物联网安全与信任机制研究

杨　乐　谢游洋

(1.秦皇岛市交通运输局　河北秦皇岛　066000;2. 秦皇岛风日和科技有限公司　河北秦皇岛　066000)

【摘　要】本文首先分析了物联网中不同物体的对信任的需要和要求,随后提出解决这个问题的方法,即分开来看机构的信誉和阅读器的信任。阅读器自然会有一些基本属性,我们以此为基础,提出论据,对路由信任进行四个假设,结果证明,只有在相隔很远时才能通信。于是,在文章中提出了另一个方法 物体将摘要保存,下次交互时,机构将其验证,从而授以阅读器的信任权限。

【关键词】物联网安全 ;信任机制 ;证据理论 ;动态运动阅读器

Things Security and Trust Mechanism

Yang Le　Xie You-yang

(1.Qinhuangdao Communications and Transportation Department　HebeiQinhuangdao　066000;

2.Qinhuangdao Wind and Sun Technology Co. Ltd　HebeiQinhuangdao　066000)

【Abstract】This paper analyzes the different objects of things on trust needs and requirements, and then propose solutions to this problem, which separated from the agency's credibility and the trust of the reader. Reader will naturally have some basic properties, we as a basis, the arguments put forward, the routing trust for four assumptions, the results show that only very far apart in order to communicate. So, we put forward in the article another way: theabstract object saved, the next interaction, the agency will verify its ordergranting permission to the reader's trust.

【Keywords】internet of things safety; trustmodel; evidencetheory; dynamic movement reader

1　前言

1999 年,在中国出现了“物联网”,随社会进步,成为新型技术。物联网顾名思义就是将任何物体连入互联网,它是通过一些信息传感设备将物体连入互联网的,如红外感应器、通过射频识别(RFID)、全球定位系统等信息传感设备,通过这些传感设备按照规定的协议将信息与网络交换,实现对任何物体的智能化管理、跟踪、识别、定位和监控等操作。

但由于物联网构成复杂,我们没有办法有效监控,而且数量太多,设备也很多等,所以存在了一些安全问题。比如说,信号泄漏与干扰、节点安全、数据融合与安全、数据传送安全、应用安全等。文中提出的信任架构,满足了不同主体对信任的需求,将机构信誉和阅读器信任隔离,通过证据理论推导动态运动阅读器的信任。

2　相应机构下属阅读器的因素

电子商务有一种信任模型,一般情况下有两种:一是以身份为基础的全部控制;二是以信誉为基础的信任管理。而有多种模型可在计算机中使用,比如向量机制、贝叶斯系统等。信誉需要建立和维护,这就必须花费很长时间,与机构稳定相对应,所以信誉体系可以在互联网中应用。但物联网在实际应用里,机构 - 阅读器和阅读器 - 标签之间发生的很多交互,所以通过阅读器的行为观察出机构信誉,阅读器成了不得不考虑的原因。

阅读器互相联系,形成网络,有许多结点的位置和数量会改变,但以信任为基础的方法要求主体存活比较长的时间,并且基于身份的方法不仅计算开销高,而且

结构固定,所以都不能用在这样有波动的环境。有的网络的探究是靠所有节点的一起作用,来改变其对别的节点的信任,最后找出不友好的节点。所以阅读器适合应用以行为为基础的信任。

推导结点的状态和和计算结点信任值有各种各样的模型,如 D—S 证据理论,这个理论的计算收敛性和延伸性比较好, 但是其中的 Dempster 合成有矛盾的危险,报告中有相同成分,假设实际情况与某个结点的报告没有一处相同,会影响到合成的结果,尤其是报告节点是伪造的,矛盾非常明显。再比如说,基于贝叶斯决策理论模型的方法,节点行为不是是就是否,因此在快速变化的网络中,恶意事件报告率也就不理想了。另一方面,贝叶斯研究出的概率需要专家解答,一般我们无法明确结论。可如果客体和主体相隔很远,就越不能明确结论,所以相隔越远,收敛越慢;基可见单一信任计算机模型或信任结构不能满足物联网中所有主体对信任的需要和要求。

