An Energy-Efficient Trust Model for Flat Wireless Sensor Networks*

YU Yanli[1], *LI Keqiu*[1*], *JU Long*[2]

(1. *School of Computer Science and Technology, Dalian University of Technology, Dalian Liaoning* 116024, *China*;
2. 65521 *Troops of PLA Workstation of Automatic Command, Liaoyang Liaoning* 111000, *China*)

Abstract: Several trust models have been proposed to effectively solve insider attacks for wireless sensor networks. However, a trust scheme also leads to extra cost from the scheme itself. Furthermore, existing trust models lack the fairness of trust evaluation for sensor nodes. In order to overcome the drawbacks of trust schemes in wireless sensor networks, we propose an energy-efficient trust model for flat wireless sensor networks. In this paper, we define an Executable Ability of a sensor node. Using the relationship between the ability of a sensor node and the difficulty of a task, our proposed model could improve the fairness of trust evaluation and enhance the efficiency of an individual node. The results of simulation show that our proposed model can rule out malicious nodes effectively, and improve the efficiency of nodes, decrease the energy expenditure of nodes, and prolong the lifetime of network.

Key words: wireless sensor networks; network security; trust management; Rasch; network lifetime

EEACC: 6210C; 6150P **doi**: 10.3969/j.issn.1004-1699.2012.011.015

一种能量有效的平面式无线传感器网络的信任管理模型*

于艳莉[1], 李克秋[1*], 鞠 龙[2]

(1. 大连理工大学计算机科学与技术学院, 辽宁 大连 116024; 2. 辽阳市 65521 部队指挥自动化工作站, 辽宁 辽阳 111000)

摘 要: 信任管理机制解决了来自无线传感器网络的内部攻击问题, 但同时产生由信任评价带来的额外开销。现有的信任管理模型对节点信任度的评价缺乏公平性, 导致节点使用率的降低。为了解决信任机制在无线传感器网络的耗能问题, 提出了一种能量有效的平面式无线传感器网络信任模型。通过节点的自身性能与任务难度的关系定义节点的执行度, 在确保信任管理有效性的同时, 增强节点信任度评价的公平性, 从而提高传感器节点的使用率, 降低了能量消耗。最后通过模拟实验, 证明该信任模型与传统信任模型相比, 能够有效检测恶意节点, 同时大大降低了节点的能量消耗, 提高了网络生存周期。

关键词: 无线传感器网络; 网络安全; 信任管理; Rasch; 网络生存周期

中图分类号: TP393 **文献标识码**: A **文章编号**: 1004-1699(2012)11-1543-06

无线传感器网络 WSNs (Wireless Sensor Networks) 的安全问题一直是国内外学者的研究热点, 由于无线传感器网络具有节点资源有限, 网络环境恶劣等特点, 使其安全问题更为复杂和困难。信任管理是构筑在社会学上的一种理论, 被认为是传统网络安全技术的有效补充, 为研究者提供了一种新思路, 在电子商务、P2P、网格、Ad hoc 等各种开放式网络环境中被广泛研究。

尽管针对安全问题, 目前已有很多方法和理论, 包括密码学、入侵检测、安全路由等, 但是这些传统安全技术无法抵挡来自于无线传感器网络内部的攻击问题[1-2]。由于资源有限而导致的传感节点的自私行为, 以及由于节点被俘获而导致的恶意行为等, 都会严重影响无线传感器网络的正常运行, 特别是节点被俘获后, 其存储的秘密信息就会暴露, 对基于密码体系的安全措施构成了很大的威胁。目前已有很多研究者, 将信任管理机制应用于无线传感器网络中的事件监测、安全路由、数据融合等各方面, 与无线传感器网络的安全体系[3]相结合, 以提高无线传感器网络的安全性和可用性[4]。

