无线传感器网络中一种基于行为可信的访问控制机制

周鸣争 汪 军 严 楠 刘 涛

(安徽工程大学计算机与信息学院 芜湖 241000)

摘 要 访问控制是无线传感器网络的一种重要应用,已有研究工作大多是通过相邻传感器之间的密钥交换来实现。从传感器行为的空间相关性和时间相关性入手,提出了一种基于相似度的以局部检测为主的分布式传感器行为可信的访问控制机制。该机制通过检验传感器本地采样值构成的时空相似度与传感器行为随机过程统计特征的符合程度来实现行为信任的访问控制。模拟仿真试验表明,该机制可以减少传感器之间的数据交换,当网络中10%的传感器存在不安全行为时,该模型可以检测到95%的不可信传感器。

关键词 无线传感器网络,访问控制,行为信任,安全

中图法分类号 TP393 **文献标识码** A

Access Control Mechanism Based on Behaviour Trust in Wireless Sensor Networks

ZHOU Ming-zheng WANG Jun YAN Nan LIU Tao

(School of Computer Science & Information, Anhui Polytechnic University, Wuhu 241000, China)

Abstract Access control is an important application of wireless sensor networks. Previous works are implemented by exchanging key among neighboring sensors. Considering that in many cases, an sensors behaviour is both spatially and temporally correlated, this paper proposed a distributed and localized behaviour trust mechanism based on similarity. this mechanism implements behaviour trust access control by using statistical hypothesis test for matching the reading sequence of sensors and statistical characters of the behaviour. The simulation results show that the mechanism can reduce the network traffic, can detect as much as 93% of the not trusty sensors when 10% of sensors are not security.

Keywords Wireless sensor network, Access control, Behaviour trust, Secure

1 引言

与传统访问控制不同,传感器网络本身特点决定了传感器网络访问控制研究的复杂性。主要难点有两个:其一是由于传感器只有有限的能量,而消息通信通常消耗了传感器大部分的能量,因此要尽量减少传感器网络中的消息通信。这就要求访问控制算法必须是一种分布式和局部的算法。其二是攻击者捕获低成本的传感器节点,破获密钥信息,进而插入恶意节点输出恶意数据来破坏网络正常获取信息的能力。因此,安全的访问控制是实现无线传感器网络安全的一个重要内容,为此目前已经有很多学者对其进行了广泛的研究[1-3]。

Zinaida Benenson 在分析当前 WSN 的数据访问方法的基础上提出了 WSN 中一种新的安全问题—授权查询问题[4]。并给出了一种基于 ECC 公钥加密系统的(n,t)查询授权的方法,以这种方式使得未授权的用户无权随意访问 WSN 中的数据。其基本思想是 WSN 内部节点使用对称密钥建立网内的数据传输路径,用户端采用 CA 公钥证书方式进行访问授权,将用户可以直接通讯的一跳邻居节点作为认证节点集,使用(n,t)节点授权认证的方法验证用户身份的合法性。只有得到足够多($\geqslant t$)节点的认证签名的用户查询请求,才能允许在其 WSN 中转发并响应目的节点。Kirk H. M. Wong 等人给出了一种基于强密码的动态用户授权模型[5]。其用户授权的基本思想是将传感器节点分为三类:网关节点、登录节点、信息提供节点。用户先在网关节点注册用户的信息和登录密码,网关节点将注册信息保存在数据库中。当用户欲向 WSN 发出查寻请求时,用户通过向 WSN 中的登录节点提交 UID 和密码来登录 WSN,验证通过后,用户便可以向 WSN 发出查询请求并使其响应目的节点。WenSheng Zhang 等人给出了一种基于移动轨迹的移动基站节点的最小授权模型[6]。该模型的基本思想是将 WSN 所监测的物理环境划分成小栅格,用小栅格来逼近移动基站的移动轨迹,以移动轨迹和移动基站信息为参数,基于 Blundo 模型[7]计算移动基站和传感器节点之间的通信密钥,通过这种通信密钥的建立来实现对移动基站的访问权限控制。HaoDong Wang 等人给出了一种基于权限等级访问控制列表(Access Control List, ACL)的分布式访问控制模型[8]。其基本思想是基于 ECC 的公钥加密系统,将 ACL 与用户信息作为证书授予用户,使用(n,t)节点授权认证方法对用户的合法性进行认证,并用 Blundo 对称密钥加密方案完成认证签名,当用户得到 n 个节点的认证签名后,其查询请求便可以在 WSN 中转发,目的节点检查用户的访

