文章编号: 1001-0920(2017)04-0715-06 DOI: 10.13195/j.kzyjc.2016.0307

基于节点行为动态变化的WSNs信任模型

叶正旺[1,3†], 温 涛[1,2], 刘振宇[1,2], 宋晓莹[1], 付崇国[1,2]

(1. 东北大学 计算机科学与工程学院，沈阳 110004；2. 大连东软信息学院 计算机科学与技术系，辽宁 大连 116023；3. 通化师范学院 网络信息中心，吉林 通化 134002)

摘 要: 在无线传感器网络信任模型中,为了解决信任值随着时间和上下文的行为变化而动态变化的问题,提出一种基于节点通信行为动态变化的信任模型. 所提模型给出了节点间的直接信任和间接信任关系的度量、信任信息的合并、信任传递的合理抽象,并提出了一种信任更新机制. 仿真结果表明,所提出的信任模型通过节点间通信行为的动态变化对信任值进行惩罚与调节,所得到的信任值能够更加敏感地反应节点间的行为变化,更加精确可靠地评价节点之间的信任关系.

关键词: 无线传感器网络；信任模型；恶意节点；安全

中图分类号: TP393 **文献标志码:** A

Trust model based on dynamic change of node behavior for WSNs

YE Zheng-wang[1,3†], *WEN Tao*[1,2], *LIU Zhen-yu*[1,2], *SONG Xiao-ying*[1], *FU Chong-guo*[1,2]

(1. School of Computer Science and Technology，Northeastern University，Shenyang 110004，China；2. Department of Computer Science and Technology，Dalian Neusoft University of Information，Dalian 116023，China；3. Network Information Center，Tonghua Normal University，Tonghua 134002，China)

Abstract: In the wireless sensor networks trust model, aiming at the problem of the dynamic change of trust value with time and context, this paper proposes a trust model based on dynamic change of node behaviors. The model provides a calculation method of direct trust and indirect trust, and integration of trust value, the transfer of trust, and also gives a trust update mechanism based on the sliding time window. The simulation results show that, the trust value is punished and adjusted by the dynamic change of the communication behaviors between nodes, and the resulting trust value can be more sensitive to the behavior change among the reaction nodes, and more accurate and reliable for the evaluation of the trust relationship between nodes.

Keywords: wireless sensor networks；trust model；malicious node；security

0 引 言

随着无线传感器网络节点硬件的提升,无线传感器网络应用的范围和领域也不断扩大,一些受环境限制的区域和行业都可以通过无线传感器网络进行数据采集和监控,例如军事、医疗、农业、环境监测等[1]. 但由于能耗、带宽、计算能力和运行环境等对无线传感器网络的限制,使无线传感器节点在开放环境下工作极易被俘获、破坏或攻击,无法保障数据传输的安全性和可靠性. 因此,建立无线传感器网络安全机制非常有必要.

目前,国内外学者对无线传感器网络安全的研究已经取得了很多成果. 主要的安全措施包括身份认证、加密、信息完整性确认和入侵检测等,但以上这些安全机制只能处理防御来自网络外部的入侵和攻击. 而对于无线传感器网络的内部攻击,这些安全机制就显得没有任何意义,因为恶意节点已经顺利进入网络内部,在网络内部开始实施具体的攻击行为. 比较典型的内部恶意攻击有自私节点、恶意转发、黑洞攻击、灰色攻击和蠕虫攻击等[2]. 针对无线传感器网络内部恶意节点攻击,现在比较流行有效的防御措施是基于信任模型的管理机制. Ganeriwal等[3]首次提出了基于信誉的信任管理框架(RFSN),并应用于无线传感器网络,该框架采用Watchdog机制监测邻居节点通信行为,将监测结果输入信誉系统模块以生成

收稿日期: 2016-03-16；**修回日期:** 2016-07-19.

基金项目: 国家自然科学基金项目(61170169, 61170168).

作者简介: 叶正旺(1982−),男,博士生,从事网络安全的研究；温涛(1962−),男,教授,博士生导师,从事网络安全、信任机制等研究.

