFIP International Conference on Network and Parallel Computing. Wuhan, China, 2004: 9-21

[11] Raya M, Papadimitratos P, Gligor V D, Hubaux J P. On data-centric trust establishment in ephemeral Ad Hoc networks//Proceedings of the 2008 IEEE INFOCOM, the 27th Conference on Computer Communications. Phoenix, USA, 2008: 1238-1246

[12] Liu J R. Trust modeling and evaluation in ad hoc networks//Proceedings of the IEEE Global Telecommunications Conference. St. Louis, USA, 2005: 1862-1867

[13] He R, Niu J, Zhang G. CBTM: A trust model with uncertainty quantification//Proceedings of the Parallel and Distributed Processing and Applications. Berlin, Germany, 2005: 541-552

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

LIU Wen-Mao, born in 1983, Ph.D. candidate. His research interests include Internet of Things and network security, etc.

YIN Li-Hua, born in 1973, Ph. D.. Her research interests include network security, etc.

FANG Bin-Xing, born in 1950, Ph.D., professor, Ph. D. supervisor, member of Chinese Academy of Engineering. His research interests include Internet of Things and network security, etc.

ZHANG Hong-Li, born in 1973, Ph. D., professor, Ph. D. supervisor. Her research interests include information security and network computing.

Background

This paper is related to the trust model of Internet of Things (IoT) environment. Internet of Things is becoming one of the most promising technologies in modern life and commercial society, the security of applications is gaining more attention, especially the peer trust should be determined before interaction. However, trust is a subjective and fuzzy concept, it's hard to depict subject trust accurately without detailed conditions. A large amount of trust architecture in e-commerce and ad-hoc network scenarios have been proposed, and many computing model such as Bayes decision model, Dempster-Shafer (D-S) theory and cloud model perform well in their environments. However, the IoT environments are complicated and subjects have different levels of trust requirements, none of the current schemas can be directly applied for the IoT environment.

In this paper, we propose a hierarchical trust model, in which a cross-layer trust loop flow is established through the following levels of trust: phenomenon, event, node, organization and authorizing, therefore short-term reader trust is derived from the phenomenon and event trust distributively, while long-term organization trust is derived from reputation and accumulative reader trust in a centralized fashion. Specifically, an improved evidence theory is introduced to deduce unstable reader-reader trust, a verifiable caching interaction digest (VCID) schema is introduced for the purposes of monitoring object-reader interaction. Even if the tag communication range is short, malicious terminal reader can be detected by the organizations after checking the interaction digest. With simulations analyzing the impact of abnormal node ratio, node density, and tag communication range on the organization trust, the hierarchical trust model can effectively detect malicious organizations from their node behaviors and has demonstrated good convergence in the distributed IoT environment.

This work is supported by the National Natural Science Foundation of China (61100181, 61173145), National Grand Fundamental Research 973 Program of China (2011CB302605) and the National High Technology Research and Development Program(863 Program) of China (2011AA010705).