本文借鉴心理学和教育测量领域的 Rasch 理论[5], 提出一种适用于平面式无线传感器网络结构的能量有效的信任模型 EETM (Energy-Efficient Trust Model)。由于传感器节点及无线网络环境的自身脆弱性, 导致传感节点的功能在一段时期内失效或通信能力降低, 现有的信任管理模型在对节点

项目来源: 国家自然科学基金项目(60973117)
收稿日期: 2012-07-20 **修改日期**: 2012-10-09

信任评估时,未考虑这一因素影响,而是采用直接降低节点的信任值,易将此类节点的行为误作为来自于恶意节点的内部攻击,使得正常节点在网络中的使用率下降,并减少了网络整体的使用寿命。本文将节点的执行度作为信任评估的度量参数引入到信任管理模型中,基于平面式无线传感器网络结构提出能量有效的信任路由算法。通过仿真实验,证明该模型能够有效识别恶意节点,并减少由信任管理所带来的额外能量消耗,较经典信任管理通用系统 RFSN 能有效提高网络寿命。

1 相关研究

目前针对无线传感器网络的信任管理系统的研究主要集中在对节点的信任值评估上,通过信任节点以满足网络的安全需求。对于无线传感器网络的信任管理机制的研究自 2003 年起逐渐得到学者的关注。

文献[6]提出了一个基于地理信息的无线传感器网络信任路由协议 TRANS(Trust Routing for Location-Aware Sensor Networks),通过节点的密码学因子、可用性因子、转发率因子和激励因子评估节点信任值,定位可疑节点位置,将其加入黑名单广播给所有节点或将其嵌入到数据包头以在路由时绕过。TRANS 的信任值评估采用直接信任值作为信任评估的唯一信任信息来源,在短时期内有效控制了由信任评估带来的能量消耗,但如果将其他节点的间接信任也用于信任评估的话,则能增加信任值评估的有效性,在长时期内达到节省整个网络的能量消耗。

文献[7]提出了一个架构完整的无线传感器网络的通用信任管理模型 RFSN(Reputation Based Framework for Sensor Betworks),通过节点行为的历史记录更新计算节点的直接信任值和推荐信任值。一些攻击者可以通过共谋方式获取高的信任评级,而 RFSN 将推荐节点自身的信任评级作为权重参数,能够有效抵御这类共谋攻击。某些恶意节点得知被归类为恶意行为节点时,通过伪造新的身份重新加入网络中造成威胁,即洗白攻击,为避免此类攻击行为,在 RFSN 中,各节点在网络初始状态下互不信任,即采用较低的初始信任值以增加攻击者的成本。但在无线传感器网络中,采用低初始信任值虽然在某种程度上能抵制洗白攻击,但同时也大大增加了网络信任评估的时间成本。

文献[8]提出了一个基于群组结构的无线传感器网络信任管理机制 GTMS(Group-Based Trust Management Scheme),采用分布式信任管理机制,在簇内、簇头和簇间分别有各自的信任值,通过网络分级评估计算节点的信任值。此外,GTMS 采用 0 到 100 的整数计算信任值以减少信任信息的存储和交互代价。但是由于 GTMS 将簇间的群组信任值作为一个整体,因此存在一定局限性,即群组中的各成员节点必须固定,一旦簇内节点消亡或有新的成员节点加入,则该群组的信任值就需要重新评估。

另外还有一些文献从无线传感器网络的数据容错[9]和数据融合[10-11],以及簇头选举[12]等方面针对不同的应用背景提出和建立了各种信任管理模型。

2 能量有效信任模型

传感器节点由多种不同类型的敏感元件监控感应监测范围内的环境数据,通过无线网络路由协议(平面或分层路由协议)将数据传输给相邻节点或簇首节点,最终达到向 Sink 节点或基站报告事件的目的。无线传感器网络的信任管理模型的基本思想是采用直接信任值和推荐信任值对节点的信任度进行综合评估,通过记录各节点间的历史交互行为计算直接信任值,根据信任群组间的推荐形成推荐信任值或声誉值,从而对节点未来的行为进行预测,及时将恶意节点从网络中剔除。