†通讯作者. E-mail: yezhengwang@neusoft.edu.cn

各个节点的信任值,采用贝叶斯公式计算信誉值来定量分析评估节点不确定性. 该信任框架比较完整,健壮性好,但需要主观假设信誉值的先验分布. 文献[4]提出了一种基于代理的信任模型ATSN,代理节点用来监控节点的行为并给出好与坏的判断,代理通过记录统计所有好行为和恶意行为,并用一个三元组定义信任空间为好、坏或不确定. 该方案有效节省了计算资源和能耗,但该算法信任计算没有考虑间接评价和更新过程. Shaikh等[5]提出了一个基于分组的信任管理机制,并应用于簇结构的无线传感器网络. 信任值的计算是通过节点监控邻居节点之间的通信行为获得,主要包括节点信任计算、簇头节点信任计算、组信任计算和基站信任计算, 从4个方面分别建立信任机制来抵御恶意节点的攻击. 该信任模型可以有效抵御恶意节点的攻击,有效保护恶意节点对好节点的诋毁和诽谤攻击,且占用很少资源. Feng等[6]提出了一个可信的基于贝叶斯的信任管理机制BTMS,模型中信任值的获得采用RFSN信任值计算方法计算直接信任和间接信任,并通过加权整合为综合信任值. 该模型引入了时间滑动窗口对信任值进行更新,并考虑了间接信任值计算过程中第三方的不确定性因素对信任值的影响,针对节点的通信行为给出了很好的信任计算方法. Jiang等[7]提出了一种综合高效的无线传感器网络信任模型,该方案中根据传感器节点接收到数据包的数量有选择性地计算直接信任值和推荐信任值. 在直接信任的计算过程中,考虑了通信信任、能量信任和数据信任. 此外,信任的可靠性和熟悉度被定义用于提高推荐节点的准确性,该信任机制得到的传感器节点信任值更精确且可靠. 文献[8-10]给出了对其他信任模型与应用的总结.

通过对以上算法的研究发现,大多数研究成果在建立信任模型过程中,通过节点间的通信行为,即通过节点间成功交互次数与不成功交互次数来评价节点之间的信任值. 但很少考虑信任度随着时间和行为上下文的变化而增减的动态性变化,不能有效抵御间谍和策略性攻击行为. 基于此,本文提出一个高可信的基于节点通信行为动态变化的信任感知模型. 该模型给出了节点间的直接信任和间接信任关系的度量、信任信息的合并、信任传递的合理抽象. 节点间信任值的计算过程引入了惩罚函数与调节函数,通过节点间通信交互成功次数与不成功次数进行更加精确的信任评估,通过引入惩罚函数实现短时间内不成功交互次数剧增节点间信任值的惩罚,快下降通信行为表现为恶意节点的信任值. 引入调节函数实现短时间内成功交互次数剧增节点对信任值的快速提升,慢增长信任值防止网络中恶意节点间通过共谋相互吹捧短时间内获得高信誉值并进行攻击. 实现信任值的“快下降,慢增长”的目标. 另外,还给出了推荐节点可信度评估机制来避免了第三方恶意推荐的风险,并以此为基础,给出一种基于滑动时间窗口的信任更新机制. 实验仿真表明,该信任模型得到的信任值随着节点间通信行为的动态变化能够有效抑制信任值的增减,有效抵御节点之间互相吹捧或者诽谤对信任值的影响,得到节点信任值的评估更加精确可信.

1 网络模型与假设

假设所有的传感器节点随机部署在一个二维空间中. 所有传感器节点具有相同的初始能量和通信半径,并具有相同的计算、通信和存储能力. 网络中的节点只与通信范围内的邻居节点进行通信. 网络部署前为每个节点都分配一个唯一的标识;网络节点部署完成后,节点之间需要通过相互通信完成网络初始化,由基站节点发起泛洪通信,向通信范围内的邻居节点广播自己的标识并记下自己的邻居节点,建立邻居列表;邻居节点再发起泛洪通信,直到泛洪通信结束,形成一个无线传感器网络拓扑结构. 本文假设网络中的节点既不增加,也不在部署后从网络中移除,并且节点之间所有的通信链路是双向安全的.

基于以上假设,无线传感器网络可以抽象为图$G=(V,E)$,V是所有节点的集合,E是所有边的集合. 每个边$e(i,j)\in E$表示该节点位于彼此的通信传输范围内.

