一种新的无线传感器网络节点信誉评测模型 AEMP

顾 翔[1,2] 邱建林[2]

(南京邮电大学计算机学院 南京 210003)[1] (南通大学计算机科学与技术学院 南通 226019)[2]

摘 要 研究了一种新的信誉评测模型,模型采用"加法奖励、乘法惩罚"的方法。该模型与现有模型相比,运算简单,资源消耗少,适合于无线传感器网络节点资源受限的特点。仿真实验表明,该模型可以快速降低实施不良通信行为节点的信任值,从原理上减少误判。该模型为无线传感器网络路由协议设计提供了新的选路依据。

关键词 无线传感器网络,信誉评测,安全路由协议

中图法分类号 TP309 **文献标识码** A

AEMP－A New Reuptation Model of Sensor Nodes in WSNs

GU Xiang[1,2] QIU Jian-lin[2]

(School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)[1]

(School of Computer Science and Technology, Nantong University, Nantong 226019, China)[2]

Abstract A reputation model of sensor nodes in WSNs named AEMP was proposed. AEMP means 'Addition Encouragement, Multiplication Punishment'. Compared with current other models, AEMP can work with simple calculation and need fewer resources. So it is fit for the character that sensor nodes in WSNs have limited resources. Emulation experiments show the model can depress the reputation value of the node that executes bad communication behaviors quickly. And it can also reduce the possibility of wrong judgment. The mode affords a new routing algorithm for designing a WSNs routing protocol.

Keywords Wireless sensor networks, Reputation evaluation, Security routing protocol

1 引言

作为物联网感知层的重要一环,无线传感器网络 WSNs (Wireless Sensor Networks)是一种以数据为中心的应用驱动型网络,它有着节点数量较大、能量严格受限、节点拓扑变化频繁等特点。WSNs 领域的关键技术包括无线通信、能量管理、节点定位、路由技术、安全机制、数据融合等。在诸关键技术中,安全机制与 WSNs 的数据可信性、网络可靠性、网络生存期直接相关,它贯穿了 WSNs 协议栈的全部层次,是核心关键技术。

目前学者们在研究 WSNs 的安全问题时,将很大一部分精力投入在密码机制上,包括加解密算法、密钥分配与管理及在此基础之上的通信节点认证等。这一体系对于抵御网络外部入侵较为有效,但缺乏足够的能力来抵御网络内部节点的攻击[1]。

为此,有学者从另一个视角对 WSNs 的安全机制进行了探讨:在对网络中各节点行为进行监测的基础上,建立起一套节点信誉评测机制,计算出各个节点的可信程度(信任值),从而为选择数据传输的中间节点(路由)提供依据。和密码体系不同,这一机制着眼于网络内部,用以识别、剔除内部行为不端的不良节点(恶意节点)。在军事领域,这些不良节点可能是被敌方俘获而破解的;在民用领域,它们则可能是为了某些不当利益而由第三方故意设置的。

本文工作目的在于设计一种适合无线传感器网络资源严格受限的节点信誉评测机制。与现有评测机制相比,新机制通信资源消耗小,时空复杂度较低,从而更为实用。

2 节点信誉评测的研究现状

基于信任管理的信誉模型研究起源于人类社会,后来逐渐被引入到电子商务、对等网络、无线局域网等计算机应用及网络通信领域中。近年来又开始引起 WSNs 领域学者的关注,提出并设计了一些 WSNs 节点的信誉评测模型。

Confident 协议[2]较早提出了 WSNs 节点信誉评测机制。该协议对邻居节点进行监测,同时进行信任值计算,将计算结果与预设置阈值相比较,来判断节点是否可信。Pietro Michiardi 等人提出的 CORE 协议[3]在计算信誉值时,除了使用由节点自身观测得到的直接信誉值,还考虑了由其它节点推荐的间接信誉值。Crosby、Pissinou 和 Gadze 提出的基于古典概率的信任评估模型[4]使用简单的统计方法进行信誉值计算。Ganeriwal 和 Srivastava 提出的基于贝叶斯(Bayesian)公

到稿日期:2011-07-31 返修日期:2011-10-01 本文受国家自然科学基金(60773041),江苏省自然科学基金(BK2010277),江苏省博士后基金(1002002B)资助。

顾 翔(1973－),男,博士后,副教授,硕士生导师,主要研究方向为无线传感器网络、协议工程、形式化技术,E-mail:gu.x@ntu.edu.cn;**邱建林**(1965－),男,教授,硕士生导师,主要研究方向为逻辑综合、信息安全。

