文章编号:1006-0464(2018)02-0168-06

基于改进贝叶斯和风险评估的无线传感网络信任模型

胡 军[1],管 春[2],胡 涛[2]

(1.南昌大学软件学院,江西 南昌 330047;2.南昌大学 信息工程学院,江西 南昌 330031)

摘 要:针对无线传感器网络加密手段和身份认证技术不能解决网络内部攻击问题,提出一种基于改进的贝叶斯和风险评估的无线传感器网络信任模型。该模型针对基本的贝叶斯信任模型进行改进,采用异常折扣因子防止非入侵因素导致的网络异常行为;为实现信任对时间的敏感性,提出了自适应遗忘因子来削弱过去行为的影响;为防止恶意节点的诋毁,利用偏离度来过滤某些推荐节点;同时提出了基于熵的风险评估机制,用于评价信任的不确定性。实验结果表明,所提出的模型具有较高的检测率与较低的误检率,能有效保障无线传感器网络安全性能,并延长网络的生命周期。

关键词:无线传感器网络;内部攻击;贝叶斯理论;风险评估

中图分类号:TP393 **文献标志码**:A

DOI:10.13764/j.cnki.ncdl.2018.02.012

Research on trust model of wireless sensor networks based on bayes and risk assessment

HU Jun[1],GUAN Chun[2],HU Tao[2]

(1.School of Software,Nanchang University,Nanchang 330047,China;
2.School of Information Engineering,Nanchang University,Nanchang 330031,China)

Abstract:Encryption and authentication technology can not solve the internal attacks problem in wireless sensor networks.A new wireless sensor networks trust model is presented based on Bayesian and a risk assessment.The model is improved mainly based on Bayesian theory and risk evaluation mechanism,with the aim to prevent the abnormal network behavior caused non invasion reasons by introducing abnormal discount factor. To reflect the sensitivity of trust on time,an adaptive forgetting factor is introduced to weaken the past actions.To prevent malicious slander,the deviation is used to filter the recommended node.Since Bayesian theory does not have the function of evaluating the uncertainty of trust,the entropy based risk assessment mechanism is developed,and it can reflect the uncertainty of trust.Finally,through a large number of experiments,the results show that the proposed model has higher detection rate and lower false detection rate,with the advantages of ensuring network security performance and extending the network life cycle.

Key words:wireless sensor networks; internal attacks; Bayesian theory; risk assessment

随着无线传感器网络(Wireless Sensor Network,WSN)技术的不断发展,应用越来越广泛,使得它面临越来越严峻的安全问题[1-3],它很容易受到恶意节点的各种攻击[4]。Ganeriwal 等人提出一种基于信誉的 RFSN 框架[5],RFSN 框架详细的给出了信任评估的计算方法。XU 等人提出一种 D_S 证据理论,区别于其它信任框架,它可以表述“不确定的”能力[6]。Li 等人在 WSN 分簇的网络中,轻量

收稿日期:2017-06-10。
基金项目:江西省普通本科高校中青年教师发展计划访问学者专项资金项目资助(赣教办函[2016]109 号)。
作者简介:胡军(1971—),男,教授,博士,硕士生导师。E-mail:hujun@ncu.edu.cn。

级的思想引入到信任决策中,通过节点的反馈信息,可以减少恶意节点对网络的危害[7]。Almennarez 等人提出一种基于 D－S 理论的 PTM 信任模型,该模型扩展性很强,可以快速获取节点的信任值[8],Shaikh 等人提出一种基于信任管理机制的 GTMS 信任管理方法,该方法可以很大程度上降低节点消耗的能量,延长网络的生存周期[9]。Lei Huang 等人提出一种基于网络节点行为的信任机制,这种机制可以辨别恶意节点和老化节点[10],Cheng Wei Huang 等提出一种考虑能量有限的情况下,既能保证路由安全,又能增加网络吞吐量的方案[11],马彬等考虑信任机制的不确定性和模糊性,提出一种基于云的信任模型[12],弥补了一些信任模型的不足之处,Gheorghe 等人提出一种自适应信任管理协议 ATMP,可以有效的评估信任值,Duan J 等人提出一种博弈论信任模型 TDDG[13],基于博弈论的信任值计算流程,分析网络的安全机制对 WSN 节点进行激励来建议博弈节点进行决策,从中获取最优的合作节点,但是没有考虑能量问题[14]。上述模型忽略了网络中异常情况下的处理方法,在不确定情况下模型存在安全问题;其次信任的权重和更新问题也没有得到很好的解决。本文提出一种基于改进贝叶斯和风险评估的 WSN 信任模型,能有效保障无线传感器网络安全性能,延长网络的生命周期。