2 基于节点行为动态变化的信任模型

2.1 直接信任值

直接信任值是节点i对节点j通过直接通信行为给出的直接信任评估,直接信任值的计算采用贝叶斯公式计算[3]. 采用Watchdog机制监测邻居节点通信行为,将监测结果用来计算各个节点的信任值,通过信息熵理论对一个随机信号或事件的不确定性或信息量进行测量. 假设先验分布服从Beta分布,通过期望值来衡量节点之间的信任值,得到如下公式[3]:

$$T_{d(i,j)}=\frac{\alpha_{ij}+1}{\alpha_{ij}+\beta_{ij}+2}, \tag{1}$$

其中α_{ij}和β_{ij}分别代表节点i与节点j在Δt时间内成功与不成功通信的交互记录次数. 本文在式(1)的基础上引入惩罚函数和调节函数计算信任值,得到直接信任值计算公式如下:

$$T_{d(i,j)}=\frac{\alpha_{ij}+1}{\alpha_{ij}+\beta_{ij}+2}\left(1-\frac{\beta_{ij}}{W}\right)\left(1-\frac{1}{\alpha_{ij}+1}\right). \quad (2)$$

其中: $1-\frac{\beta_{ij}}{W}$ 是惩罚函数, W 是节点之间具有影响力的总通信次数. 通过惩罚函数的引入,使得短时间内节点之间不成功通信次数增加时,节点表现为恶意的行为,则该节点信任值快速降低,实现信任值的快下降的目标. 通过节点间的通信行为的动态性变化对信任值进行惩罚,能够快速精确地识别节点的恶意行为,更加快速有效地抑制恶意节点攻击,惩罚函数是通过节点之间通信行为中恶意行为的动态变化对信任值的惩罚. 另外,为了避免恶意节点通过共谋相互吹捧实现恶意节点信任值的迅速提升,引入调节函数 $1-\frac{1}{\alpha_{ij}+1}$. 该函数并不是一个线性函数,随着节点之间成功交互通信成功次数的增加,表达式越来越接近于1,但接近于1的速度并不是突然的增加.这种设计是通过节点间成功通信行为的友好行为的动态变化,实现对节点之间突然增加的通信成功次数对信任值的影响,通过调节函数的引入可实现信任值慢增长的目标. 这种设计能够有效抑制节点之间的共谋或坏嘴攻击. 另外,在现实网络环境中,节点之间的通信行会受到节点之间网络拥塞、噪音等不确定因素的影响,通过该函数可以有效调节不确定因素对信任值的影响. 大多数信任模型研究并没有考虑这方面的因素,因此所获得的节点信任值都是理想状态下的一种表现. 本文通过增加该函数使得信任值更加精确可信;更能反映真实的网络环境的动态变化对信任值的影响;更加有效地保证网络通信过程中节点之间的信任关系.

2.2　间接信任值

为了更加精确地获得节点之间的信任值,本文引入间接信任值和直接信任值共同完成对节点的可信度进行评估. 间接信任值是由第三方对评估节点行为给出的推荐信任值. 节点 i 对节点 j 的间接信任值由各推荐节点对节点 j 的直接信任值合成,推荐节点由节点 i 和节点 j 共同的邻居节点组成,但并不是所有的推荐节点都是可信的,不可信的推荐节点将虚假信息提供给节点用来评估节点的可信度会影响对节点真实可信度的判断. 为了更好更准确地通过推荐节点来计算间接信任值,需要选择可信的共同邻居节点作为推荐节点. 首先定义一个指定的信任阈值 δ,在节点 i 对节点 j 共同的邻居节点集合中选出直接信任值高于 δ 的节点作为推荐节点集合. 假设节点 i 对节点 j 共同的邻居节点的信任值分别为 $T_{i1}, T_{i2}, \cdots, T_{i(k-1)}, T_{ik}$. 当 $T_{ik} \geqslant \delta$ 时,节点 k 被选为推荐信任节点,否则该节点被忽略.

