基于能量监测的传感器信任评估方法研究

范存群,王尚广,孙其博,王红熳,张光卫,杨放春
(北京邮电大学网络与交换技术国家重点实验室,北京 100876)

摘 要: 目前解决无线传感网节点安全的方式多种多样,无线传感器也将随着物联网的发展而呈现多样化.根据物联网传感层的特点和其特有的安全问题,本文提出了一种基于能量监测的信任评估方法来解决无线传感网节点的信任问题.该方法首先针对无线传感器能耗情况,创建了传感器能量监测机制;然后,根据监测能量机制中的监测信息,通过互相关系数方法分析计算,得出传感器所处的几种信任度;最后,对传感器进行信任评估,并给出评估结果.仿真对比结果表明,本文提出的方法具有较高的准确性.

关键词: 无线传感网; 能量监测; 信任评估; 相关系数
中图分类号: TN301.4 **文献标识码:** A **文章编号:** 0372-2112 (2013) 04-0646-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.04.004

A Trust Evaluation Method of Sensors Based on Energy Monitoring

FAN Cun-qun, WANG Shang-guang, SUN Qi-bo, WANG Hong-man, ZHANG Guang-wei, YANG Fang-chun
(*State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

Abstract: At present all kinds of security methods are used to solve security problems of WSNs (wireless sensor networks). Along with the development of Internet of Things, wireless sensors in sensing layer of Internet of Things will also be diversified. Therefore, according to the sensing layer's characteristics and its unique security problems of Internet of Things, we propose a trust evaluation mechanism based on energy monitoring to solve the security issues of sensing layer. Firstly, this paper establishes an energy monitoring mechanism of wireless sensors. Secondly, it uses the correlation coefficient method to calculate the data of energy monitoring and conclude the trust metric of sensors. Simulation results show that the trust evaluation method of wireless sensors proposed in this paper has higher accuracy.

Key words: WSNs(wireless sensor networks); energy monitoring; trust evaluation; correlation coefficient

1 引言

物联网传感层中无线传感器可以用于铁路、公路、航道、隧道、气象监测、水电系统、管道、仓储及战场等当中,实现物体与现存的互联网间的融合.在当前物联网应用日益多样化,相应的安全策略需要有更好的统一解决方案.无线传感器不仅面临外部的安全威胁,同时面临着内部节点被俘获后产生的内部攻击.传统的密码安全策略[1,2]主要用于抵抗节点面临的外部攻击,还有一些节点安全认证方法[3~5]以及信任评估方案[11,12]用于网络安全当中.但是这些方案的处理过程都建立在消耗节点自身能量的基础上,对于野外作业的无线传感节点,节点能量往往得不到及时补充,这很大程度上影响到节点的工作寿命.

目前,针对节点能量及其监测的一些研究已被应用于一些无线传感网来解决能量过度损耗的问题.Goel 和 Imielinski[6]提出了无线传感节点能量监测的方法,用一种基于监测的预测模块来解决能量效率监测.所提出的该模块主要功能是通过监测无线网络中传感器节点的能量情况,从而使得在节点具有相似任务的情况下,由能量较高的节点来完成任务,这样避免了能量低的节点因过早的能量耗尽而影响到整个无线传感网络的服务时间.同样思路的有 Chan 等人[7]的能量图法.文献[8]的作者对无线传感网中节点剩余能量的检测方法进行了研究分析,给出了两种能量检测方法:一种方法是基于软件,靠读取最大接收能量指示的值判断节点能量消耗的情况;另一种方法是基于硬件,利用 AD 采集本地电源供电电压信息,判断节点电量消耗情况.2009 年,

收稿日期:2012-05-02;修回日期:2012-07-03
基金项目:教育部新世纪优秀人才支持计划(No.NCET100263);教育部博士点基金 - 优先发展领域(No.20110005130001);国家 863 高技术研究发展计划(No.2011AA01A102);国家 973 重点基础研究发展规划(No.2009CB320406);中国博士后科学基金(No.2011M500226)

成小良等人[9]重点对无线传感网中的实时能耗进行了研究,结合无线传感网应用实际,综合分析了通信活动、计算活动及物理特性因素对节点能耗的影响,提出一种基于无线通信和计算特征分析的节点能耗模型.