式的评估模型(BRSN模型)是到目前为止影响比较大的一种模型[5,6],它利用贝叶斯方法进行信誉的不确定性分析,其后,一些学者在贝叶斯公式和β分布基础上,研究节点信誉信息计算,提出了相关信任管理方法[7-10]。

唐文、胡建斌等人针对信任的主观模糊性提出了一种基于模糊逻辑的评估模型[11],运用IF-THEN规则进行形式化建模。成坚、冯仁剑等人提出一种基于D-S证据理论的评估模型[12],综合考虑直接、间接信誉值,并使用Dempster组合规则予以合成。冯建昭、杨光等人先后分别提出了基于β分布的恶意节点识别模型[1,13],引入第三方间接可信度,将多种攻击类型相对应的信誉值进行整合。

尽管不少学者提出了很好的模型,但是这些模型多数还只停留在理论阶段,与实际应用还有较大的距离。其主要原因在于:

① 信任计算的复杂度超出了WSNs节点的能力范畴。WSNs节点的运算能力、存储空间、自身能量有限是WSNs节点不同于其他网络类型节点的一个重要特征。目前多数理论模型的公式都过于复杂,模型越精致,所占用的存储单元也就越大,计算也就越复杂。这一方面大大增加了节点的工作负担及能耗,另一方面也对节点完成正常数据采集和通信功能带来不利影响。

② 多数理论模型所涉及的参数较多。大部分参数都需要通过节点间相互通信获取,并需要对参数历史数据进行保存,这些工作消耗了节点原本就宝贵而有限的资源。

③ 一些理论上的因素在实践中对评测结果可能影响并不大,在工程实践中完全可以而且也应该被忽视。但由于模型并未在实际应用中得到检验,无法确知哪些因素可以简化以及如何简化,最终只能导致模型复杂化。

④ 目前部分信誉评测机制还停留在就信誉论信誉的阶段。而信誉评测的一个目标是判断节点的可靠程度,从而为传输数据找到合适路由。如果能从这个角度入手,将模型设计和路由协议设计综合考虑,模型将更为实用。

3 一种简化的WSNs节点信誉评测模型

在对已有信誉评测模型进行分析研究后,设计提出了一种"加法奖励、乘法惩罚"的WSNs节点信誉评测模型AEMP(Addition Encouragement, Multiplication Punishment)。

3.1 信誉、信任和不良通信行为

在现有的研究报告或论文中,信誉和信任是两个经常出现而又紧密相关的概念。肖德琴等在文献[10]中给出了两者的定义:"信誉定义为一个实体对另一个实体的评价,被看作是一种概率分布;信任 T_{ij} 是节点 i 对节点 j 将要发生的行为的主观期望,即计算两个节点之间信誉概率分布的统计期望。"在这个定义中,信誉和信任关系密切,其本质上描述的是同一个问题,即一个实体对另一个实体的评价,而被评价实体自身性质却没有得到表述。这两个术语如此接近,以至在一些文献中会看到它们被不作区分地混用。

在我们设计的AEMP模型中,并没有考虑信誉参数的概率分布。对信誉参数进行概率分布的假设需要有WSNs节点分布的先验知识,例如信誉服从β分布的前提假设是均匀分布,这是一个比较强的假设。在AEMP模型中,对信誉和信任进行了重新定义。

定义1(信誉) 信誉是WSNs节点自身的属性,它描述了节点按照协议要求进行规范的通信和评价的愿望。

定义2(信任) 信任 T_{ij} 反映了节点 i 对于节点 j 的认可程度。一般地,节点 j 的信誉越高,i 给予 j 的信任值也就越大。

在这个定义中,信誉和信任的关系就犹如质量和重量的关系,信任是信誉评测的结果,不同节点得到的关于同一个节点的信任值会不尽相同,但它们都是对同一个信誉值的反应。

网络中恶意节点通常会实施各种攻击行为。网络中正常节点由于各种原因,如能量策略、优先级设置等,有时也会发生丢包、不转发包等类似于恶意行为的通信行为。为了简化模型,我们不区分这些行为是由恶意节点或是正常节点实施的,而是将它们统称为不良通信行为。

定义3(不良通信行为) 在无线传感器网络中,节点不按照所在网络的协议规范进行数据采集和转发的行为称为不良通信行为。

3.2 节点信誉评测模型AEMP

节点 i 对于节点 j 进行信誉评测的目的在于计算得出信任值 T_{ij},而不是判断被评测节点是正常节点或恶意节点,评测结果用于路由选择。本文提出的节点信誉评测模型在信誉评测期间有如下假设:

① 网络中各个节点独立进行信誉评测,不转发自己计算得到的关于某个节点的信任值,即信任值计算为直接信誉。关于间接信誉的计算与融合将另文阐述。

② 节点仅对自己的邻居节点(可以直接通信的节点)进行信誉评测。

③ 假设不良通信行为的判断方法已经解决,即在发生某一次通信行为后,可以确知该次通信行为是正常行为或是不良行为。这也是目前所有信誉评测模型的通用假设。

假设节点 i 正在对节点 j 进行信誉评测,计算得到的信任值为 T_{ij},当节点 i 观测到节点 j 的一次通信行为后,对 T_{ij} 作如下更新:

$$T_{ij}=\begin{cases}T_{\max}, & \text{正常通信,且 } T_{ij} \text{ 已达上限}\\ T_{ij}+step, & \text{正常通信,且 } T_{ij} \text{ 未达上限}\\ \tau * T_{ij}, & \text{该次通信为不良通信行为}\end{cases}$$

式中,$T_{\max}$ 是预定义的网络节点最大信任值;$step$ 是节点 i 观测到节点 j 发生正常通信行为后,对于节点 j 信任值的增长步长;τ 是节点 i 观测到节点 j 发生不良通信行为后,对于节点 j 信任值的折扣系数。

该模型要点在于,信任值积累以动态方式进行累积(加法奖励),而以乘法方式减少(乘法惩罚)。一旦观测到不良通信行为发生,信任值将大幅度快速减少,但仍有继续参与通信的机会。模型仅需记录保存对被观测节点的当前信任值即可。

3.3 AEMP模型的仿真实现

为了对AEMP模型的性能参数进行测试,使用MATLAB对模型进行了仿真实现。仿真场景为:在1000×1000的范围内,随机分布了20个无线传感器网络节点,每个节点最大通信半径为300。

无线节点采用自由空间范围内的通信模型[14],计算公式为:

$$P_R(d)=P_r-PL(d_0)-10\eta\log_{10}(\frac{d}{d_0}) \quad (2)$$

式中，P_r 为传播的信号强度，$PL(d_0)$ 为 d_0 传播过程信号强度的减弱量，η 为传播距离减弱的指数。

图 1 给出了节点分布情况。图 2 是当 $PL(d_0)$ 取 55dB、η 取 4.0 时，得到的节点间通信连接情况，两个节点之间的连线表明它们可以直接通信。

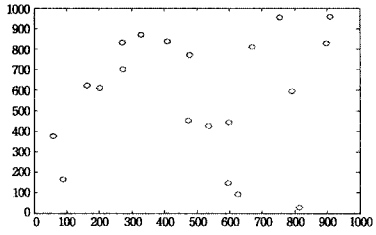

图 1　节点分布示意图

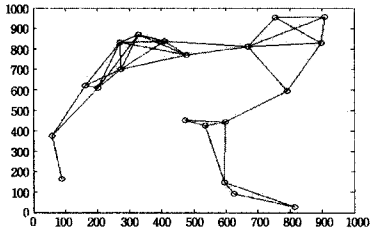

图 2　节点通信连通示意图

虽然 AEMP 模型的作用在于计算节点信任值，而不在于识别恶意节点，但在仿真过程中，为了得到计算数据，给信任值设定下限阈值，当节点信任值低于此阈值时，评测终止（在其它模型中，认为发现恶意节点）。

在仿真场景中，设 5 号节点为不良节点，它以概率 0.7 实施不良通信行为，信任值上限 T_{max} 为 50，下限阈值为 5，τ 取值 0.5，*step* 取值 1。当 5 号节点的所有 6 个邻居节点均发现它的信任值低于下限阈值时，仿真终止，同时记录从仿真开始至终止所需的时间。

重复 500 次仿真实验，图 3 给出了这 500 次实验的结果：横坐标为时间，纵坐标为实验结果在此时间段范围内的实验次数。从图中可以看出，实验结果基本呈正态分布，在 100－200 时间段的次数最多，有 360 次。500 次实验的平均时间值为 156.3。这张图表明，为了获得较为准确的实验结果，多次实验取数学平均值的方法是可取的。