3 阅读器和机构无法直接信任

生活中很多地方用得到物联网,但各应用之间有所不同,所以各应用对信任的标准互不相同。在互联网里,之所以信任容易管理是因为机构数量较少,而且状态长期稳定。但是在阅读器环境中有所不同,因为通信互相之间的距离和成本受到限制,所以阅读器不能遍布每个角落部署不,所以各个阅读器之间相互联系,从而形成了阅读器网络,并且结点之间一一对应相等。又因为结点随时可能改变位置,失去作用,数量增加,所以阅读器的信任不稳定而且受区域限制。

阅读器之间合作处理其他机构的标签,可以出现一些数据或者交换指令。但是,阅读器和机构所在环境不同,互相之间不能直接信任,那么具有分布式层次化的特点的信任体系来解决。

4 信任结构图

在物联网环境的信任结构中, 因为各个部分的大小、稳定程度和功能不太一样,如果我们把结构中的各个关系放在一起的话,系统会比起以前复杂,所以信任建构中的关系分成三个层次:机构层、物体层和阅读器层。长期的信誉处理机构的信任度使用在机构层,缓存的交互信息检测节点与标签的交互使用在物体层,邻居监控节点的行为使用在阅读器层。信任像流水在各个层之间传递,得到阅读器的信任度就需要参照结点的信誉

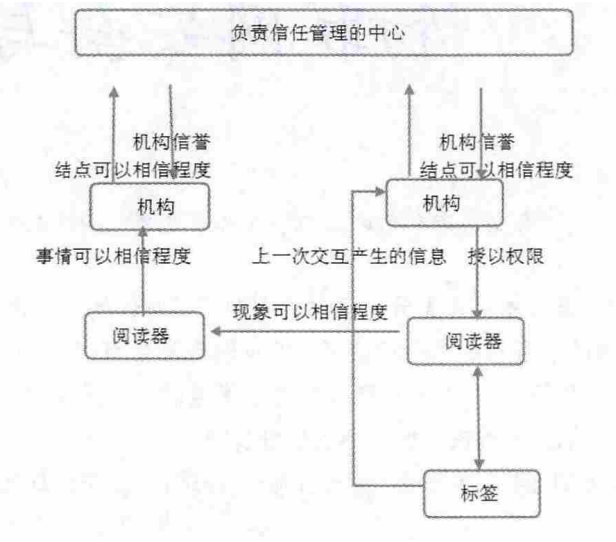

图 1 信任结构图

了,得到信誉值就要看阅读器有什么样的行为。有层次的信任机构制度可以使网络的信任变得简单,从而使不同事物的对信任的需求得到满足。

4.1 根据证据理论推导信任

因为在物联网中,结点与结点之间没有什么可靠的东西,分布式的环境又没多少专家知识,而且节点不能确定观察到的现象,也就只能通过证据理论来推导出信任,贝叶斯推导比它都严格,所以很轻松就能得出想要的结论,它是一种有效的节点信任推导方法,在处理“现象 - 行为 - 节点状态”的推导链中表现的性能也较好。

4.2 证据理论

证据理论并不是确定推导, 我们查看现有的资料,来证明假设是不一定的。通过各种论据,得出阅读器的可信任的结果,分析它的功能。抽象的说,如果结点 p 不能相信,结点 p 存在不友好的行为能支持假设。如 A1,A2,…,An;判断这些不友好行为的有无,也需要查看 p 的旁边的结点的现象 B1,B2,…,Bm,同时出现“现象 - 功能 - 状态”链。

4.3 不友好行为的推导

依据路由信任的“中间结点放弃数据包”,有四种假设:①节点未丢弃数据包,被邻居节点检测到,记为 p0;②节点未丢弃数据包,但未被邻居节点检测到,记为 p1;③节点丢弃数据包,因无法连接邻居节点,记为 p2;④节点恶意丢弃数据包,记为 p3。