1　基本的贝叶斯信任模型

根据贝叶斯理论,Ganeriwal 等人在 WSN 网络信任评估模型中提出基于信誉的框架 RFSN,该框架利用信誉分布与 Beta 拟合,信任值利用其数学期望值表示。i 节点一共转发了$(\alpha+\beta)$次任务给 j 节点,j 节点完成了 α 次任务,β 次任务失败,直接信任值计算为:

$$D_{ij}=E(\mathrm{Beta}(\alpha+1,\beta+1))=\frac{\alpha+1}{\alpha+\beta+2} \quad (1)$$

为了得到评估节点 i 与被评估节点 j 的之间的间接信任,假设节点 i 和节点 j 之间有 n 个共同的邻居节点,节点 k 为其中某邻居节点,间接信任由 i 节点对 k 节点综合信任 T_{ik} 和节点 k 对节点 j 的综合信任 T_{kj} 共同决定,那么节点 i 采纳的节点 k 对节点 j 的推荐信任值为:

$$I_{ij}(k)=T_{ik}\cdot T_{kj} \quad (2)$$

当 i 节点有 n 个对 j 节点的推荐者时,则评估节点 i 对评估节点 j 的间接信任值 I_{ij} 为:

$$I_{ij}=\frac{\sum_{k=1}^{n}(T_{ik}\cdot T_{kj})}{n} \quad (3)$$

在 WSN 网络信任评估模型中,单独依赖直接信任或者间接信任来评价节点之间的信任,既不准确也不可靠,通常将被评估节点的直接信任值和间接信任值相互融合,我们称这种信任为综合信任,综合信任可以很好的保证节点之间准确性和可靠性,其计算公式如下:

$$T_{ij}=\lambda_1\cdot D_{ij}+\lambda_2\cdot I_{ij} \quad (4)$$

其中 T_{ij} 为综合信任值,D_{ij} 为直接信任值,I_{ij} 为间接信任值,λ_1、λ_2 为权重因子,代表直接信任和间接信任在综合信任计算中所占的比例,比例越大,对 T_{ij} 的影响越大,而且 $\lambda_1+\lambda_2=1$。

2　基于改进贝叶斯和风险评估的信任模型

本文对基本贝叶斯信任模型中做了三方面的改进,首先引入了异常折扣因子,削弱了网络中由非入侵因素造成网络节点异常行为,其次提出了自适应遗忘因子来替代固定遗忘因子,可以动态的适应信任值的变化,最后对间接信任值的计算方法也做了改进,利用偏离度来过滤一些恶意的推荐节点,这样可以更加合理的获取间接信任值。以上改进能有效提高可靠性,保证网络的安全。

针对不是由恶意节点攻击造成的误检,而是由于网络自身因素导致的网络节点异常行为,引入异常折扣因子 fs,其定义为:当判断节点行为异常时,该行为异常是由恶意节点入侵所导致的概率,f 的计算公式如下:

$$f=\frac{N_{intru}}{N_{detec}} \quad (5)$$

其中,f 是异常折扣因子,N_{intru} 是由恶意节点入侵引起的节点异常行为的次数,N_{detec} 是网络中检测出的节点异常行为的总数。

基本贝叶斯信任评估模型中,信任模型会平等的对待正常行为和异常行为,这种机制反而对信任评估造成影响,它不能体现信任的时效性,节点越靠近当前的行为越能体现节点接下来的行为,过去时间越久的行为参考价值越小,因此要考虑远期交互行为的时间衰减,减少历史久远的数据对信任值的影响,引入自适应遗忘因子来解决这一问题,假设节点 A 和节点 B 交互历史中,合作的次数为 α,不合作的次数为 β,一个周期后,增加 r 次合作,s 次不合作,