本文受安徽省教育厅自然科学基金重点项目(KJ2007A046)资助。

周鸣争(1958—),男,教授,主要研究方向为计算机网络与信息安全;**汪 军**(1975—),男,硕士,副教授,主要研究方向为信息安全;**严 楠**(1979—),男,硕士,讲师,主要研究方向为无线网络;**刘 涛**(1972—),女,硕士,副教授,主要研究方向为信息安全。

问权限和认证情况并响应用户请求。Perrig 针对传感器网络提出了 SPINS[9]安全协议簇，包括 SNEP 和 μTESLA 两个协议。SNEP 提供了数据的机密性、完整性、鲜活性。μTESLA 提供了数据广播的访问控制，基站作为密钥分发中心(KDC)广播认证密钥。基于 μTESLA 协议，D. Liu 等提议了多层和适合于多个发送者的广播访问控制协议[10,11]。其基本思想是将访问控制分成多层，使用高层密钥链认证低层密钥链，低层密钥链认证广播数据包。

当前关于访问控制问题的研究主要集中在密钥的分配管理、节点授权、数据在网络中传输的机密性和隐私保护、数据的完整性、数据聚合的安全性、网络的容侵容错、路由的安全、用户的身份认证等方面。其机制主要采用基于密钥管理模式来解决节点的访问控制问题，但并不能处理被捕获传感器节点恶意攻击行为而造成的不可靠和不安全问题[12,13]。

近年来，网络的可信研究已成为一个研究热点[14,15]。网络可信技术是在原有网络安全技术的基础上增加行为可信的安全新方法，强化了对网络状态的动态处理，为实施智能自适应的网络安全和服务质量控制提供了策略基础。所谓信任模型，是指通过节点本身及与其它节点交互的历史来建立量化的评价体系，以信任值度量节点的可信程度。本质上是节点的实际物理属性和其行为的一个综合能力的反映。网络节点信任不仅包括对节点的身份信任，也包括对节点的行为信任。

与已有工作不同，本文将可信计算思想与传感器网络访问控制相结合，从传感器节点行为的空间相关性和时间相关性入手，利用传感器状态估计向量(或测量值)的标称化差定义了节点之间相似度和相似度矩阵，用节点之间空间信息形成一致性测度，用节点之间的时间信息形成可靠性测度，利用其一致性和可靠性测度定义了节点的行为可信度，提出了一种基于行为可信的访问控制机制。该机制可以通过检验本地读数序列来计算信任值，以减少传感器之间因频繁地交换数据带来的通信开销，从而有效地节省传感器的能量。这一机制既可在数据层实现，也可扩展到应用层。本文第 2 节概述了传感器节点信任值的计算及可信行为决策控制策略；第 3 节介绍了基于行为可信的访问控制机制；第 4 节给出仿真及结果分析，证实了该算法的有效性；最后给出了本文的结论。

2 节点行为信任模型

传统信任模型认为信任就是认证信任的实体和不信任的实体，并拒绝不信任实体的访问，是为了保证网络环境安全性的一种安全机制。在无线传感器网络中，行为认证过程不仅具有空间相关性，而且具有时间相关性。也就是说，参与认证的传感器节点行为(即节点的输出数据)在进行认证时不仅与节点本身的历史有关(时间相关)，也会与同区域内其它节点的数据相关(空间相关)，并且节点行为的特征随时间的变化规律具有某些统计特征[16]。因此，可以将节点行为特征随时间的变化规律用随机过程来描述，简称为认证节点的行为过程。并利用同一区域内传感器采集的数据在时间、空间上的相关性进行节点行为信任值计算，从而减少传感器之间的数据交换。它是一种分布式和局部的算法。