另外,研究者也提出了一些对传感器信任评估有借鉴意义的研究方案.文献[11]中基于实际证据进行分析和扩展信任属性,通过进行分类,收集和演示建立信任水平模型,并且最后生成的可信水平包括信誉值,瓶颈分析和属性分析.Delaet 等[12]通过 RSS 技术来分析节点,并将节点的信任进行量化,从而区分出恶意节点和正常节点.

然而,尽管上述研究[1~5,11~13]取得了较好的研究成果,但是在抵御敌手的入侵攻击和控制攻击上还存在一定的问题.当节点受到敌手攻击并被控制后,节点所存储的秘密就会暴露,敌手掌握了节点密钥,对于一些基于认证的安全方法并不能及时发现节点密钥的泄露,这可能对整个传感网络的安全构成威胁.因此,本文把对传感节点准确的安全性评估、优化节点安全评估能耗以及非安全节点遭遇入侵估测作为目标,提出一种基于能量监测的传感器信任评估方法.通过能量监测机制获取节点能耗信息,与理论能耗情况进行互相关系数方法计算,进而根据相关性来判断节点所处的安全状态,对于非安全节点通过区间跃变方法估算遭遇入侵时间.实验结果表明本文所提出的方法对节点信任度评估具有很高的准确性,能准确判定受敌手入侵攻击的内部非安全节点.

2　背景知识

2.1　节点能量监测方法

通常情况下,物联网无线传感层节点所采用的能源大都是来自电池供电,所以对其能量量化的研究是比较直观的.目前对节点能耗监测的方法主要有以下两类[9]:(1)软件方法,利用节点运行时产生的与能耗相关的特征信息计算剩余能量,估计精度相对较低,但不会增加硬件成本;(2)硬件方法,基于电源电压、电流监测的简单模型,节点上需增加检测电路.可对移动节点进行能量监测,结果精确,但需要增加硬件开销.2.1.1 和 2.1.2 节主要介绍了基于软件方法和硬件方法能量监测的工作原理.

2.1.1　基于软件方法的能量监测

无线传感网中节点的消息信号都是通过节点内部的射频芯片发送出去的,射频芯片是节点内部消耗电量最大的器件,而射频芯片所发送的信号强度跟自身的电量有着直接的关系.即使射频芯片保持一个恒定的功率发送信号,当对射频芯片供电不足时,信号强度也无法达到额定的参数值.其实,经过测定,发送信号的强度是随着发送器件供电状态的变化而改变的,并且呈一种不严格的线性变化.当通过探测信号强度的变化即可以判断某个节点的能耗情况和剩余电量.这样就能通过简单的软件,利用接收到信号的强度来判断所发送信号的节点的能量情况.

一般情况下,都是采用文献[10]中接收信号强度指示的计算方法:

$$RSSI = 10^{\frac{G_{rf}}{10}} \frac{1.2567 \times 10^4 V_C^2}{(2^{2B})R} \left\{ \frac{1}{N} \sum_{n=0}^{N-1} Y_{lorQ}^2[k,n] \right\} \quad (1)$$

其中,G_{rf}为从接收天线到 ADC 的模拟增益;B 为 ADC 的分辨位数;R 为 ADC 的输入阻抗;V_C 为 ADC 的参考电压;$Y_{lorQ}[k,n]$为经过 AD 转换后的信号强度的 N 次采样值.

由于信号强度跟传播距离相关,对于移动节点来说,该方法并不适用,且由于存在干扰信号,该方法对测量到的能量信息并不是很准确.这种方法一般用于对节点的能量区域估计,有些研究中只需考虑节点当前的能量状态从而对节点进行任务调度.能量状态的设定如:高、中高、中、中低、低,等.

2.1.2　基于硬件方法的能量监测

电池供电的节点能量情况与电动势的高低成正比[8],可以通过 AD 转换将节点电源的电压信息采集到微控制单元(MCU,Micro Controller Unit).