则更新方法修正为：

$$\alpha^{\text{new}}=\alpha\cdot\theta+(1+\frac{\alpha}{\alpha+\beta})\cdot r \tag{6}$$

$$\beta^{\text{new}}=\beta\cdot\theta+(2-\frac{\alpha}{\alpha+\beta})\cdot s \tag{7}$$

引入偏离度 dev 来过滤虚假的推荐信任值，偏离度可以对被评估节点给予虚假的评价、毁谤正常节点等行为进行筛选过滤，偏离度用来评价评估节点与被评估节点的综合信任值和推荐者与被评估节点的综合信任值的偏离程度，dev 计算公式：

$$\text{dev}=\frac{|T_{ij}-T_{kj}|}{T_{ij}} \tag{8}$$

其中 T_{ij} 为评估节点 i 与被评估节点 j 的综合信任值，T_{kj} 推荐者 k 对被评估节点 j 的综合信任值。dev 越大，推荐者 k 推荐的信任值偏离程度越大，推荐者 k 就越不可靠。

改进后的贝叶斯信任模型计算公式为：

$$T(i,j)=\omega_1 D_{ij}+\omega_2 I_{ij}=\omega_1\cdot\frac{\alpha^{\text{new}}+1}{\alpha^{\text{new}}+f\beta^{\text{new}}+2}+\omega_2\cdot\frac{\sum_{k=1}^{n}(T_{ik}\cdot T_{kj})}{n} \tag{9}$$

其中其中 $T(i,j)$ 为节点 i 与节点 j 的综合信任值，ω_1、ω_2 分别是它们的权重，且 $\omega_1+\omega_2=1$。ω_1 越大，表示直接信任值对信任值的影响程度越大。

为了使信任模型适用性更强，在原有信任模型中加入基于熵的风险评估机制，将信息熵应用到 WSN 节点信任评估模型中来量化风险值。风险可以反映节点近期的不可靠程度，一个对象对于另一个对象来说，熵越小，表示实体越可信，否则，实体越不可信，只考虑节点直接交互行为带来的风险值，r、s 分别表示一个周期节点 i 和节点 j 合作次数和不合作次数。则风险值计算公式如下：

$$R_{ij}=\begin{cases}1+p\log_2 p+(1-p)\log_2(1-p), & 0.5\leqslant p\leqslant 1\\ -p\log_2 p-(1-p)\log_2(1-p), & 0\leqslant p\leqslant 0.5\end{cases} \tag{10}$$

将风险值加入到原有的信任模型中，可以表现信任的不确定性，则新的节点信任模型更新为：

$$T(i,j)=\omega_1 D_{ij}+\omega_2 I_{ij}-\omega_3 R_{ij} \tag{11}$$

其中 D_{ij}、I_{ij}、R_{ij} 分别为直接信任值、间接信任值和风险值，ω_1、ω_2、ω_3 分别为它们的权重，且 $\omega_1+\omega_2+\omega_3=1$，它们的值越大，表示对信任值计算的影响越大。改进后的信任模型增加了风险评估机制，风险评估机制与信誉机制相结合，可以更准确节点信任值，两者兼顾了贝叶斯理论和熵的优点，使评估模型具有很好的适应性。

3 实验结果与分析

本文采用 Matlab 2010 软件作为仿真工具，仿真环境相关参数设置为：网络部署区域为 200 m × 200 m，100 个节点随机分布在部署区域，网络中的节点处于静止状态，每个节点都有唯一的 ID 标识，其它参数如表 1 所示。仿真时从 Sinkhole 攻击、Sybil 攻击和 Dos 攻击中随机选择，节点的数据转发率设置为[0.9,1] 的随机值。每次选择的默认攻击点数目分别是{1,3,5,7,10,15,20}，对每个数目都独立做 20 次仿真实验，最后结果取平均值。

表 1 仿真实验参数设置

参数	默认值
权重因子 λ_1、λ_2	0.5、0.5
权重因子 ω_1、ω_2、ω_3	0.6、0.3、0.1
异常折扣因子 f	0.6
偏离阀值	0.2
节点通信半径	30 m
节点初始能量	1 J
传输能耗	60 nJ/bit
接收能耗	50 nJ/bit
放大器功耗	10 pJ/(bit/m²)
每个节点每轮传递数据包大小	100 bit