2.1 相似度矩阵

若传感器网络中参与认证的传感器集合为 $S=(s_1,s_2,\cdots,s_n)$，$z_i(k)$表示 k 时刻传感器 s_i 的输出。设系统可用如下状态方程和输出方程描述：

$$\begin{cases} X(k+1)=\Phi(k)X(k)+G(k)V(k) \\ Z(k)=H(k)X(k)+W(k) \end{cases} \tag{1}$$

式中，$\Phi(k)$，$G(k)$，$H(k)$分别表示状态转移矩阵、过程噪声分布矩阵及输出矩阵，式(1)中省略了各传感器编号的下标；$V(k)$和 $W(k)$分别表示具有零均值和正定协方差矩阵的高斯噪声向量。采用 Kalman 滤波算法[17]进行状态更新。在 k 时刻，由于传感器所处的噪声环境和自身行为的不一致，会形成略有差异的状态估计向量。为度量这一差异，定义如下的状态估计向量的标称化差：

$$u_{ij}(k)=C_{ij}^{-1/2}(k|k)[\hat{X}_i(k|k)-\hat{X}_j(k|k)] \tag{2}$$

式中，$C_{ij}(k|k)=P_i(k|k)+P_j(k|k)$，表示两个测量的估计误差协方差之和。采用正态型隶属度函数的模糊测度，定义 k 时刻两状态向量的相似度为

$$d_{ij}(k)=\exp[-bu_{ij}^T(k)u_{ij}(k)] \tag{3}$$

式中，b 是系数，$u_{ij}(k)$是列矢量，$d_{ij}(k)$是标量。因传感器网络中节点由独立同质传感器组成，故状态向量间的相似程度也表征了测量值自身之间的相似程度，二者是一致的。当网络中传感器无法用状态方程表示时，可直接用测量值计算相似度。

由相似度可得 k 时刻参与认证各传感器的相似度矩阵为

$$D(k)=\begin{bmatrix} 1 & d_{ij} & \cdots & d_{1n} \\ d_{21} & 1 & \cdots & d_{2n} \\ & & \ddots & \\ d_{n1} & d_{n2} & \cdots & 1 \end{bmatrix} \tag{4}$$

相似度矩阵包含了 k 时刻传感器网络 $S=(s_1,s_2,\cdots,s_n)$的测量在空间分布的信息，是进行传感器节点行为空间信任计算的尺度。同样，时间系列$\{D(k),k=1,2,\cdots\}$包含了到当前时刻为止的节点在时空分布的信息，是进行传感器节点行为信任数据时空计算的尺度。

2.2 基于相似度的节点行为信任度的计算

设 $c_i(k)$是 k 时刻传感器节点 i 的一个计数器(初值为零)。考察式(4)中 $D(k)$的第 i 行，若 $d_{ij}(k)\geqslant E_1$(E_1 是设定的阈值)，则计数器加 1。此时第 i 行扫描之后的 $c_i(k)$终值表示 k 时刻与传感器 i 测量数据较为相似的测量数据数。$c_i(k)$大，表示 k 时刻传感器 i 的测量值与大多数测量值一致，这些测量值可能组成一个真值的聚类；$c_i(k)$小，表示 k 时刻传感器 i 的测量值与大多数测量值不一致，而成为“野值”的可能性较大，节点的信任度较低。因此 $c_i(k)$是测量值一致性的度量。定义 k 时刻传感器 i 的一致性测度为

$$p_i(k)=c_i(k)/n \tag{5}$$

显然有 $0\leqslant p_i(k)\leqslant 1$，这实际上是一种可能性测度。于是，由传感器组 $S=(s_1,s_2,\cdots,s_n)$得到的 k 时刻一致性向量为 $p(k)=[p_1(k),p_2(k),\cdots,p_n(k)]$。