无线传感器节点的计算、存储、通信能力有限,性能易受网络环境、节点电量等因素影响,与 P2P、网格等传统网络节点的行为表现并不相同,因此传感器节点的性能降低未必是恶意行为,特别是对于多功能集成智能传感器节点而言,一种功能降低并不影响其他功能的实现。EETM 模型将节点行为与节点当前性能相关联,在节点的性能基础上评估其信任值,增强了节点的使用效率,从而降低了能量消耗,延长网络的整体寿命。

2.1 网络模型

在平面结构的无线传感器网络中,所有节点处于平等地位,具有完全一致的功能。网络中没有中心节点,拓扑结构简单,一般采用自组织协同算法。本文设定为平面式的网络结构,所有节点均为静止的,每个节点均能采集数据,同时也能作为中继节点进行数据转发,节点间以多跳方式向 Sink 进行事件报告和数据传输。本文采用分布式信任管理方法,每个节点上维护和管理一个信任表,记录和更新邻居节点的信任值信息,当节点的信任等级低于可信阈值时,将其加入黑名单由 Sink 广播给所有节点。

2.2 信任状态与信任值定义

信任管理机制将信任值作为事件报告[9]和路由选择[6,12]的评价参数,参与到事件报告和路由选择的管理中,以确保数据与节点的可靠性[13]。

目前信任值表示方式主要有两种:连续信任值和离散信任值。本文采用[0,1]的实数来计算信任值,以提高信任评估的准确性,同时考虑无线通信的开销,又基于连续信任值对节点的信任状态进行评级,信任状态的评级数量可以由具体的网络应用背景决定,一般而言,为满足信任管理系统的基本要求至少分为可信状态、不确定状态和不可信状态,即 $N\geqslant 3$。

本文将信任状态划分为 5 种,即 $N=5$,$\text{state}^r(v_i)$ 表示节点 v_i 第 r 轮的信任状态,定义为:

$$\text{state}^r(v_i)=\begin{Bmatrix}\text{VT} & f\leqslant T^r(v_i)<1\\ T & g\leqslant T^r(v_i)<f\\ U & h\leqslant T^r(v_i)<g\\ S & l\leqslant T^r(v_i)<h\\ D & 0\leqslant T^r(v_i)<l\end{Bmatrix} \tag{1}$$

其中 VT,T,U,S,D 表示信任的 5 种状态,分别为极可信状态、可信状态、不确定状态、可疑状态和不可信状态,节点 v_i 的当前信任状态依据其当前的信任值来判断。$T^r(v_i)$ 为节点 v_i 第 r 轮的信任值,其定义将在下文中表示。参数 f,g,h,l 表示各信任状态阈值,用于划分信任状态,其中 $f_{r+1},g_{r+1},h_{r+1},l_{r+1}$ 表示第 r+1 轮的信任状态阈值,分别定义为:

$$f_{r+1}=\begin{cases}\dfrac{1}{2}\left(\dfrac{\sum\limits_{\text{state}^r(v_i)=\text{VT}}T^r(v_i)}{|\text{VT}|}+g_0\right) & |\text{VT}|\neq 0\\ f_r & |\text{VT}|=0\end{cases}$$

$$g_{n+1}=\begin{cases}\dfrac{1}{2}\left(\dfrac{\sum\limits_{\text{state}^r(v_i)=\mathbf{T}}T^r(v_i)}{|\mathbf{T}|}+g_0\right) & |\mathbf{T}|\neq 0\\ g_n & |\mathbf{T}|=0\end{cases}$$

$$h_{n+1}=\begin{cases}\dfrac{1}{2}\left(\dfrac{\sum\limits_{\text{state}^r(v_i)=\mathbf{U}}T^r(v_i)}{|\mathbf{U}|}+h_0\right) & |\mathbf{U}|\neq 0\\ h_n & |\mathbf{U}|=0\end{cases}$$

$$l_{n+1}=\begin{cases}\dfrac{1}{2}\left(\dfrac{\sum\limits_{\text{state}^r(v_i)=\mathbf{S}}T^r(v_i)}{|\mathbf{S}|}+l_0\right) & |\mathbf{S}|\neq 0\\ l_n & |\mathbf{S}|=0\end{cases} \tag{2}$$