由文献[9]可知,信任值具有传递性,因此本文的间接信任模型通过选出的信任推荐节点进行计算. 间接信任是通过共同邻居节点的推荐信任值进行评估的,采用信任链机制对间接信任进行评价. 间接信任 $T_{\mathrm{ind}}(i,j)$ 计算如下:

$$T_{\mathrm{ind}}(i,j)=\frac{\sum\limits_{m\in N_k, m\neq i} T_d(i,m)\times T_d(m,j)}{|N_k|}. \quad (3)$$

其中: $T_{\mathrm{ind}}(i,j)$ 表示节点之间的间接信任值, $T_d(i,m)$ 表示节点 i 对节点 m 的直接信任值, $T_d(m,j)$ 表示节点 m 对节点 j 的直接信任值, $|N_k|$ 表示节点 i 和节点 j 之间共同信任推荐节点的个数.

2.3　综合信任值

节点的综合信任值由直接信任和间接信任加权求和得到. 综合信任值的计算公式为

$$T(i,j)=\lambda T_d+(1-\lambda)T_{\mathrm{ind}}. \quad (4)$$

其中: $T(i,j)$ 表示节点 i 对节点 j 的综合信任值, T_d 和 T_{ind} 分别表示节点之间的直接和间接信任值, λ 表示直接信任的权重.

3　信任模型更新机制

无线传感器网络数据的传输具有实时性和动态性,因此传感器节点间的信任值需周期性更新. 另外,节点的信任值需考虑节点的历史信任关系和现有信任关系进行综合评估来获得更加精确可信的信任值. 为了解决这个问题,本文引入时间滑动窗口对信任值进行更新.

时间滑动窗口被用来更新节点的信任值. 每个时间窗口包括几个时间子窗口,每一个子窗口为一个周期的时间. 在对节点的信任值进行评估时,只有在时间滑动窗口范围内的数据记录才有效. 假设现在时间窗口长度为 m,这意味着该时间窗口包含 m 个子窗口,在本文中表示为要考虑的历史记录个数. 具体的时间滑动窗口的更新操作如图1所示.

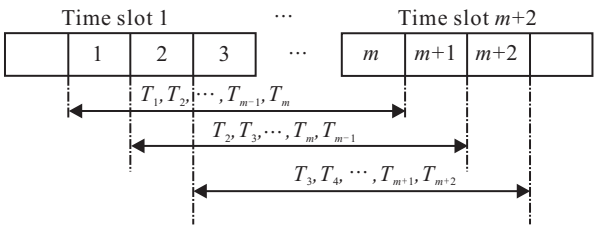

图 1　时间滑动窗口

从图1可以看出,该时间滑动窗口被分成 m 个子窗口,并从左向右平移. 随着时间滑动窗口子窗口

的移动,数据记录信息也随着更新,信任值更新变化过程为: $T_1, T_2, \cdots, T_{m-1}, T_m; T_2, T_3, \cdots, T_m, T_{m+1}; T_3, T_4, \cdots, T_{m+1}, T_{m+2}$. 根据每个子窗口记录的信任值来对信任值进行综合评估. 每个周期的信任值为$T(i), i = 1, 2, \cdots, m$,其中$m$为子窗口的个数. 在一个周期结束后,下一个子窗口中的信任值更新为

$$T(i+1)_{\text{new}} = \beta T(i) + (1-\beta)T(i+1), \quad (5)$$

其中β为历史记录的权重. 由于信任机制的时间衰减性,离当前越久的子窗口对信任值的影响越小,因此需要建立各个历史子窗口信任值的衰减权重系数来完成现有信任值的计算. 衰减原理可以用许多不同的方式实现. 本文采用指数衰减函数β作为历史记录的权重. β的定义方式如下:

$$\beta = \mathrm{e}^{-\rho(t-t_0)}. \quad (6)$$

其中: ρ是调节因子,且$\rho \in (0,1)$; t和t_0分别是当前信任值和历史信任值的计算时间.

4 仿真与性能分析

为了验证该信任模型各方面的性能,用Matlab进行仿真实验. 首先,验证本模型中节点间的通信行为动态变化的惩罚和调节对直接信任值的影响,实现动态更新信任值的性能; 然后,分别实现无恶意节点情况下与有恶意节点攻击情况下节点间通信行为的动态性对信任值的评估性能,并与RFSN[3]和BTMS[6]进行性能对比. 具体的参数如表1所示.

表 1 实验参数

Parameters	Value
Initial energy / J	0.5
Initial trust value	0.5
Packet length / bit	2 000
d_0 / m	37
E_{elec} / (nJ/ bit)	50
E_{DA} / (nJ/(bit · signal))	5
λ	0.6
δ	0.6

4.1 调节函数与惩罚因子对直接信任值的影响

图2给出了基于时间的节点间记录成功和不成功的通信交互次数对直接信任值的理论评估结果. 假设历史交互总记录数W为150.