对传感器 i 而言，除了与其他传感器的行为一致性问题外，还存在自身的行为可靠性问题，这种可靠性往往通过自身测量的时间系列表现出来。将传感器的周期性读数视作一个按照时间次序排列的序列，该读数序列本质上是节点行为过程的一个样本值。考虑到传感器只有有限的计算和存储能

力，因此在传感器上只保存一段时间内的样本值。设$[p_i(1), p_i(2), \cdots, p_i(k)]^T$表示传感器$i$的一致性测度的时间序列，令

$$\bar{p}_i(k)=\frac{1}{k}\sum_{t=1}^{k}p_i(t) \tag{6}$$

表示平均或综合的一致性测度。如果序列波动不大，则说明传感器i的性能比较稳定或环境噪声较小，即可靠性较高。故可直观地定义传感器i的可靠性测度为一致性测度的方差，即

$$\sigma_i^2(k)=\frac{1}{k}\sum_{t=1}^{k}[\bar{p}_i(k)-p_i(k)]^2 \tag{7}$$

用于节点行为信任可靠属性值的计算。在信任计算中信任度高的传感器节点应是一致性较大且可靠性较高者，即$\bar{p}_i(k)$较大而$\sigma_i^2(k)$较小。对传感器i而言，$\bar{p}_i(k)$较大并不意味着$\sigma_i^2(k)$较大或较小，反之亦然。故引入映射$f[\bar{p}_i(k), \sigma_i^2(k)]$进行综合，使节点行为可信度与$\bar{p}_i(k)$正相关，且与$\sigma_i^2(k)$负相关。如用双线性定义行为可信度：

$$q_i(k)=f[\bar{p}_i(k), \sigma_i^2(k)]=[1-a\sigma_1(k)]\bar{p}_i(k) \tag{8}$$

式中，a是一个合适的系数，通常$0<a\leqslant 1$。这是因为一致性与可靠性相比在行为信任中显得更为重要一些。这样，便可根据$q(k)$值的大小对传感器信任度进行排队，然后采用不同的门限方法进行信任度等级的划分。

相似度计算需要计算n个传感器两两之间的标称化差，一致性测度计算需要将n_2维的相似度矩阵元素与阈值逐一比较，计算的复杂度为$O(n^2)$。为减少计算量，在计算综合一致性测度和可靠性测度时，应使用如下递推算法：

$$\bar{p}_i(k)=\frac{k-1}{k}\bar{p}_i(k-1)+\frac{1}{k}p_i(k) \tag{9}$$

$$\sigma_i^2(k)=\frac{k-1}{k}\left\{\sigma_i^2(k-1)+\frac{1}{k}[p_i(k)-\bar{p}_i(k)]^2\right\} \tag{10}$$

3 基于行为可信的访问控制算法

3.1 节点行为可信等级的划分

为了能有效地利用节点行为信任值进行访问控制，可将各个节点可信度按实际应用的需求，划分为L个信任等级，并将这些信任等级从高到低顺序编号为整型变量$r, r\in[1, L]$，它们所代表的信任区间范围从高到低的顺序分别是

$$\left[1-\frac{TH_1}{L-1}, 1\right], \left[1-2\times\frac{TH_1}{L-1}, 1-\frac{TH_1}{L-1}\right], \cdots, \left[TH_0, 1-(L-2)\times\frac{TH_1}{L-1}\right], [0, TH_0] \tag{11}$$