3.1 正常节点和恶意节点的信任值变化

仿真实验中，先观察正常节点和恶意节点的信任值变化如图 1 所示，从图中可以看出，随着采样周期的变化，正常节点的信任值逐渐升高，恶意节点的信任值逐渐降低，实验表明，节点信任值的上升速度不如节点信任值的下降速度，这是因为风险评估机制的引入，模型对节点失常行为感知很敏感，即便网络中存在伪善节点，模型也可以较快的将其识别出来，因此，本文将风险评估机制引入信任模型能有效的鉴别正常节点和恶意节点，尤其是伪善节点较多

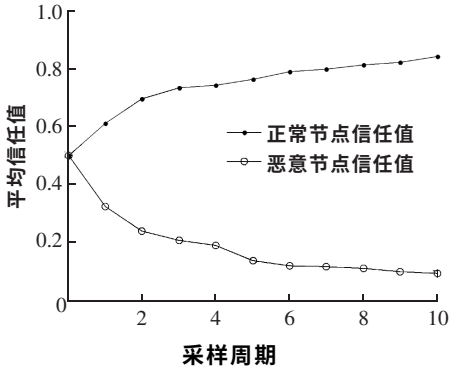


图 1 节点信任值变化图

是,可以及时的发现,并将其隔离出网络,从而提升网络安全性能。

3.2　异常折扣因子 f 对网络安全性能的影响

图 2 是检测率随异常折扣因子变化图,从图中可以看出,随着 f 的增大,检测率增大,这是因为 f 越大,节点异常行为被削弱的程度越小,所以检测率越高。图 3 是误检率随异常折扣因子变化图,随 f 的增大,误检率先增大,后减小,这是因为,当 f 较小时,有些恶意节点的不合作行为将会被忽视,使它们被误检为正常节点,所以误检率较大,当 f 值很大时,非入侵因素会造成正常节点行为异常,被误认为是恶意节点,所以误检率较大,所以图 3.8 中误检率随异常折扣因子的变大,先减小后增大,其中,当异常折扣因子为 0.7 时,误检率最低,效果最好,本实验环境下,异常折扣因子取 0.7 最佳。

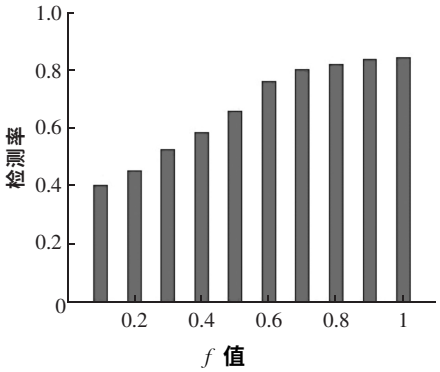


图 2　检测率随异常折扣因子变化图

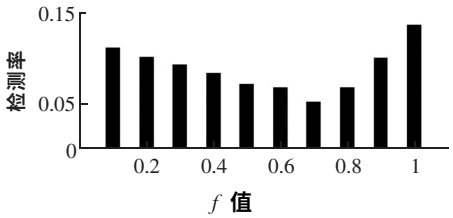


图 3　误检率随异常折扣因子变化图

3.3　网络安全性能分析

仿真通过检测率和误检率来评价网络性能,通过本文所提出的信任方案(简称 BRSN)、无风险评估方案(简称 NRSN) 以及文献[5]RFSN 3 种方案进行实验对比,从检测率图 4 中可以看出,本文引入风险评估机制后检测率比其它两种方案都要高,因为风险评估机制引入,使得模型对节点失常行为比其它方案更敏感,很容易识别出网络中的伪善节点,因此检测率更高,而其它两种方案没有这种机制。从误检率图 5 中可以看出,本文方案误检率最低,相比于其它两种方案,本文方案因为风险评估机制的引入,可以及时识别某些恶意节点,以免模型将恶意节点错检成正常节点,所以误检率较低,可以得出结论,本文所提方案检测率最高,误检率最低,网络安全性能最好。