其中 **VT**,**T**,**U**,**S** 分别代表极可信、可信、不确定和可疑状态下的节点集合,将四种信任状态下各节点集合当前的平均信任值与初始 f_0,g_0,h_0,l_0 值进行平均取值,从而实现节点信任状态具备自适应性。其中,信任状态阈值参数初始值 f_0,g_0,h_0,l_0 的设定由具体的应用场景决定,在本文实验中分别设定为 0.8、0.6、0.5 和 0.3。为计算方便,用整数形式映射信任状态值 SV,本文设定为 $\text{SV}=\{2,1,0,-1,-2\}$,其中正区间表示极可信和可信状态,负区间表示可疑和不可信状态,0 表示不确定状态。节点的初始信任状态的预定义方式一般有两种[1]:全部节点统一初始化为相同的信任状态,或经过一个初始化阶段进行信任状态初始化。另外,对于信任状态的初始化方法有三类[1]:高初始值、低初始值和中间值。本文采用统一初始状态方式和高初始值方法,初始状态下所有节点的信任状态均设为可信状态,即假设网络建立的初始阶段比较安全,整个网络属于一个组织所有,具有天然的彼此信任的基础,采用乐观的信任态度以缩短节点信任评估的时间开销。

在滑动窗口 W 下,记录两节点间交互的成功次数 $s_{i,j}$ 和失败次数 $u_{i,j}$,成功记为 1,失败记为 0,如图 1所示。

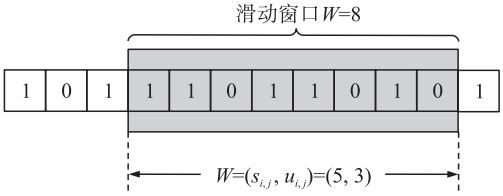


图 1　EETM 的滑动窗口机制

各节点记录和维护自己的信任值表,向相邻可靠的节点传输数据,基于数据转发率评价其他节点的行为,同时每隔一段周期更新当前第 r 轮相应节点的直接信任值和间接信任值信息。

在滑动窗口 W 下,基于统计学的 $beta(\alpha,\beta)$ 分布函数,其中 α,β 为两个参数,令 $\alpha=s_{i,j}+1$,$\beta=u_{i,j}+1$[14],定义节点 j 在节点 i 上的直接信任值 $\text{DT}_{i,j}$ 为:

$$\text{DT}_{i,j}=\frac{s_{i,j}+1}{s_{i,j}+u_{i,j}+2} \tag{3}$$

节点 j 在节点 i 上的间接信任值 $\text{IT}_{i,j}$ 定义为:

$$\text{IT}_{i,j}=\frac{\sum\limits_{k\in\mathbf{VT}\cup\mathbf{T}}\text{SV}_{i,k}\cdot\text{DT}_{k,j}}{\sum\limits_{k\in\mathbf{VT}\cup\mathbf{T}}\text{SV}_{i,k}} \tag{4}$$

其中 $\text{SV}_{i,j}$ 中表示节点 j 在节点 i 上的信任状态值,$k\in\mathbf{VT}\cup\mathbf{T}$ 表示节点 **k** 来自于信任状态为极可信状态 **VT** 和可信状态 **T** 的节点集合,即节点 j 在节点 i 上获得的间接信任值 $\text{IT}_{i,j}$ 是由所有可靠节点计算得到的,对于不确定状态和可疑状态节点的推荐信任值不予考虑。