式中，TH_0是信任阈值，即当节点的行为信任值小于TH_0时，进行认证的节点就不信任该节点，且$TH_0+TH_1=1$，例如，我们假设$L=5$，即行为信任等级分为5级，分别为非常信任（信任等级为1）、信任（信任等级为2）、比较信任（信任等级为3）、基本信任（信任等级为4）和不信任（信任等级为5）。信任阈值TH_0的取值通常基于式（1）：

$$TH_0=\frac{q_n(t)-q_e(t)}{2} \tag{12}$$

式中，$q_n(t)$是传感器节点在正常行为时的信任期望函数，在比较稳定的环境（例如自然环境中的温度）中，可以认为$q_n(t)$是一个常数；$q_e(t)$是传感器节点在不正常错误行为中信任的期望函数；t是传感器采样的时刻。考虑到节点行为的特征只有在行为发生后才能被传感器感知，并且行为特征的变化规律与行为发生的具体时刻无关，只与距离行为发生时刻的时间间隔有关，因此，假设行为在t_0时刻发生，并且行为（特征）至少可以持续T_{th}时间，则行为过程分别满足$q_e(t)=q_e(t-t_0)=q_e(\tau), 0\leqslant\tau=t-t_0\leqslant T_{th}$。并且定义$q_e(0)$为行为刚刚发生时行为特征的期望值，$TH_0(0)$作为行为的信任阈值。$q_e(t)$可以在部署前保存在传感器内存中或是在部署后通过汇聚点（sink node）将$q_e(t)$通过消息分发给各个传感器。

3.2 信任推荐

无线传感器网络关键服务是环境感知并将感知数据传输到基站，即数据汇集和数据转发。因此信任关系可分为簇内信任和路径信任。对于任何一个节点，簇内信任可依据自己对邻居节点的监控，根据式（9）、式（10）和式（12）计算其作为主体关于被监控邻居节点（客体）的直接信任值。而路径信任则需要邻居节点的推荐。假设有m个节点$E_1, E_2, E_3, \cdots, E_m$，节点$E_i$和$E_{i+1}(0\leqslant i\leqslant m-1)$存在信任值$q_i$，这时常常需要据此计算$E_1$对于$E_m$的信任值$q$。由于$E_1$对于$E_m$的信任值是通过中间节点传递的，因此把这叫做信任推荐，其计算算法如下：

$$q=q_1\otimes q_2\otimes\cdots\otimes q_m \tag{13}$$

式中，$\otimes$被称作信任值逻辑乘计算符。由于q_z值在$[0,1]$上，由式（13）可知，推荐信任值不高于推荐节点对被推荐客体节点的信任值，也不高于主体对推荐节点的信任值。符合sun[18]指出的信任关系必须满足串联传递不会增加信任值的公理。

3.3 信任合成

在无线传感器网络环境中，众多节点间信任关系构成了一个信任网络，两个节点之间常常存在多条路径信任推荐值。这时，就需要将这些信任值合并成一个推荐信任值。

假设存在n个推荐信任值$q_1, q_2, q_3, \cdots, q_n$，则可以根据下面的算法合并成一个推荐信任值$q_i$。

$$q=q_1\oplus q_2\oplus\cdots\oplus q_n \tag{14}$$

其中$\oplus$的定义为

$$q_i=\begin{cases}q_1, & q_1\geqslant q_2\\ q_2, & q_1<q_2\end{cases} \tag{15}$$

每个主体节点在获得对客体节点直接信任值和推荐信任值后，就需要将这些信任值合并成一个信任值。假设主体节点S对客体节点A的直接信任值为q_{sad}，而相关节点的推荐信任值为q_{sai}，则可以根据式（16）将其合并成一个主体S对客体A的信任值q_{sa}

$$q_{sa}=\begin{cases}q_{sad}, & q_{sad}\geqslant q_{sai}\\ q_{sad}+(1-q_{sad})(q_{sai}-q_{sad}), & q_{sad}<q_{sai}\end{cases} \tag{16}$$

式（16）反映了社会关系中的信任产生思想，即解决如何看待自身经验以及他人推荐的重要性。在现实社会关系中，主体对客体产生一个信任值，通常是在自己直接信任值的基础上进行调整，如果自己的直接信任值高，而他人推荐的信任值低，则不会影响到自己对客体的信心。若自己的直接信任值低，而他人推荐的信任值高，则会对客体的信任值进行微调。

