基于贝叶斯网络的量化信任评估方法

林 青[1],戴慧珺[2],任德旺[2]
(1.西安培华学院,陕西 西安 710125;
2.西安交通大学,陕西 西安 710049)

摘 要: 随着云计算的不断发展,物联网逐步涉及各行各业,其中包含大量的感知信息、个人或群体的隐私信息。此外,物联网最直接、最严峻的安全隐患是网络中参与信息采集与数据融合的恶意节点,以合法身份发送虚假信息、窃听发送指令等,所以保障物联网安全刻不容缓,尤其是确保节点之间的信任关系。为决定新节点是否可以加入网络,以及排除网络中已有的恶意节点,利用贝叶斯网络量化评估节点间的信任概率,通过节点信任状态分级,融合先验信任概率,分配信任条件概率,推理预测评估节点的信任概率,确定信任等级。通过仿真实验,结果证明了该评估方法的有效性,并在一定程度上降低了评估的主观性。

关键词: 贝叶斯网络;信任评估;条件概率分配;物联网
中图分类号: TP309.2 **文献标识码:** A **文章编号:** 1673-629X(2016)12-0132-05
doi:10.3969/j.issn.1673-629X.2016.12.029

A Quantitative Trust Assessment Method Based on Bayesian Network

LIN Qing[1],DAI Hui-jun[2],REN De-wang[2]
(1.Xi'an Peihua University,Xi'an 710125,China;
2.Xi´an Jiaotong University,Xi'an 710049,China)

Abstract: With the continuous development of cloud computing,Internet of Things (IoT) gradually involves in all walks of life,which contains large amounts of sensitive information,privacy information.In addition,the most direct and serious security risks are malicious nodes involving in information acquisition and data fusion,which send false information and eavesdrop instructions sent with legal identity.Therefore,it is greatly urgent to ensure the security of IoT,especially trust relationship among nodes.In order to determine whether to allow the new node to join the network and to remove the existing malicious nodes,a quantitative trust assessment method is proposed based on Bayesian network.Through classification of trust status of nodes,integration of trust priori probability and allocation of conditional probability,the trust probability of assessment nodes could be predicted and inference to determine the trust level.The simulation results show the effectiveness of assessment method and that the assessment subjectivity can be reduced to some extent.

Key words: Bayesian network;trust assessment;conditional probability allocation;Internet of Thing

0 引 言

物联网已经在车联网、铁路安全防灾等基础领域得到了广泛应用,但是物联网是一个开放的环境,大多设备无人监管,极易遭受恶意攻击。恶意攻击不仅包括外界对设备的破坏,而且包含网络中潜藏的恶意节点,以合法的身份发起内部攻击。所以,节点相互间的信任问题成为关键。目前,保障感知信息安全的方法主要有两种:一种是利用感知节点的相似性综合处理多个数据,以排除恶意节点发送的虚假信息;另一种是为保证原始数据的真实性,采用数据加密认证技术确保数据安全[1-2]。

在进行数据融合之前,需要对节点行为进行检测和信任评估,以确保数据的真实性和网络的安全性。关于建立节点信任模型和评估节点的可信度,已提出了众多信任评估模型,比如,层次化的信任评估模型[3-4]、分布式行为信任评估模型[5-6]、基于角色的信任评估模型[7-8]、周期性节点行为信任评估模型[9-10]等,在异常节点检测和确定节点信任度方面起到了重

收稿日期: 2016-01-28 **修回日期:** 2016-05-11 **网络出版时间:** 2016-10-24
基金项目: 2015 陕西省教育科学研究基金项目(15JK2091);西安培华学院课题资助项目(PHKT16090)
作者简介: 林 青(1979-),女,讲师,硕士,研究方向为数据挖掘与大数据;任德旺(1989-),男,西安交通大学电子与信息工程学院博士研究生,研究方向:云计算与信息安全。
网络出版地址: http://www.cnki.net/kcms/detail/61.1450.TP.20161024.1117.066.html