由图2可知,信任值随着节点间通信行为成功交互次数的增加平缓增长. 但只要存在不成功行为记录,即使成功交易次数很多,信任值始终也不会超过0.5. 节点间的通信行为动态变化的惩罚和调节对直接信任值的更新过程保障了直接信任值的时效性并迅速给出反应,真实反应网络环境变化中恶意与友好行为对信任值的影响,使得该模型的信任评估更加精确,并符合信任模型快下降、慢增长的目标.

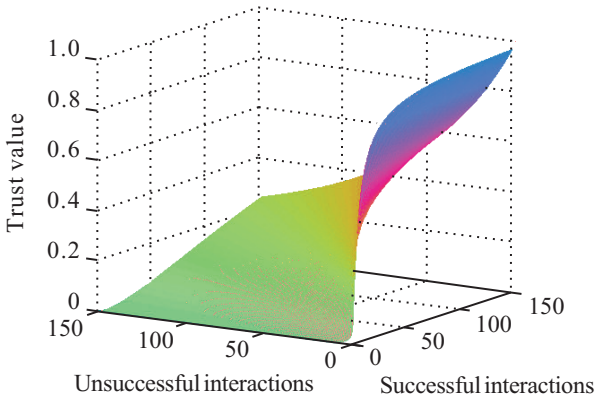

图 2 通信交互次数对直接信任值的影响

为了更好地说明加入惩罚函数和调节函数的节点行为动态变化对直接信任值的影响,提取仿真实验中一组特殊的数据进行说明. 相对应的节点之间的成功与不成功行为次数和对比算法的直接信任值如表2和图3所示, α_{ij}和β_{ij}分别代表节点i与节点j在Δt时间内通信成功与不成功通信的交互记录次数.

表 2 举例说明惩罚函数和调节函数对直接信任值的影响

α_{ij}	β_{ij}	RFSN	BTMS	Our trust
7	4	0.636 364	0.598 974	0.524 103
21	12	0.636 364	0.578 286	0.552
35	20	0.636 364	0.547 368	0.532 164
49	28	0.636 364	0.514 768	0.504 473
63	36	0.636 364	0.481 584	0.474 059
77	44	0.636 364	0.448 13	0.442 385

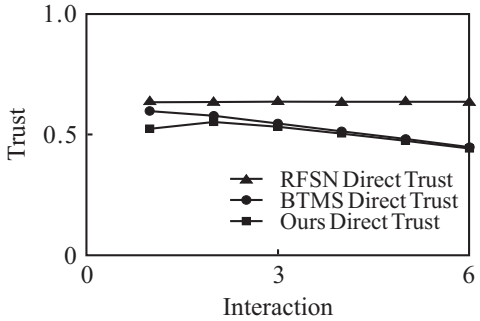

图 3 表2中实例数据直接信任值对比

由表2和图3具体的对比数据可知,算法RFSN中的直接信任值在这组数据中始终相同,没有体现出节点通信行为动态变化对节点之间信任关系的影响,无法通过信任值客观公正地评价节点的行为好坏. 但随着节点间通信行为的变化,不成功交互次数的增加,算法BTMS中直接信任值受惩罚因子的影响

迅速降低. 本文提出的算法综合考虑了节点间通信行为的动态变化对信任值的影响,通过节点之间成功交互次数与不成功交互次数的行为变化,动态更新节点间的信任关系. 当节点间通信行为成功交互次数提高时,好的行为对信任值并没有明显的急剧提升,但节点间不成功交互次数增加时,恶意的行为对信任值进行惩罚使信任值迅速下降. 这组实例表明:加入惩罚函数和调节函数的信任模型能够通过节点间通信行为的动态变化实时更新信任值,实时反应节点间的信任关系,获得的节点之间信任值更加精确可信,能够更精确地确定节点行为的好坏.

4.2　信任值比较

下面对该信任模型中节点之间的直接信任值和综合信任值分别在无恶意节点情况下和有恶意节点情况下通信过程进行仿真,并与RFSN和BTMS进行对比.