图 1 为能量监控原理图,图中射频收发芯片是一块集成了 MCU 的射频芯片,芯片自身带有 AD 接口.芯片内部同时带有电压基准芯片,输出电压 1.8V,作为 AD 转换的基准电压.并且由于图中节点工作的电压跟芯片基准电压不相同,所以采用了分压电阻进行分压.硬件方法可以得到较准确的监测结果.

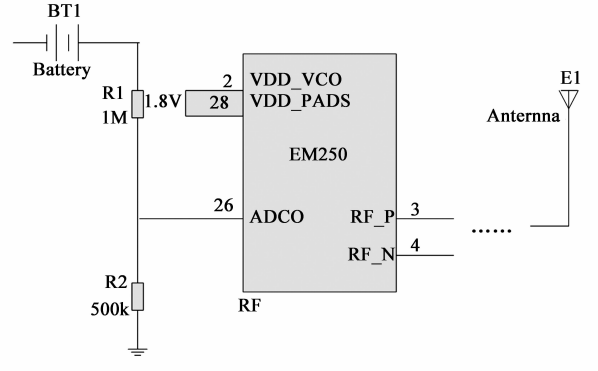


图1　能量监控原理图

2.2　物联网传感层中的信任评估与管理

物联网传感层中的网络节点跟 WSNs 一样具有网络应用相对单一、节点资源受限的特点.但相比于物联网传感层而言,WSNs 的授权策略较为简单,无须采取授权凭证方式的信任管理.物联网由于融合了各种各样的应用和服务,节点结构、作用等存在较大的异同.

所以,目前对物联网传感层的信任管理的研究主要集中于对节点进行信任值评估,借助信任值评估增强传感层的安全性,用信任管理识别恶意节点、自私节点,识别错误数据,将信任管理应用于物联网无线传感层的网络中可以全面提高物联网的安全性和可靠性.目前,无线传感网中的信任评估主要分为以下四类:

(1)层次式和平面式信任评估.层次式信任评估是指对信任值的评估、传递以及存储等管理具有层次特点,与网络拓扑及信任值的应用有紧密联系[13].平面式信任管理是指在信任管理的过程中,网络中所有节点及基站地位是平等的,采取相同的计算模型和管理策略,没有明显的中心或层次.

(2)通用信任评估.通用信任评估是指综合考虑信任的各方面要素建立的一套完整的信任管理框架,包括信息采集、传递、存储、计算、更新等信任管理各方面的设计.信任值的计算不具有针对性,是对节点可信性的一个综合评估[12].

(3)基于本地信息采集的信任评估.由于节点资源有限,为了减少通信及计算耗费,有的在信任值评估时,只简单考虑节点本身对被评估节点的观察结果以及交互行为评价等本地信息,从而节省其他节点传输信誉值的能量消耗.

(4)全局信任评估和本地信任评估.全局信任评估是指节点在整个网络中具有唯一的信任值.本地信任评估指被评估节点在不同评估节点处的信任值可能不一致,节点根据本地信任值[14]以及邻居节点发送的信誉综合决策.

3 基于能耗的信任评估方法

物联网中无线传感节点的状态和行为是判断节点是否可信的依据,受控的传感节点会在进行中心规定的任务外的敌手任务数据收集,发送以及传感监测等任务,对于节点的这些受控行为都建立在消耗节点自身能量的基础上.所以通过对传感节点自身能耗情况进行硬件方法的数据采集,将获得的能量信息阶段性的发送回监测中心,从而判断出节点各个时间段的行为和状态,如图 2 所示,进而综合计算和分析获得每个节点是否处于可信的状态下.它主要包括:节点能耗分析;量化的信任评估方法;非安全节点状态估计.

3.1 节点能耗分析

从节点获得的能量信息是节点在具体时刻内部电源剩余的电量信息 $E(t)$,从任意时刻 t_1 到接下来的另一时刻 t_2,通过 $E(t_2)-E(t_1)$可以得到 t_2-t_1 这段时间内的具体的能量消耗 $\Delta E(t_2-t_1)$.当接收到的剩余能量信息是一段时长为 t_{packet}的能量信息,起始时刻为 t_0.引入微分的计算方法,可以得到一个以时间为变量的节点功率函数:

$$W_n(t)=-[E(t)]',\ t\in[t_0,(t_0+t_{\text{packet}})] \tag{2}$$

为和标准状况下进行比较,这里设定一个合理的并可作为比较的标准函数 $W_s(t)$,该函数根据节点生产厂家所提供的节点执行某一具体事件时所发生的具体功耗参数来表示某时刻节点执行该事件时的标准能耗功率情况,即 $W_s(t)$表示节点某时刻在任务事件下所发生能耗功率的理论值.