要作用。

文献[8]中提出一种基于节点行为检测的信任评估模型及异常行为检测算法,将直接信任值、统计信任值与推荐信任值 3 种信任因子作为异常行为检测算法的输入,计算节点行为的综合信任值并判断网络是否存在恶意攻击。贝叶斯网络作为一种有力的推理预测工具,预测行为信任,文献[9]中提出的机制不仅可以预测单属性的行为信任等级,而且可以预测多属性条件下的行为信任等级。文献[11]中利用贝叶斯网络处理不确定数据的优势,提出融合室内数据的模型,以得到需要的正确数据。贝叶斯网络在预测多因素作用下的趋势变化方面有很大优势,并广泛应用于因果数据挖掘,所以结合贝叶斯网络的众多优点,用于量化评估物联网节点的信任度,以保障物联网的安全。然而贝叶斯网络推理预测的核心是先验概率的可靠性和条件概率的合理性,先验概率主要通过统计分析和专家意见得到;迭代学习是条件概率表生成的主要方法,但是当数据不足时,大多采用主观判断,并且当节点数目增多时,分配的工作量非常大。

为此,文中利用贝叶斯网络评估网络节点的信任概率,通过对网络节点状态分级,利用证据理论融合先验信任概率,并提出一种节点状态划分相同情况下的条件概率分配规则,简单灵活。与信任阈值进行了比较,判断节点是否可信。

1　相关理论

1.1　贝叶斯理论

贝叶斯网络是利用有向无环图和条件概率表表示变量交互的概率模型,由节点和连接组成,节点表示变量而连接表示变量间的因果关系。节点和连接定义了网络的定性部分,而网络的定量部分由相关节点的条件概率组成。条件概率是给定父节点各状态组合情况下独立变量的概率。网络节点由根节点、中间节点、叶节点组成。给定根节点的概率和中间节点的条件概率,就可以计算叶节点的概率。边缘概率给出了事件 A 的概率是相互排斥事件 $B_1,B_2,\cdots,B_n$ 和 A 的联合概率之和[12-14]。

$$P(A)=\sum_i P(A_i^B) \tag{1}$$

根据乘法规则,式(1)可以写为条件概率:

$$P(A)=\sum_i P(A\mid B_i)P(B_i) \tag{2}$$

每个节点状态的概率通过边缘化其父节点状态计算得来。在证据给定的情况下,后验概率可以通过贝叶斯理论计算:

$$P(A\mid B)=\frac{P(B\mid A)P(A)}{P(B)} \tag{3}$$

式(3)可以用边缘概率表示如下:

$$P(A\mid B)=\frac{\sum_C P(A,B,C)}{\sum_A\sum_C P(A,B,C)} \tag{4}$$

1.2　证据理论

贝叶斯网络节点的先验概率的获得主要通过历史数据统计分析而来,不同的统计方式之间存在误差;但当数据不足或缺失时,多采用多专家意见,但多专家意见存在不确定性和偏见,导致数据的可靠性会降低。所以,可以将多个专家的意见通过证据理论结合起来,增加数据的可靠性[15]。

针对每个节点,分配三种状态:{Yes}、{No}、{Yes,No}。通过专家确定每种状态的可信度 $b(p_i)$:

$$\begin{aligned} &b(p_i)\rightarrow [0,1]\\ &b(\varphi)=0\\ &\sum_{p_i\subseteq P} b(p_i)=1 \end{aligned} \tag{5}$$

根据 DST 联合规则,把多个证据结合起来。假设有 n 个不同专家数据集,联合规则为:

$$b_{1-n}=b_1\oplus b_2\oplus\cdots\oplus b_n \tag{6}$$

为了融合统一多个证据,降低证据间的冲突,使用标准化元素 $(1-k)$。由于 n 个证据集之间相互独立,这种联合可以通过“与”操作完成。假设 $b_1(p_a)$ 和 $b_2(p_b)$ 是对相同事件的两组独立的证据集,根据 DST 联合规则组合两组证据,如式(7)所示:

$$[b_1\oplus b_2](p_i)=\begin{cases}0 & p_i=\varphi\\ \dfrac{\sum_{p_a\cap p_b=p_i} b_1(p_a)b_2(p_b)}{1-k} & p_i\neq\varphi\end{cases} \tag{7}$$