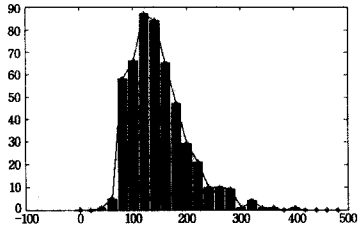

图 3　500 次仿真实验时间分布

3.4　仿真实验数据分析

在 AEMP 模型中，涉及到的参数有信任值上限、信任值下限阈值、不良行为概率、折扣系数 τ、信任值增长步长 *step*。为考察这些参数不同取值对模型评测性能的影响，我们进行了大量实验：每个取值实验 150 次，最终实验结果为这 150 次实验结果平均值。实验结果为两个值，一个为从实验开始至实验终止所需的时间，另一个为在实验持续期间，节点实施的不良通信行为次数。实验中，各参数基本取值为：信任值上限值 50，信任值下限阈值 5，节点不良行为概率 0.7，折扣系数 0.5，信任值增长步长 1。表 1 考察信任值上限对于模型评测性能的影响。实验中除信任值上限值外，其余各参数设置为基本取值。从表 1 中可以看出，信任值上限的取值对于评测性能影响不大。

表 1　信任值上限对于评测的影响

信任值上限	时间	不良行为发生次数
100	119.6	46.4
80	116.8	45.4
60	118.0	46.0
40	112.7	43.6
20	122.1	46.3

表 2 考察信任值下限阈值对于模型评测性能的影响。实验中除信任值下限阈值外，其余各参数设置为基本取值。从表 2 中可以看出，信任值下限阈值对于评测性能有一定的影响。下限阈值越大，节点可以犯错的机会越小，因为这将导致其它节点对它的信任值迅速下降到阈值以下。实践中，建议在参数设置上，在连续发生 4 次不良行为后，使信任值低于阈值。在上限值取 50，折扣系数 0.5 的情况下，下限阈值可取为 5。这样既可以较快发现不良节点，也不至于因为偶然的通信失败导致误判。

表 2　信任值下限阈值对于评测的影响

信任值下限	时间	不良行为发生次数
20	49.7	19.8
10	80.5	31.1
5	123.3	47.7
3	154.5	59.7

表 3 考察折扣系数 τ 对于模型评测性能的影响。实验中除 τ 外，其余各参数设置为基本取值。τ 的取值对于性能的影响与信任值下限阈值的影响基本一致，两者共同决定了节点可以连续发生不良行为的最大次数。由于实践中信任值取整数，从方便计算的角度考虑，τ 值取 0.5 较为合适，这时的计算负担是最小的。

表 3　折扣系数 τ 对于评测的影响

折扣系数	时间	不良行为发生次数
0.9	611.5	237.0
0.7	177.8	69.5
0.5	124.2	48.0
0.3	84.8	33.3

表 4 考察信任值增长步长 *step* 对于模型评测性能的影响。实验中除 *step* 外，其余各参数设置为基本取值。从表中可以看出，*step* 值在 3 以内对结果影响不大。*step* 值取得过大，会使得不良节点能借助正常通信行为快速修复信任值，增加判断所需的时间。在实践中，该参数取值为 1 即可。

表 4　增长步长 step 对于评测的影响

增长步长 step	时间	不良行为发生次数
5	299.8	115.9
4	193.2	74.8
3	164.5	62.3
2	139.0	53.7
1	115.2	44.6

表 5 考察节点不良行为概率对于结果的影响。实验中除

节点不良行为概率外，其余各参数设置为基本取值。在实践中，不良行为以多大概率执行不良通信行为完全由不良节点自主决定。从表中可以看到，不良节点执行不良通信行为的概率越大，就越容易被发现。

表5 节点不良行为概率对于评测的影响

不良行为概率	时间	不良行为发生次数
0.9	93.3	46.2
0.7	116.7	45.4
0.5	189.8	53.1
0.3	602.9	100.4

4 与 BRSN 模型的对比

BRSN 模型利用贝叶斯公式对信誉分布与 β 分布进行拟合，该模型认为节点 i 评测到的关于节点 j 的信任值为[5]：

$$C_{ij}=E(Beta(\alpha_{ij}+1,\beta_{ij}+1))=\frac{\alpha_{ij}+1}{\alpha_{ij}+\beta_{ij}+2} \quad (3)$$

式中，α_{ij} 为节点 i 观测到的节点 j 执行正常通信行为的次数，β_{ij} 为节点 i 观测到的节点 j 执行不良通信行为的次数。自2004年该模型提出后，许多学者在此基础上作了进一步的研究，但诸多改良模型的核心始终为假设信誉服从 β 分布，式(3)也一直被用于计算信任值。

AEMP 模型与该模型相比较，有如下一些优点：

① AEMP 模型不需要保留历史数据，而 BRSN 模型则需要更多的存储空间保存自评测开始以来正常通信和不良通信行为的次数。在实际网络运行中，当一个节点同时对所有邻居节点展开评测时，存储空间的需求将不能被忽略。