首先,无恶意节点攻击情况下,节点间的通信行为表现为通信成功次数随着运行时间的推进稳定增长,通过仿真实验得到各个模型的直接信任值和综合信任值对比如图4和图5所示. 在无恶意节点攻击情况下,节点间通信行为表现为成功交互次数的增加,该值直接作用调节函数对信任值进行动态更新,当成功交互次数急剧增加时,信任值的增长受到限制,不能短时间内迅速提升节点间的信任值.

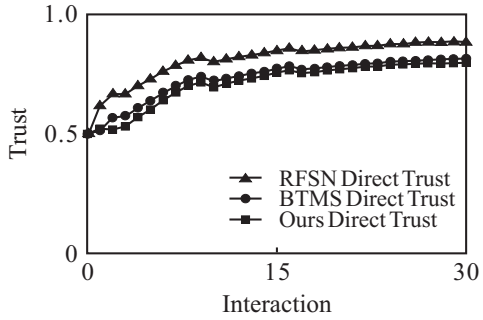

图 4　正常情况下的直接信任值对比

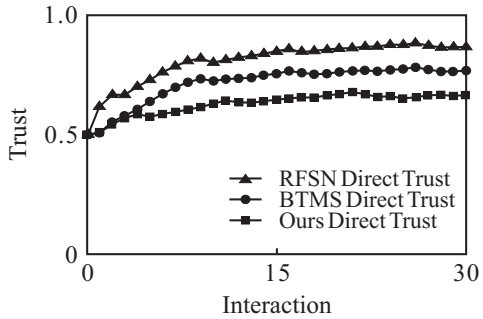

图 5　正常情况下的信任值对比

由图4和图5可知:所提出算法信任值的增长速度始终低于RFSN和BTMS算法,有效避免了短时间内节点之间通过成功交互次数的增加来迅速提升信任值,实现了信任值慢增长的设计目标,更加适应了网络中节点间通信行为表现为好的行为对信任关系的影响.

其次,有恶意节点攻击情况下的直接信任值和综合信任值对比如图6和图7所示. 由于恶意节点的攻击行为,使得节点间的通信行为表现为不成功交互次数的增加,该值直接作用惩罚函数对信任值进行惩罚操作,当不成功交互次数急剧增加时,快速降低节点间的信任值,实现了信任值快下降的设计目标.

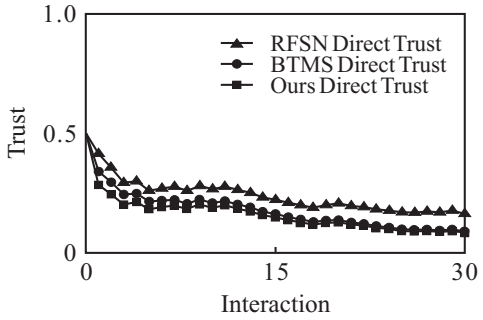

图 6　恶意节点攻击情况下的直接信任值对比

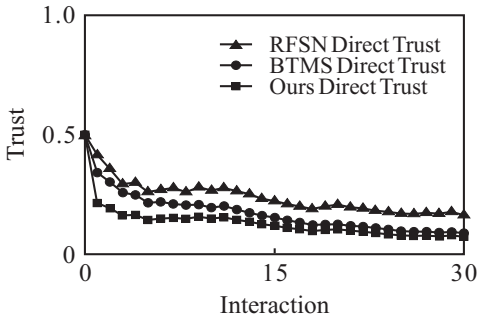

图 7　恶意节点攻击情况下的信任值对比

由图6和图7可知:本文所提出算法的信任值始终低于RFSN和BTMS的信任值;充分反应了当节点之间的不成功交互次数增加时,本模型中信任值对恶意的通信行为表现为更加敏感;更加精确可靠地评价了节点之间的信任关系,更快速有效地识别出恶意节点,对恶意攻击行为反应更加敏感.

4.3　信任模型代价分析

由于无线传感器本身节点能量及计算能力的限制以及WSNs内存与带宽的限制,建立基于信任模型的安全机制必须考虑节点与网络的开销,保障以可接受的资源代价实现有效的安全措施.