其中,b_{1-2} 表示对同一事件两个专家的联合知识;k 用于估测两个专家的冲突度,由式(8)确定:

$$k=\sum_{p_a\cap p_b=\varphi} b_1(p_a)b_2(p_b) \tag{8}$$

2　基于 BN 的量化信任评估方法

文中的信任评估模型将物联网的感知层节点分为传感器、中继及基站 3 类节点。比如在车联网中,每辆车就是一个节点,节点间相互信任,才能可靠地传输信息,防止敏感信息被窃取或节点的隐私信息泄露。主要有三种信任衡量指标:

(1)直接信任值。因为恶意节点发起的攻击主要有窃取、篡改信息、注入大量错误信息等,所以数据包的转发量可以作为异常检测的重要指标之一,节点是否故意生成重复数据包或插入错误数据包是衡量数据传输服务质量的另一个重要指标。

(2)推荐信任值。只通过节点直接观测所得的直

接信任值衡量节点行为过于主观，所以，还需要参考其他节点的观测值，从而更客观地评价节点。节点只向相邻节点发送代评估节点的推荐信任值。

(3)历史统计信任值。主观性过多会影响信任评估的可信度，因此，节点行为的信任评估必须兼顾信任的主客观性，长期大量的节点行为统计可以得到具有稳定性与代表性的客观评价。

节点成簇是一种值得推崇的组网模式，能在数据融合过程中检测节点行为，以及时排除异常节点。簇内节点相互信任，实时评估，以确保网络安全。针对一个节点的评估中，当被评估节点作为子节点，其余节点就是父节点，形成贝叶斯网络结构。所以，可以用贝叶斯网络推理被评估节点的信任概率，其中父节点的先验概率表示自身的信任概率，子节点的条件概率表示父节点对子节点的信任程度。最后以概率的形式表示被评估节点的信任度。

基于贝叶斯网络的信任量化评估方法，用于确定新加入节点的安全性，或者检测网络中潜在的恶意节点。方法的主要步骤如图 1 所示。在网络参数确定中，主要是基于证据理论的先验概率融合，以及条件概率表的分配。

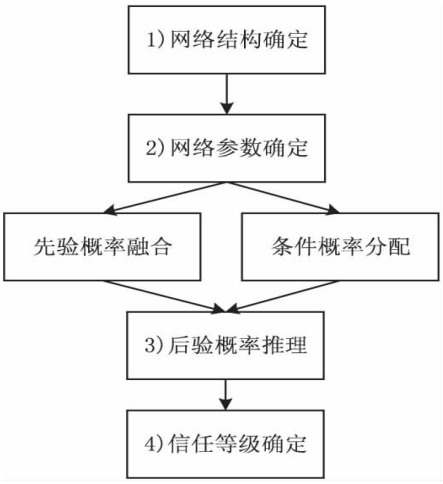
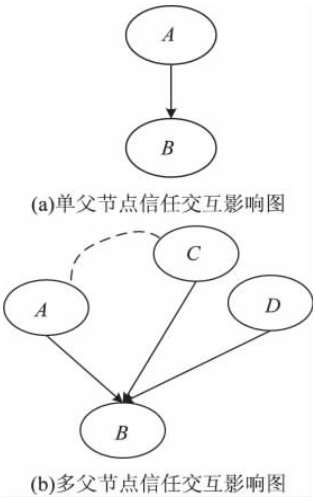


图 1 评估方法的主要步骤

2.1 网络结构确定

感知节点之间相互交互，只有相互信任，才能向对方发送或者接收数据。对于新加入的节点，主要通过网络中对其比较了解的节点确认信任等级；对于网络中的合法节点，通过与其交互的簇内节点对其的信任等级综合评估，以及时排除恶意节点。节点之间相互确定信任等级形成信任交互影响图，如图 2(a)所示，被评估节点 B 的信任等级通过辅助节点确定。而图 2(b)中，通过簇内的其他节点(称为辅助节点)确定被评估节点 B 的信任等级。如果将被评估节点作为输出节点，则辅助节点就是输入节点，输入节点与输出节点之间存在信任因果联系，可以将其转化为贝叶斯网络结构。