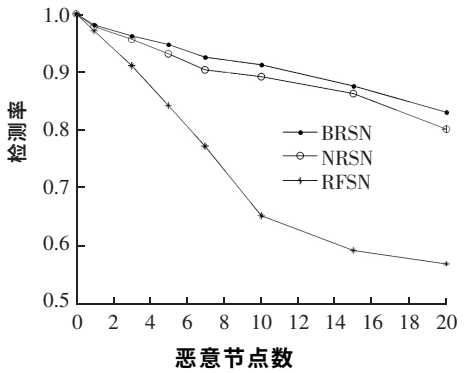


图 4　检测率随恶意节点个数变化图

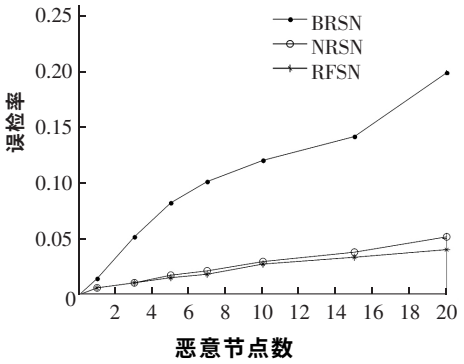
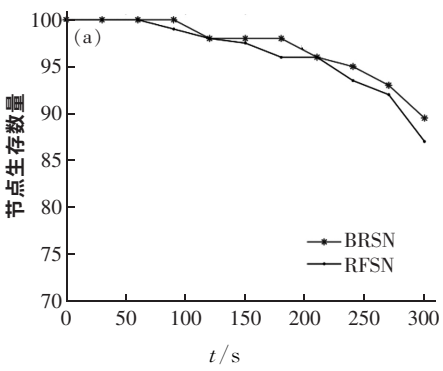


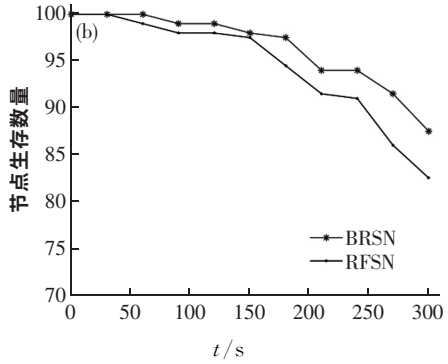
图 5　误检率随恶意节点个数变化图

3.4　节点生存数量分析

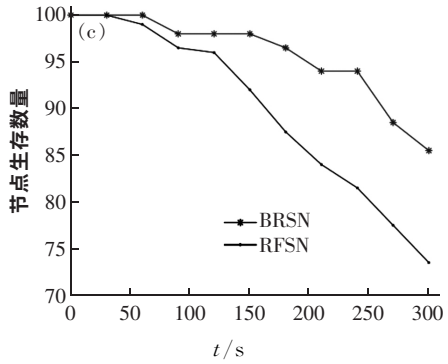
为了分析节点生存的数量,仿真分别使用 5、10、15、20 个恶意节点,每种数量的恶意节点分别进行 20 次仿真实验,结果取平均值。图 6 显示了仿真实验中本文所提方案 BRSN 与文献[5]RFSN 方案节点生存数量对比图,随着仿真实验的进行,4 种不同恶意节点情况下,随着时间的推移,BRSN 和 RFSN 方案节点存活数量都逐渐减少,本文所提方案 BRSN减少的速度相对较慢,而RFSN方案减少的



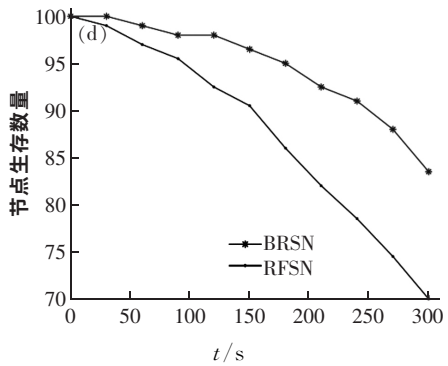
(a) 恶意节点数:5



(b) 恶意节点数:10



(c) 恶意节点数:15



(d) 恶意节点数:20

图 6 节点生存数量随时间变化图

速度较快,尤其当恶意节点较多时,这种区别越明显,这是因为 RFSN 方案中不能及时识别出恶意节点,致使转发数据时需要消耗更多的能量,造成节点的能量迅速下降,从而导致过早死亡,而本文所提方案 BRSN 能均衡使用网络中节点的能量,可以避免过度消耗某些节点,使网络中节点能量消耗更加均衡,可以延长网络的生命周期。