在无线传感器网络的信任管理中,为尽可能减少节点间不必要的查询和计算,同时保证足够的交互次数以预测节点行为,本文在不同阶段分别采用不同的信任值计算方式来计算节点间的信任值,节点 j 在节点 i 上的信任值 $T_{i,j}$ 定义为:

$$T_{i,j}=\begin{cases}\mathrm{IT}_{i,j} & |\mathrm{HI}_{i,j}|\leqslant W\\ \lambda\cdot\mathrm{DT}_{i,j}+(1-\lambda)\,\mathrm{IT}_{i,j} & W<|\mathrm{HI}_{i,j}|<2W\\ \mathrm{DT}_{i,j} & |\mathrm{HI}_{i,j}|\geqslant 2W\end{cases}\quad(5)$$

其中$|\mathrm{HI}_{i,j}|$表示节点 j 与节点 i 交互的次数,W 表示滑动窗口的大小。当节点间交互次数不大于 W 时,信任值 $T_{i,j}$即为间接信任值,当节点间交互次数不小于 $2W$ 时,信任值 $T_{i,j}$即为直接信任值,否则信任值由直接信任值和间接信任值共同计算得到。其中参数 λ 表示直接信任值的权重,$\lambda=\dfrac{|\mathrm{HI}_{i,j}|-W}{W}$。

本文采用分段函数计算综合信任值,以减少无线传感器网络的通信代价。只有在节点间交互次数不足以准确评估信任值时,节点向邻居节点发送推荐信任请求。

2.3 执行度与节点能力

Rasch 理论是项目反应理论中的一种模型,由丹麦数学家和统计学家 Georg Rasch 提出的一个潜在特质模型,并在心理学、教育学、统计学和医学中得到了广泛的应用。通过个体在项目上的表现来测量不可直接观察的、潜在的变量,如态度、能力等等。根据 Rasch 模型的基本原理,个体对任务所做出的反应概率可以用个体的能力与该任务难度的一个关于被试者的能力与任务难度的差异值的指数函数来表示。对 Rasch 模型中的客观测量有两个基本要求[4]:1)对于任何任务,能力高的比能力低的个体有更大的可能性成功;2)对于任何个体在容易任务上的表现应始终好过在困难任务上的表现。Rasch 模型基本原理的计算方法表达为 $P\{X_{mi}=1\}=\dfrac{e^{\beta_m-\delta_i}}{1+e^{\beta_m-\delta_i}}$,其中 $P\{X_{mi}=1\}$ 表示随机选择第 m 个被试者对任务 i 做出成功反应的概率;β_m 是是被试者 m 的能力水平;δ_i 表示任务 i 的难度参数;e 是自然指数。

基于 Rasch 的基本理论,定义节点的执行度为:

$$E_{i,j}=P(\beta_{i,j},\delta_k)=\frac{e^{\beta_{i,j}-\delta_k}}{1+e^{\beta_{i,j}-\delta_k}}\quad(6)$$

其中 $\beta_{i,j}$代表节点 i 观测到的节点 j 的能力,δ_k 代表任务类型为 k 的难度,$P(\beta_{i,j},\delta_k)$代表能力值为 $\beta_{i,j}$ 的节点在执行难度值为 δ_k 的任务时成功的概率,即节点 j 在节点 i 上的执行度 $E_{i,j}$。当 $E_{i,j}=0.5$ 时,表示节点 j 当前的观测能力与任务难度相当,成功完成该任务的概率为 50%。