3.4 信任更新

在无线传感器网络的运行过程中，需要考虑信任的更新问题，每当进行一段时间周期（如经历 n 次事件后），节点需要重新计算其信任值，为减少计算量，在使用式(9)、式(10)递推算法的同时，引入一个权重因子 λ，通过式(17)来平衡当前周期信任值 Q 与上一周期信任值 Q' 的重视程度。

$$Q=(1-\lambda)Q+\lambda Q' \tag{17}$$

3.5 算法描述

基于行为可信的访问控制算法的主要思想是在现有的身份认证机制的基础上增加节点行为信任的控制和管理，强化对网络节点行为可信状态的动态处理；传感器网络为分族的层次结构，族头负责本族内部节点的行为安全认证，路由节点之间由下一跳节点负责对上一跳节点的行为认证；进行认证的族头节点在进行认证时，首先对认证节点的行为信任等级进行确认，如果节点的行为信任等级为不信任，则丢弃该节点的输出数据或断开其连接。否则将按节点的行为信任等级进行相应的权限处理，以使其认证过程安全、可靠。

算法分为两个阶段，首先，族头节点按网络部署时所设置的密钥管理（如所有节点共享一个主密钥方式）进行身份认证，如果失败，则将该传感器的安全状态标记为 false，拒绝访问请求；然后，安全认证的族头节点与相关节点交换信息，计算密钥认证通过的请求服务节点的信任度 q_i 与信任等级。当传感器节点信任等级 $r_i(t)$ 大于 $TH0$ 时，则将该传感器的状态标记为 false，拒绝访问请求；否则将其状态标记为对应的访权限 W_i，响应完成其相应权限的访问。具体描述如表 1 所列。

表 1　行为可信的安全认证算法

```
//For each authentication sensor;
int turst authentication (qe,a,b )
{
  int status = Wi;
  int i;
   logical j
   j=keyauthenticated(sensor i)
   if (not j)
     statusi= false;
  while(j)
   {
     receiving data from neighbors sensor;.
     computing the TH0;
     computing the qi and ri for sensor i;
  if (ri>TH0 )
       statusi= Wi;
     else
       statusi= false;
       }
     if (statusi= Wi)
       access control with Wi
     else
       do nothing;;
reset();
}//end turst authentication
```

表 1 中的算法利用传感器本地读数的时间与空间相关性进行信任度计算，T_{th} 时间后，只有位于实践汇聚区域中的传感器才需要与其邻居进行数据交换，所以传感器进行数据交换的频率为 $1/T_{th}$。传感器网络在 T_{th} 时间内产生的消息量为 $\alpha \cdot n \cdot N$。α 代表区域面积与传感器的部署区域面积的比值，$0<\alpha \leqslant 1$。所以，当数据汇聚特征的持续时间 T_{th} 大于传感器的采样间隔 ΔT 或者融合区域小于传感器网络的部署区域时，该算法只需其 α/m 的消息量，因此是高效节能。

4　仿真及其结果分析

4.1 仿真环境

在仿真试验中，$n=1024$ 个传感器节点均匀部署在 50a×50a 的区域中。假设传感器的无线通信半径为 $\sqrt{2}a$。每个传感器节点能量初值为 2J，数据包大小为 525bytes，控制包大小为 256bytes，不信任行为为恶意伪装攻击和节点故障而引起的不正确消息，即节点的身份认证是正确的，而传输的数据是错误的，且与正常值有一定的偏差。由于假设节点行为具有显著不正常的特征，令 $q_n(t)=0.25$ 为常数。假设传感器的采样频率为 10Hz，即 $\Delta T=0.1$s，行为特征的持续时间 $T_{th}=1$s，则在 T_{th} 时间内的采样次数 $m=10$。取式(3)中 $b=5$；采用式(5)定义的一致性测度，取 $E_1=0.5$，取式(8)中 $a=1$。图 1 是模拟试验的部署图，图中每一个点 (x,y) 代表一个传感器，$1\leqslant x,y\leqslant 50$。图中方块表示不信任行为的传感器。其中，不信任行为传感器的数目为 103 个，约占传感器总数的 10%。为测试本文算法性能，将实验结果与 SNEP 算法的节能性进行了比较。仿真平台采用 SENSE[19]，这是一个专门用来模拟传感器网络的环境的平台。在 SENSE 中，被模拟的传感器网络分为 4 个层次：应用层、网络层、MAC 层和物理层。我们的算法建立在 MAC 层。然后，对算法的不信任行为检测概率、数据汇聚的精度和能耗进行了仿真分析。