①的推导规则:B1 AND B2 AND B3 AND B5→A0; ②的推导规则:B1 AND B2 AND B4 AND B5 AND

(B6 OR B8)→A1；③的推导规则:B1 AND B2 AND B4 AND B9→A2；④的推导规则:B1 AND B2 AND B4 AND B7 AND B5→A3。①的知识不确定度为 CF0;②的知识不确定度为 CF1;③的知识不确定度为 CF2④的知识不确定度为 CF3。根据推到法则,我们可以观察结点有什么现象,得出哪种假设可能成立。打个比方,结点 X 在 T 时间接收到的数据包在节点 N、标签是 T 并且命令类型,但接下来节点 N 没有发出与之匹配的命令,而且标签 T 近期比以前运动的快，所以可以假设是这个原因使结点没有发出与之匹配的命令,则 A2 的概率分配函数为:

$$m(A2)=\min\{CER(B1),CER(B2),CER(B4),CER(B9)\}CF2。$$

CER(Bi)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:

$$Bel(A2)=m(A2),Pl(A2)=1-Bel(A2)=m(A2)+m(D),$$

其中 D={Ai}。

其它推导类似。

4.4 标签机构授以阅读器权限

阅读器 Rn 和标签需要交互,但是在此之前,含该标签的机构 OA 需要对其授以权限。阅读器发出请求,OA 接收之后,就开始计算其的信任值:$T(Rn)=\alpha TOA(Rn,OB)+(1-\alpha)TG(OB)$,其中直接信任是 TOA(Rn,OB),间接信任是 TG(OB),即含有 Rn 的机构 OB 的信誉,可以通过 G 获得,α 是比重不协调因子。如果 T(Rn)< 阈值 Tmin,就不授以权限;否则授以权限。

4.5 修正错误的手段

机构对结点授以权限可能存在错误,修正错误靠的是信任将信息反馈出来，标签会提供一些交互信息,因此机构获得可信度,结点的授权更加完善。然后机构的信誉值将其反应。如果被授以权限的结点发生故障或者有不友好的行为，借点就会通知机构 O,O 降低信任值 $Tn(R)=\delta Tn-1(R)$,如果 Tn(R)＜Tmin,机构就会撤销该授权。

4.6 VCID 的收敛速度

用缓存前次交互摘要的方法检测不友好的最后一个结点能有效的检测出不友好结点,如果阅读器的密度小也能检测。我们设计了三组实验,根据检测邻居节点对标签的行为,推导恶意事件。在证据理论实验中,结点数量少,距离大,所以无法检测到不友好事件,当结点数是 80 时,信誉值才有所下降,采用贝叶斯的决策的实验检测成功率低。

云模型和基于熵模型的方法在检测阅读器 - 标签的交汇中会被标签短距离通信限制。但是在 VCID 的实验中，如果结点数量是 40，不友好事件也能被检测到。随阅读器密度的增加,不友好结点碰到标签的次数随之增加,而不友好机构的信誉值会立刻下滑。

5 结束语

物联网的存在是我们便利了很多。一些复杂、危险、机械的工作可以通过物联网来完成,而攻击者很容易就能接触到物联网机器、感知节点从而造成了破坏。感知节点多种多样,却无法拥有安全保护能力。物体通过接入网与应用服务器通信,阅读器由 RFID 阅读器组成,若想得到安全保障,机构必须对标签授以权限。

本文通过各种模型的不足提出了一个缓存交互摘要方案。通过“现象得到信任 - 功能得到信 - 结点得到可信 - 机构得到信任 - 授以权限得到信任”将机构的信誉值和阅读器的信任度结合在一起。

参考文献

[1] 彭春燕. 基于物联网的安全构架 [J]. 网络安全技术与应用,2011,(5):13–14.

[2] 聂学武,张永胜.物联网安全问题及其对策研究[J].计算机安全,2010,(11):4–5.

[3] 石磊.网络可信评估仿真实验模型的设计与研究[D].河北大学,2010 年.

[4] 蒋建.面向网络环境的信息安全对抗理论及关键技术研究[D].中国科学院研究生院(软件研究所),2004 年.

作者简介：

杨乐(1980–),男,汉族,本科,电子工程工程师;主要研究方向和关注领域:通信、计算机及信息化建设维护。

谢游洋(1981–),女,汉族,电子工程助理工程师;主要研究方向和关注领域:电子设备及新能源开发及应用。