(a)单父节点信任交互影响图

(b)多父节点信任交互影响图

图 2 信任交互影响图

图 2(a)是最简单的信任交互影响图，也是最简单的贝叶斯网络结构，父节点和子节点的数目都为 1，分析和推理相对比较简单。图 2(b)中父节点有多个，如果父节点状态较多，子节点的后验概率的计算量较大，最复杂的是条件概率表的生成，分配条件概率的数目为所有父节点状态的乘积。

2.2 网络参数确定

每个节点的状态有三个，也就是每个节点存在的信任等级分为 3 级，分别为信任(信任等级为 1)、基本信任(信任等级为 2)、不信任(信任等级为 3)。节点的信任等级通过直接信任值、推荐信任值以及历史统计信任值等综合统计而来，以概率统计的形式显示，信任概率分布之和为 1。信任概率指对观测节点的信任程度。例如节点 A 的信任概率统计为(0.9，0.08，0.02)，表示信任节点 A 的概率为 0.9，基本信任节点 A 的概率为 0.08，不信任节点 A 的概率为 0.02。

(1)先验概率的融合。

一个节点的信任概率不同的统计方式，或者采用多专家知识，彼此之间存在分歧或者冲突。为了降低不一致，提高先验概率的可靠性，通过证据理论进行融合。例如节点 A 按方式 1 和方式 2 统计信任概率，分别为(0.84，0.1，0.05)和(0.8，0.1，0.1)，通过证据理论融合，得到 A 的可靠的可信概率为(0.97，0.01，0.02)。

(2)条件概率的影响。

在已知父节点信任概率分布的前提下，确定子节点的信任概率分布，主要任务是确定父节点影响下子节点的条件概率分布。例如，$P(B = L_1 \mid A = 1) = 1$ 表示已知 A 的信任等级为 1 时，B 的信任等级同样为 1 的信任概率为 1。在先验概率不变的情况下，条件概率变化对后验概率的影响非常大。条件概率表示，当 A 信任时，B 也为信任的概率较大；当 B 为基本信任

时,B 为信任的概率会降低;当 B 为不信任时,B 侧重于不信任。

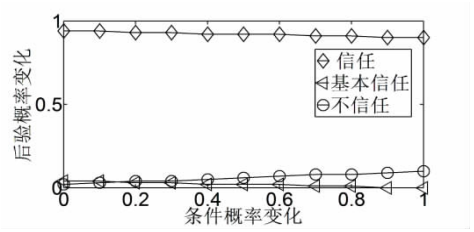


图 3　后验概率与条件概率之间的变化关系

以图 2(a)中网络为例,分析条件概率的影响,假设父节点状态为信任,则子节点信任;父节点状态为不信任,则子节点状态为不信任,即 $P(B=L_1 \mid A=L_1)=1$ 和 $P(B=L_3 \mid A=L_3)=1$。分析当父节点状态为基本信任时子节点的条件概率。当 $P(B=L_2 \mid A=L_2)$ 从 0 变化到 1,增量为 0.1,$P(B=L_1 \mid A=L_2)=P(B=L_3 \mid A=L_2)=\{1-P(B=L_2 \mid A=L_2)\}/2$。P(B)的变化趋势如图 3 所示,$P(B=L_1)$ 的概率逐渐变小。

(3)条件概率分配规则。

利用贝叶斯公式,物联网节点的信任等级有 m 个,即每个节点的状态为 m 个,状态 1 表示节点最期望的状态,状态 m 表示节点最不期望的状态。假如 $m=5$,有:非常信任(信任等级是 1)、信任(信任等级是 2)、比较信任(信任等级是 3)、基本信任(信任等级是 4)、不信任(信任等级是 5)。

如果父节点数目为 n,则父节点状态组合数为 m^n,父节点数目或者子节点的状态数目增加,则父节点的状态组合数目指数增加。所以,条件概率分配的工作量大以及盲目性高是最大的瓶颈。所以提出一种自动分配方法以降低主观性。