基于信任模型的无线传感器网络安全机制是在原有的系统中加入信任管理模型,这必然要增加节点开销,其中包括额外的计算以及存储负担. 对于分布式通信网络而言,信任证据的传播、信任的更新也会产生额外的通信开销. 本文的信任模型采用与RFSN和BTMS类似的数学模型,下面对不同信任模型的能耗开销、计算开销与内存开销进行对比分析.

能耗开销. 无线传感器网络节点的能耗是有限的,节能一直是无线传感器网路研究的重点,本文信任模型的能耗主要包括行为监督、信任计算、更新和推荐信任收集. 其中:行为监督采用Watchdog机制;信任计算和更新机制采用简单的计算可以实现;推荐信任计算对推荐节点进行筛选,避免了冗余节点通讯的能耗. 与RFSN和BTMS的能耗相比,并没有产生多余的能耗开销,但能耗一直是无线传感器网络研究的一个重点,实现最小的能耗获取更好的性能一直是一个NP问题.

计算开销. 无线传感器网络节点在计算能力上也受到限制,本文设计的信任模型在计算上不会对网络节点增加任何额外负担,信任值的计算和更新机制采用最简单的运算就可以实现,不存在复杂的计算过程. 而在BTMS中,更新机制采用了指数计算,计算复杂度要远远高于本文信任模型.

内存开销. 由于无线传感器网络受节点硬件与网络协议的限制,还要考虑节点的内存和带宽. 本文信任模型占用的内存和带宽不会对网络产生很大的影响,与RFSN 和BTMS的内存开销基本一致.

5 结 论

本文提出了一个高可信的无线传感器信任感知模型,通过感知节点通信行为计算节点之间的信任值来有效识别、隔离恶意节点. 在信任计算中引入惩罚函数与调节函数来反映节点通信行为的动态变化对信任值的影响,并给出了信任值的更新机制. 仿真表明,所提模型获得的信任值更加精确可信,对恶意攻击行为的信任关系反应更加敏感,能快速有效地识别出恶意节点. 但该模型值对通信行为的动态变化以及对信任值的影响考虑得不够全面,下一步的工作重点是考虑多方面的节点行为建立信任模型,更加全面地实现恶意节点识别.

参考文献(References)

[1] Akkaya K, Younis M. A survey on routing protocols for wireless sensor networks[J]. Ad Hoc Networks, 2005, 3(8): 325-349.

[2] Duan J, Yang D, Zhu H, et al. TSRF: A trust-aware secure routing framework in wireless sensor networks[J]. Int J of Distributed Sensor Networks, 2014, 2014(1): 1-14.

[3] Ganeriwal S, Balzano L K, Srivastava M B. Reputation-based framework for high integrity sensor networks[J]. ACM Trans on Sensor Networks, 2004, 4(3): 66-77.

[4] Chen H, Wu H, Zhou X, et al. Agent-based trust model in wireless sensor networks[C]. The 8th ACIS Int Conf on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing. IEEE Computer Society, 2007: 119-124.

[5] Shaikh R A, Jameel H, D'Auriol B J, et al. Group-based trust management scheme for clustered wireless sensor networks[J]. IEEE Trans on Parallel and Distributed Systems, 2008, 20(11): 1698-1712.

[6] Feng R, Han X, Liu Q, et al. A credible bayesian-based trust management scheme for wireless sensor networks[J]. Int J of Distributed Sensor Networks, 2015, 2015(2): 1-9.

[7] Jiang J, Han G, Wang F, et al. An efficient distributed trust model for wireless sensor networks[J]. IEEE Trans on Parallel and Distributed Systems, 2015, 26(5): 1228-1237.

[8] Han G, Jiang J, Shu L, et al. Management and applications of trust in wireless sensor networks: A survey[J]. J of Computer and System Sciences, 2014, 80(3): 602-617.

[9] Ishmanov F, Malik A S, Kim S W, et al. Trust management system in wireless sensor networks: Design considerations and research challenges[J]. Trans on Emerging Telecommunications Technologies, 2015, 26(2): 107-130.

[10] 张仕斌, 方杰, 宋家麒. 一种面向WSNs的可信数据融合算法研究[J]. 小型微型计算机系统, 2014(10): 2347-2352.
(Zhang S B, Fang J, Song J L. Study on an algorithm of trusted data fusion oriented on WSNs[J]. Mini-micro Systems, 2014(10): 2347-2352.)

(责任编辑:齐 霁)