② AEMP 的计算更为简单，运算工作量小于 BRSN 模型。当折扣系数取 0.5 时，仅通过移位操作即可实现信任值的更新，即使折扣系数取其它值，运算量也要小于式(3)。

③ AEMP 模型在信任值更新上更符合实际规律。节点偶尔的非主观因素不良通信行为可以通过今后的正常通信行为逐步弥补，同时一次不良通信行为将带来信任值的大幅下降，使它被路由协议选中执行数据转发任务的可能性降低。而 BRSN 模型中，评测执行时间越长，α_{ij}、β_{ij} 值累积越大，新发生的不良通信行为给信任值带来的影响就越小。有学者注意到此问题，在改进模型中引入遗忘因子，这使得模型无论在执行上还是计算上都更为复杂，消耗更多资源，从而更加削弱了模型的实用价值。

④ 最为重要的是，AEMP 评测的效果优于 BRSN 模型。使用同样 WSNs 场景通过 MATLAB 进行基于 BRSN 模型的仿真实验，信任阈值取 0.4(BRSN 模型推荐值)，节点不良行为概率取 0.7。进行 150 次实验，得到的平均实验时间为 315.2，平均不良行为发生次数为 128.7。两个数值均不及 AEMP 模型。

结束语 AEMP 模型在实施中较现有信誉评测模型需要更少的运算和存储资源，同时由于参数数量少，在合理设计路由协议的基础上，也将需求更少的通信资源。这些对于资源极为有限的 WSNs 节点而言，具有较大的实用意义。

在本文中，所有信誉评测工作由评测节点独立完成，未考察第三方节点进行信任推荐的情形。仿真实验显示，综合本节点观测而得的直接信任和第三方节点推荐而得的间接信任，将使得模型工作更为高效。关于这方面的工作将另文阐述。

设计信誉评测模型的目的在于，在此基础上设计出 WSNs 基于信任机制的安全路由协议。为了降低评测模型消耗的通信资源，可以考虑采取选择触发评测时机、将评测所需数据在正常通信数据包中捎带传输、评测工作交由选取出的节点承担等手段。我们正在进行这方面的研究工作，并初步取得了良好的实验效果。

参 考 文 献

[1] 杨光，印桂生，杨武，等. 无线传感器网络基于节点行为的信誉评测模型[J]. 通信学报，2009，30(12)：18-26

[2] Buchegger S, Boudec J L. The Selfish Node: Increasing Routing Security in Mobile Ad Hoc Networks[R]. RR3354. IBM, 2001

[3] Michiardi P, Molva R. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks [C]// Proceedings of Sixth IFIP Conference on Security Communications and Multimedia (CMS2002). Portoroz, Slovenia: Kluwer Academic Publisher, 2002: 107-121

[4] Crosby G V, Pissinou N, Gadze J. A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks[C]// Proceedings of the 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS 2006). 2006

[5] Ganeriwal S, Srivastava M B. Reputation-based Framework for High Integrity Sensor Networks[C]// Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04). 2004: 66-77

[6] Ganeriwal S, Srivastava M B. Reputation-based Framework for High Integrity Sensor Networks[J]. ACM Transactions on Sensor Networks, 2008, 4(3): 1-37

[7] Dai Hongjun, Jia Zhiping, Dong Xiaona. An Entropy-based Trust Modeling and Evaluation for Wireless Sensor Networks[C]// Proceedings of 2008 International Conferenece on Embedded Software and Systems(ICESS2008). 2008: 27-34

[8] Mohi M, et al. A Bayesian Game Approach for Preventing DoS Attacks in Wireless Sensor Networks[C]// CMC'09. 2009: 507-511

[9] 邓黎黎，刘才兴. 无线传感器网络信任模型的研究与设计[J]. 传感器与仪器仪表，2010，26(8-1)：100-102

[10] 肖德琴，冯健昭，杨波，等. 基于无线传感器网络的信誉形式化模型[J]. 计算机科学，2007，34(6)：84-87，100

[11] 唐文，胡建斌，陈钟. 基于模糊逻辑的主观信任管理模型研究[J]. 计算机研究与发展，2005，42(10)：1654-1659

[12] 成坚，冯仁剑，许小丰，等. 基于 D-S 证据理论的无线传感器网络信任评估模型[J]. 传感技术学报，2009，22(12)：1802-1807

[13] 冯健昭，肖德琴，杨波. 基于 β 分布的无线传感器网络信誉系统[J]. 计算机应用，2007，27(1)：111-113，117

[14] 赵洪磊，王英龙，张先毅. 基于传播模型的无线传感器网络覆盖的研究[J]. 计算机应用与软件，2010(01)：114-116