每种状态组合中,状态 1 到状态 m 的个数分别为 $k_1,k_2,\cdots,k_m$,相互之间的关系如式(9)所示:

$$k_1+k_2+\cdots+k_m=m,0\leqslant k_i\leqslant m,i=1,2,\cdots,m \tag{9}$$

根据父节点状态组合确定子节点的条件概率,分别为 $P(C_n=1 \mid \sum P_n)=k_1/m$,$P(C_n=2 \mid \sum P_n)=k_2/m,\cdots,P(C_n=m \mid \sum P_n)=k_m/m$,并存在式(10)所示关系:

$$P(C_n=1 \mid \sum P_n)+P(C_n=1 \mid \sum P_n)+\cdots+P(C_n=m \mid \sum P_n)=1 \tag{10}$$

其中,$\sum P_n$ 表示一种具体的父节点状态组合。

这种分配规则的缺点是只适合所有节点状态划分一致的情况,如果节点状态各异,方法灵活度将大打折扣,可以尝试通过状态归一化映射进行分配。

父节点的状态组合影响子节点的条件概率的分布,不同状态组合分配的条件概率不同。假如 3 个父节点,每个节点有 3 个状态,总共存在 27 个状态组合,通过归类发现,状态组合分为 3 种类型,在不同的状态组合影响下,子节点的最佳状态也不相同。针对不同类型,设计了相应的分配规则,如下所示:

(1)3 个相同,如:{1,1,1},{2,2,2},{3,3,3},共 3 个。3 个状态完全相同,说明子节点的最佳状态与父节点组合的状态相同,所以,最佳状态的条件概率为 1,其余状态为 0。

(2)2 个相同,如:{1,1,2},{1,1,3},{2,2,1},{2,2,3},{3,3,1},{3,3,2}等,共 18 个。2 个状态相同,说明子节点的最佳状态与其相同,将三分之二的条件概率分配给最佳状态,剩余三分之一的条件概率分配给其中一个状态。

(3)3 个不同,如:{1,2,3},{1,3,2},{2,1,3},{2,3,1},{3,1,2},{3,2,1},共 6 个。3 个状态完全不同,说明子节点的 3 个状态可以均分条件概率,每个状态分得三分之一。

2.3　后验概率推理

判断一个节点的信任等级,通过与其交互次数最多的 5 个节点确定,这样就形成一个包括 5 个父节点和 1 个子节点的贝叶斯网络结构。如果节点数不足 5 个时,选取与其有间接关系的节点。为得到节点的先验概率,通过两种方式进行评估,最后采用证据理论进行融合。父节点依次为 A,B,C,D,E,子节点为 F。

根据前面讲的条件概率分配规则,当父节点为 5 个时,得到条件概率分配规则表,如表 1 所示。

表 1　5 个父节点的条件概率分配表

子节点状态	5 个父节点状态组合			
	5 个相同	4 个相同	3 个相同	2 个相同
最佳状态	1	0.8	0.6	0.4
次要状态	0	0.2	0.2	0.4
其余状态	0	0	0.2	0.2

将融合的先验概率和分配的条件概率,结合贝叶斯理论,利用 GeNIe 软件,计算子节点 F 的可信概率,推理结果如图 4 所示。推理结果表示节点 F 的信任概率不超过 0.91。

2.4　信任等级确定

由上计算得到观测节点的信任概率,设置可信阈值 $\alpha=0.8$,如果最高信任概率大于等于可信阈值,则判断观测节点可信,否则不可信。显然节点 F 可信。

为了分析父节点对子节点的可信概率对子节点的可信概率的影响,交换父节点信任概率和不信任概率,即降低信任概率,增大不信任概率,当这样变化的父节点数目由 0 变到 5 时,如图 5 所示。当有一个父节点不信任子节点时,子节点的信任概率低于信任阈值,相