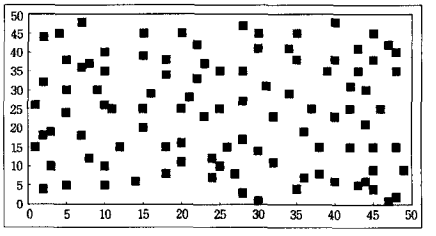

图 1　模拟试验部署

4.2 安全性分析

定义传感器的不信任行为的概率为不正常行为的传感器数目与传感器总数的比值。如果传感器的最终信任等级为不信任，则认为网络识别了该传感器的不信任行为。定义不信任行为的检测概率为检测到不信任行为的传感器数目与同一区域传感器总数的比值。在从(15,5)到(35,25)的 21a×21a 的区域内，通过调整区域中不信任节点的数量来验证信任模型的有效性与准确性。结果如图 2 所示。

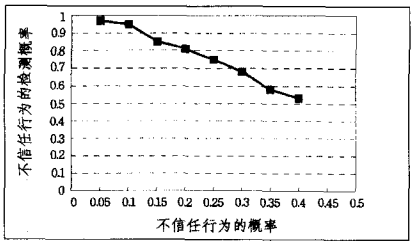

图 2　不信任行为检测概率随不信任行为概率的变化规律

从图2中可以看出不信任行为检测概率随着不信任行为概率的增长，近似呈线性递减。最佳结果是当传感器不信任行为的概率低于10%时，传感器网络可以检测到区域内91%的不信任行为。

4.3 能耗分析

基于本文算法可与现有的各种身份认证算法相结合使用，为了评估算法的平均能量开销，我们选择SNEP协议作参考，分别统计未加行为可信认证和加有行为可信认证情况下认证节点的平均能量消耗。每个节点的初始能量是2J，我们使用与文献[20]一样的能量消耗模型，使用式(13)计算接收一个报文的能耗，使用式(14)计算发送一个报文的能耗，节点在睡眠状态不消耗能量。

$$E_{Rx}=l*E_{dec} \tag{18}$$

$$E_{Tx}=l*E_{dec}+l*e_{fs}*d^2 \tag{19}$$

实验结果如图3所示。结果表明，在应用可信行为认证机制后，节点处理每个分组的能耗仅增加0.7毫焦左右，进一步说明了本文算法利用传感器本地读数的时间与空间相关性进行信任度计算，T_{th}时间后，只有位于实际认证区域中的传感器才需要与其邻居进行数据交换，所以传感器进行数据交换的频率为$1/T_{th}$。传感器网络在T_{th}时间内产生的消息量为$\alpha\cdot n\cdot N$。α代表认证区域面积与传感器的部署区域面积的比值，$0<\alpha\leqslant 1$。所以，当认证区域小于传感器网络的部署区域时，该算法只需其α/m的消息量，因此是高效节能的。