由于节点的能力水平受节点当前的剩余能量和物理环境等多种综合因素影响,因此无法通过具体的物理参数直接计算获得节点的能力值,本文用信任值预测节点行为能力,且仅当节点 j 在节点 i 上的信任状态发生改变时,更新计算节点 i 对节点 j 的观测能力值 $\beta_{i,j}$,定义为:

$$\beta_{i,j}=\ln\left(\frac{T_{i,j}}{1-T_{i,j}}\right)\quad(7)$$

根据实际的无线传感器网络应用背景(如根据数据传输类型)预先设定标准任务,并确定各项标准任务的难度参数 δ_k 和难度种类本文设定任务的难度种类为 5 种,$\delta_k=\{2,1,0,-1,-2\}$,其中由 Rasch 基本理论的难度参数定义可知,难度参数值越高代表任务的难度越高。

3 EETM 算法

EETM 信任模型采用多跳的形式传输数据,采用分布式信任管理结构,由各节点管理和维护相邻节点的信任信息,在其信任值表中记录各邻居节点的信任值信息,包括节点的直接信任值、间接信任值、信任状态、观测能力值和节点执行度等信任信息。算法详细描述了 EETM 算法,基于信任路由协议选择下一跳节点以实现可靠的数据转发,同时根据数据转发率,记录下一跳节点的行为结果,每隔一段时间,更新邻居表中所有节点的信任值信息。

算法:EETM 算法

```
for 节点 j 从节点集合 VT,T 中随机选择
  if E_{i,j}<0.5 then
    Request(下一节点);
  else 节点 i 发送事件数据
    if 数据成功转发 then
      Set 行为记录值为 1;
    else Set 行为记录值为 0;
    end if
  end if
end for
for
  if |HI_{i,j}|<=W
    Request 间接信任值从可信节点集合中
    Update(IT_{i,j})
    T_{i,j}=IT_{i,j}
  else if |HI_{i,j}|>W
    Update(DT_{i,j})
    if |HI_{i,j}|>2W
      T_{i,j}=DT_{i,j}
    else T_{i,j}=λ·DT_{i,j}+(1-λ)·IT_{i,j}
end for
Update(f,g,h,l)
for
```

```
  Update(SV_{i,j})
  if SV_{i,j} ≠前一状态值 then
    Update(β_{i,j})
  end if
end for
```

4　实验分析

4.1　仿真环境

根据本文前面所述的网络模型,采用 TRMSim[15] 仿真平台对 EETM 模型和 RFSN 进行了一系列模拟实验,分别在能量消耗、事件报告率、恶意节点检测率三个方面对实验结果进行分析,与 RFSN 信任模型进行比较,RFSN 是一个较为完整的无线传感器网络信任管理系统,在同领域中得到广泛认可。本文提出的 EETM 与 RFSN 信任管理系统类似,均采用直接信任和间接信任两种信任评估方式进行计算,同时与 RFSN 信任管理系统所采用的数学方法相同,均利用 beta 分布函数方法计算直接信任值,而该方法具有计算方法简单、计算量小等特点。因此本文将 RFSN 作为与 EETM 信任模型的实验比较分析对象。

基本的实验参数如表 1 所示。

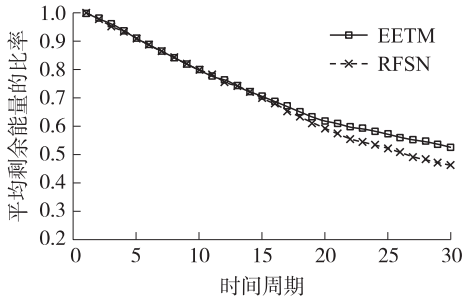
表 1　实验参数

参数	数值
节点数量	72
范围	100 m×100 m
事件感应距离	20 m
节点初始能量	2 J
$E_{\text{receiving}}$	1 nJ/bit
E_{elec}	50 nJ/bit
ε_{fs}	10 pJ/(bit·m^{-2})
ε_{emp}	1.3 pJ/bit