反,随着不信任子节点的父节点数目增加,子节点的不信任概率迅速增加。即表明,一旦出现不信任的父节点,子节点的信任概率迅速降低。

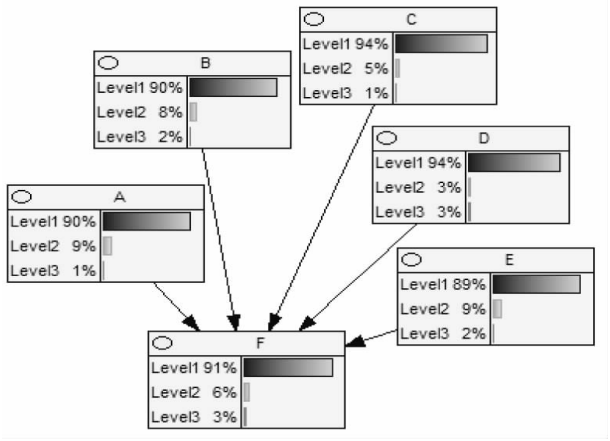


图 4 节点 F 的信任概率推理

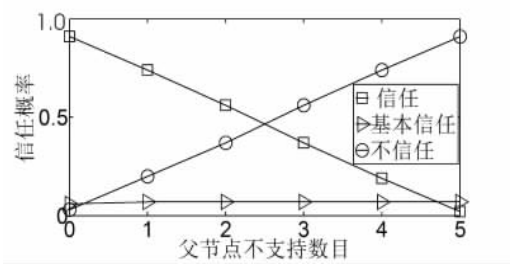


图 5 敏感度分析

3 结束语

物联网安全至关重要,防止恶意节点攻击,确保网络安全的重中之重是确定网络节点相互信任。为此,文中利用贝叶斯网络预测节点的信任概率,以判断新加入节点是否合法,或者判断具有合法身份的节点是否为恶意节点。提出的方法主要包括网络结构确定、网络参数确定、后验概率推理以及信任等级确定。为确保可靠的先验概率,采用证据理论融合;为获得合理的条件概率,制定了分配规则;利用 GeNIe 软件推理观测节点的信任概率,并判断是否在阈值范围内。最后通过实验发现,如果一个父节点不信任子节点,子节点的信任概率将低于信任阈值。提出的条件概率分配方法只适合节点状态划分一致的情况,未来将尝试通过状态归一化来分配状态划分不一致时的条件概率。

参考文献:

[1] 刘宴兵,胡文平.物联网安全模型及关键技术[J].数字通信,2010,37(4):28-33.

[2] 龚雪红.基于信任的物联网感知节点安全成簇机制研究[D].重庆:重庆邮电大学,2014.

[3] 刘 敏.基于信任评估的战术互联网安全分簇算法研究[D].郑州:解放军信息工程大学,2010.

[4] He Daojing,Chen C,Chan S,et al.A distributed trust evaluation model and its application scenarios for medical sensor networks[J].IEEE Transactions on Information Technology in Biomedicine,2012,16(6):1164-1175.

[5] Li X,Zhou F,Du J.LDTS:a lightweight and dependable trust system for clustered wireless sensor networks[J].IEEE Transactions on Information Forensics & Security,2013,8(6):924-935.

[6] Zhu H,Du S,Gao Z,et al.A probabilistic misbehavior detection scheme towards efficient trust establishment in delay-tolerant networks[J].IEEE Transactions on Parallel & Distributed Systems,2014,25(1):22-32.

[7] Ayday E,Lee H,Fekri F.Trust management and adversary detection for delay tolerant networks[C]//Military communications conference.[s.l.]:IEEE,2010:1788-1793.

[8] 刘宴兵,龚雪红,冯艳芬.基于物联网节点行为检测的信任评估方法[J].通信学报,2014,35(5):8-15.

[9] 田立勤,林 闯.可信网络中一种基于行为信任预测的博弈控制机制[J].计算机学报,2007,30(11):1930-1938.

[10] 张润莲,武小年,周胜源,等.一种基于实体行为风险评估的信任模型[J].计算机学报,2009,32(4):688-698.

[11] 贯 力.基于贝叶斯网络的室内环境监控数据融合方法研究[D].长春:吉林大学,2013.

[12] 赵 洁,肖南峰,钟军锐.基于贝叶斯网络和行为日志挖掘的行为信任控制[J].华南理工大学学报:自然科学版,2009,37(5):94-100.

[13] 王 辉.用于预测的贝叶斯网络[J].东北师大学报:自然科学版,2002,34(1):9-14.

[14] 王晓东,胡珊逢,叶庆卫,等.基于贝叶斯网络的可信概率评估方法[J].华中科技大学学报:自然科学版,2012(S1):79-82.

[15] Sentz K,Ferson S.Combination of evidence in Dempster-Shafer theory[M].Albuquerque,New Mexico:Sandia National Laboratories,2002:1-5.