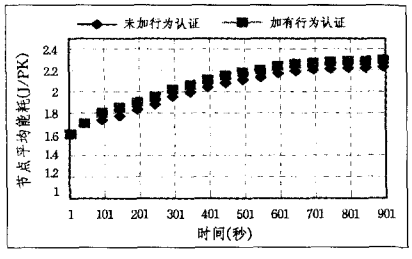

图3 节点平均能耗

结束语 本文从传感器节点行为的空间相关性和时间相关性入手，利用传感器节点状态估计向量(或测量值)的标称化差定义了节点之间相似度，提出了一种基于行为可信的访问控制机制，解决了已有研究工作基于密钥身份认证不能处理节点错误行为的访问控制问题。分析和仿真结果表明，该方法直观有效，既能控制传感器节点本身故障数据的干扰，又能阻止伪装成合法节点的恶意攻击。而且，当传感器网络中发生大规模不安全行为时，本文提出的算法依然可以保证较高的认证概率。本文选用的可信测度映射函数是最简单的双线性函数。分析一致性测度、可靠性测度和行为可信度之间的关系，设计一种有效的更加合适的测度函数，将是我们下一步的主要研究工作。

参 考 文 献

[1] 崔莉，鞠海玲，苗勇，等. 无线传感器网络研究进展[J]. 计算机研究与发展，2005，42(1)：163-174

[2] 李建中，高宏. 无线传感器网络的研究进展[J]. 计算机研究与发展，2008，45(1)：1-15

[3] 任丰原，黄海宁，林闯. 无线传感器网络[J]. 软件学报，2003，14(7)：1282-1291

[4] Benenson Z，Gedicke O R N. Realizing Robust User Authentication in Sensor Networks[C]// Stockholm. Sweden：2005

[5] Kirk H M，Zheng Wong-yang，Cao Jian-nong. A Dynamic User Authenticationg Scheme for Wireless Sensor Networks Pdf[C]// 2006

[6] Zhang Wen-sheng，Song Hui，Zhu Sen-cun. Least Privilege and Privilege Deprivation. Towards Toleraling Mobile Sink Compromises in Wireless Sensor Networls[C]// ACM MobHoc. 2005：182-188

[7] B R. An Optimal Class of Symmetric Key Gneration Systems[C]// Paris. France，1985

[8] Wang Hao-dong. Distributed User Access Control in Sensor Networks[C]// San Francisco. CA，2006

[9] Perrig A，Szewczyk R，et al. SPINS：Security protocols for sensor network[J]. Wireless Networks，2002，8(5)：521-534

[10] Liu D，Nini P. Multi-level μTESLA：a broadcast authentication system for distributed sensor networks[J]. ACM Transactions on Embedded Computing Systems (TECS)，2004，3(4)：800-836

[11] Liu D，et al. Practical broadcast authentication in sensor networks[A]// Proceedings of The 2nd Annual International Conference on Mobile and Ubiquitous Systems：Networking and Services[C]. Piscataway，2005：118-129

[12] Eschenauer L，Gligor V D. A Key- management Scheme for Distributed Sensor Networks[C]// Proceedings of 9th ACM Coference on Computer and ommunication Security. New York：ACM Press，2002：41-47

[13] 裴庆祺，沈玉龙，马建峰. 无线传感器网络安全技术综述[J]. 通信学报，2007，28(8)：113-122

[14] 林闯，彭雪海. 可信网络研究[J]. 计算机学报，2005，28(5)：751-758

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

[16] 刘敏华，萧德云. 基于相似度的多传感器数据融合[J]. 控制与决策，2004，19(5)：534-537

[17] John M R. Fusion of multi-sensor data[J]. The IntJ of Robotics Research，1988，7(6)：78-96

[18] Sun Y，Yu W，et al. Information Theoretic Framework of Trust Modeling and Evaluation for ad hoc Networks[J]. IEEEE Journal on Selected Areas in Communications，2008，19(7)：1716-1730

[19] Chen G，Branch J，Pflug M J，et al. SENSE：A sensor network simulator and emulator[C]// Schmidt D，ed. Proc. of the 2nd Int'l Conf. on Pervasive Computing. Vienna：Springer-Verlag，2004：249-267

[20] Heinzelman W B，Chandrakasan A P，Balakrishnan H. An application-specific protocol architecture for wireless microsensor networks[J]. IEEE Transaction on Wireless Communications，2002，1(4)：660-670