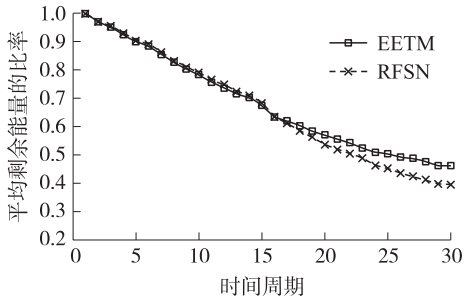
4.2　实验结果分析

图 2 显示了在恶意节点比率分别为 10% 和 30%,的网络环境中剩余节点的平均能量的比率。随着实验轮数的增加,我们观察到经过 15 轮的时间周期之后,采用 EETM 信任模型,网络中所剩余的能量要与采用 RFSN 信任模型相比高,且随着时间的增长,两者差距越来越大,说明 EETM 模型能够明显降低节点的能量消耗。实验中,在 15 轮周期之前两者无能量差异的原因在于,此时无论是 RFSN 还是 EETM 信任模型,由于信任证据信息不足,即节点间的交互次数尚未满足对信任值进行评估的数量,因此,信任系统也没有正式参与到节点的路由选择中。

图 3 显示了恶意节点比率分别为 10%、20%、30% 和 40% 的网络环境中,从源节点探测到事件数据开始经过多跳路由转发,到达目的 Sink 节点后的平均事件数据报告率。我们观察到无论是哪一种恶意节点比率,EETM 的事件数据报告率都高于 RFSN 的事件数据报告结果,特别是当恶意节点数量在 10% 左右时,两者差距最显著。随着恶意节点比例增高,两者差异不是很明显,但 EETM 的结果仍好于 RFSN 信任模型。



(a)10%恶意节点



(b)30%恶意节点

图 2　平均能量消耗比率

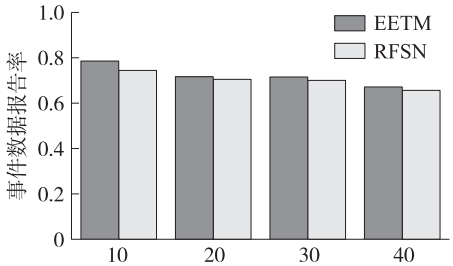


图 3　平均事件数据报告率比较

图 4 显示了恶意节点比率分别为 10%、20%、30% 和 40% 的网络环境中,每组 5 次随机模拟实验的平均恶意节点检测率。我们观察到使用 EETM 进

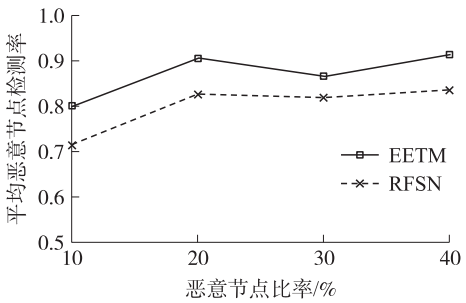


图 4　恶意节点比率对事件检测的影响

行恶意节点检测时,恶意节点的检测率均达到了80%以上,结果大大好于 RFSN 信任模型的恶意节点检测率。

图5显示了40轮评估周期中,网络所剩余的存活可用节点数量的变化。我们观察到在第18轮评估周期之后,采用 EETM 信任模型的存活可用节点的平均数量均要高于 RFSN 信任模型,因此,从实验结果可以说明 EETM 信任模型能够延长网络的整体生存周期。

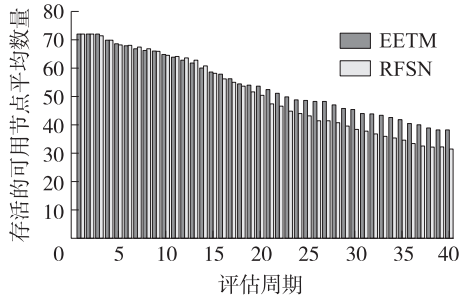


图5 网络生存期分析

5 结论

本文提出的 EETM 信任模型引入节点能力作为信任度的度量参数,将节点性能与节点的信任值相关联,提出节点执行度这一概念,确保节点信任评估的公平性。另外为减少无线传感器通信代价,采用分段式计算综合信任值。仿真试验结果表明 EETM 信任模型能够有效识别网络中的恶意节点,提高事件报告率,降低了信任机制在平面结构的无线传感器网络应用中带来的额外开销,提高了节点的使用率,延长了网络生存周期。

参考文献:

[1] 荆琦,唐礼勇,陈钟. 无线传感器网络中的信任管理[J]. 软件学报,2008,19(7):1716-1730.