综上所述,改进的贝叶斯理论和风险评估机制完善了很多信任评估的不足之处,模型具有更强的适应性,实验表明,本文所提模型不仅可以提升网络的安全性能,还可以延长网络的生命周期。

4 结语

本文针对基本贝叶斯理论进行改进,引入风险评估机制,提出一种基于改进贝叶斯和风险评估的 WSN 信任模型。模型综合各方面因素来评价节点的信任度,实验结果表明,本文提出信任模型具有较高的检测率与较低的误检率,保障网络安全性能的同时,还能延长网络的生命周期。但是,无线传感器网络依然存在一些问题需要进一步研究,如传感器节点能量有限,怎样做到在不降低信任评估准确性前提下,优化算法,使得消耗的能量更少。本文模型是建立在节点静态状态情况下,如何将本文信任模型应用到动态的网络节点中是下一步要研究的问题。

参考文献:

[1] MODARES H, SALLEH R, MORAVEJOSHARIEH A. Overview of Security Issues in Wireless Sensor Networks[C]//IEEE Computer Society, 2011: 308-311.

[2] BLILAT A, BOUAYAD A, CHAOUI N E H, et al. Wireless Sensor Network: Security Challenges[C]// Network Security and Systems, 2012: 68-72.

[3] LI Y X, QIN L, LIANG Q. Research on Wireless Sensor Network Security[C]//International Conference on Computational Intelligence and Security, 2010: 493-496.

[4] 张中科,汪芸.无线自组织网络下抵抗内部节点丢弃报文攻击的安全模型[J].计算机学报, 2010, 33(10): 2003-2014.

[5] GANERIWAL S, BALZANO L K, SRIVASTAVA M B. Reputation-based Framework for High Integrity Sensor Networks[J]. Acm Transactions on Sensor Networks, 2008, 4(4): 1-37.

[6] JIANG L, XU J, ZHANG K, et al. A New Evidential Trust Model for Open Distributed Systems[J]. Expert Systems with Applications, 2012, 39(3): 3772-3782.

[7] LI X, ZHOU F, DU J. LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks[J]. Information Forensics & Security IEEE Transactions, 2013, 8(6): 924-935.

[8] ALMENAREZ F, MARIN A, DYAZ D, et al. Developing a Model for Trust Management in Pervasive Devices[C]//IEEE International Conference on Pervasive Computing and Communications Workshops, 2006: 5-271.

[9] GHEORGHE L, RUGHINIS R, TATAROIU R. Adaptive Trust Management Protocol Based on Intru-

sion Detection for Wireless Sensor Networks[J].IEEE Research,2013:1-7.

[10] HUANG L, LI L, TAN Q. Behavior-Based Trust in Wireless Sensor Network[C]//BLP,2006:214-223.

[11] CHENG W, LIAO X, SHEN C, et al. A Trust-Based Routing Framework in Energy-Constrained Wireless Sensor Networks [M]. Berlin Heidelberg Springer, 2006:478-489.

[12] 杨永飞,刘光杰,戴跃伟.基于信任的反馈云模型 WSN 节点信任评价机制 [J].计算机科学,2015,42(6A):388-392.

[13] DUAN J, GAO D, YANG D, et al. An Energy-Aware Trust Derivation Scheme With Game Theoretic Approach in Wireless Sensor Networks for IoT Applications[J].Internet of Things Journal IEEE,2014,1(1):58-69.

[14] GHEORGHE L, RUGHINIS R, TATAROIU R. Adaptive Trust Management Protocol Based on Intrusion Detection for Wireless Sensor Networks[J].IEEE Research,2013:1-7.

[15] 谭文群,包学才,邓承志.基于信号飞行时间与误差分析的改进无线传感网络 Bounding-box 定位算法[J].南昌大学学报(理科版),2016,40(5):389-394.

[16] 徐晓斌,张光卫,王尚广.基于轻量云模型的 WSN 不确定性信任表示方法 [J].通信学报,2014,35(2):63-69.