[2] Yanli Y, Keqiu L, Wanlei Z, et al. Trust Mechanisms in Wireless Sensor Networks: Attack Analysis and Countermeasures[J]. Journal of Network and Computer Applications,2012,35(3):867-880.

[3] 王建萍,李明,周线为. 基于声誉和信任组的无线传感器网络实体认证研究[J]. 传感技术学报,2008,21(10):1780-1784.

[4] Lopez J, Roman R, Agudo I, et al. Trust Management Systems for Wireless Sensor Networks: Best Practices [J]. Computer Communications,2010,33(9):1086-1093.

[5] Wright B D, Mok M. Rasch Models Overview [J]. Journal of Applied Measurement,2000,1(1):83-106.

[6] Tanachaiwiwat S, Dave P, Bhindwale R, et al. Secure Locations: Routing on Trust and Isolating Compromised Sensors in Location-Aware Sensor Networks [C]//Proceedings of the SenSys 2003. New York, ACM Press,2003:324-325.

[7] Graneriwal S, Balzano L, Srivastava M. Reputation-Based Frame-Work for High Integrity Sensor Networks[J]. ACM Transactions on Sensor Networks,2008,4(3):1-37.

[8] Shaikh R A, Jameel H, d'Auriol B J, et al. Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks[J]. IEEE Transactions on Parallel and Distributed Systems,2009,20(11):1698-1712.

[9] Krasniewski M, Rabeler B. TIBFIT: Trust Index Based Fault Tolerance for Arbitrary Data Faults in Sensor Networks[C]//The International Conference on Dependable Systems and Networks, Washington DC: IEEE Computer Society,2005:672-681.

[10] 顾伟刚,马征,王国军. 基于信任模型使用随机分散路由的安全数据收集协议[J]. 传感技术学报,2011,24(7):1060-1065.

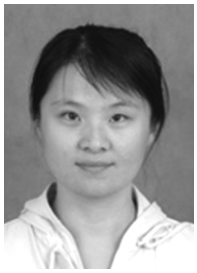
[11] Hur J, Lee Y, Hong S M, et al. Trust Management for Resilient Wireless Sensor Networks[C]//Proceedings of the ICISC 2005, Berlin, Heidelberg: Springer-Verlag,2006:56-68.

[12] 王潮,贾翔宇,林强. 基于可信度的无线传感器网络安全路由算法[J]. 通信学报,2008,29(11):105-112.

[13] Xiao X, Peng W, Hung C, et al. Using Sensor Ranks for in-Network Detection of Faulty Readings in Wireless Sensor Networks[C]// Proceedings of the Sixth ACM Workshop on Data Engineering for Wireless and Mobile Access. Beijing: ACM Press,2007:1-8.

[14] Jøsang A. A Logic for Uncertain Probabilities [J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001,9(3):279-311.

[15] Múrmol F G. TRMSIM-WSN: Trust and Reputation Models Simulator for Wireless Sensor Networks [C]//The IEEE International Conference on Communications, Dresden: IEEE Computer Society,2009:1-5.



于艳莉(1980-),女,大连理工大学计算机科学与技术学院博士研究生,主要研究方向为无线传感器网络信任管理,yuyanli07@163.com;

李克秋(1971-),男,大连理工大学计算机科学与技术学院教授,博导,计算机科学与技术学院副院长。主要研究领域包括计算机网络与安全,云计算,web 技术,多媒体应用等,keqiu@dlut.edu.cn。