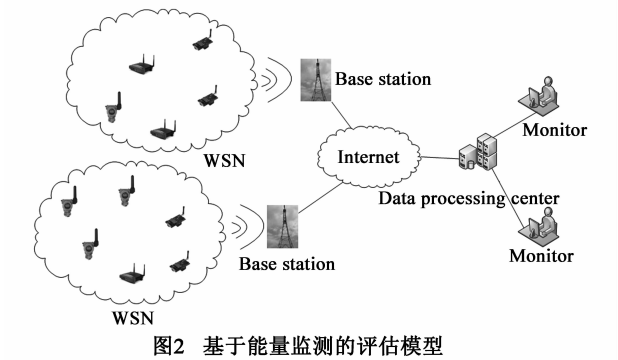


图2 基于能量监测的评估模型

3.2 量化的信任评估方法

为比较节点的能耗情况是否处于异常状态,就需要与节点当前能耗的理论值进行合理地比较并判断节点是否处于非安全状态.简单的线性差值比较显然是不能够准确地表示出节点能耗的差异,而且实时的同步比较对节点的能量消耗来说是一个限制.所以,在这里引入相关系数的概念进行阶段性比较[15],首先给出相关系数的定义.

定义 1(相关系数) 相关系数是变量之间相关程度的指标.相关系数用 ρ 表示,相关系数的取值范围为 $[-1,1]$.$|\rho|$值越大,误差 Q 越小,变量之间的线性相关程度越高;$|\rho|$值越接近 0,Q 越大,变量之间的线性相关程度越低.

当存在两个样本函数 X,Y 时,则 X 与 Y 的互相关系数可以表示为:

$$\rho_{xy}=\frac{\sum_{i=1}^{N}(X_i-\bar{X})(Y_i-\bar{Y})}{\sqrt{\sum_{i=1}^{N}(X_i-\bar{X})^2}\sqrt{\sum_{i=1}^{N}(Y_i-\bar{Y})^2}} \tag{3}$$

通过阶段性接收到的数据,使得每次接收的数据为一段时间 t_{packet}的能耗测量信息值.从而得到实际节点从 t_0 时刻在 t_{packet}时间内的能耗功率 $W_n(t)$,与同样时间内根据任务事件得到的能耗功率的理论函数 $W_s(t)$计算出它们的互相关系数:

$$\begin{cases}\text{Cov}(W_s,W_n)=E(W_s,W_n)-E(W_s)E(W_n)\\ \rho_{sn}=\dfrac{\text{Cov}(W_s,W_n)}{\sqrt{D(W_s)}\sqrt{D(W_n)}}\end{cases} \tag{4}$$

为使最后的信任结果具有准确的区分性,这里在

相关系数的基础上做一个阶段性的量化比较,设定两个阈值,划分成三个区间后进行再分析计算,进而判断出节点是否处于可信状态.这里,给出两个阈值分别为 $\Delta\rho_1$ 和 $\Delta\rho_2$,划分出的三个区间分别为:$(0,1-\Delta\rho_1-\Delta\rho_2]$;$(1-\Delta\rho_1-\Delta\rho_2,1-\Delta\rho_1]$;$(1-\Delta\rho_1,1)$.其中 $\Delta\rho_1$,$\Delta\rho_2$ 的取值情况由后面的实验分析给出.

(1)当 W_n 和 W_s 的互相关系数 $\rho_{ns}\in(1-\Delta\rho_1,1)$时,$W_n(t)$与 $W_s(t)$接近于线性相关,则认为节点的实际能耗情况与理论能耗情况非常接近,可以判断出节点处于安全状态下,即可信任的.

(2)当 W_n 和 W_s 的互相关系数 $\rho_{ns}\in(1-\Delta\rho_1-\Delta\rho_2,1-\Delta\rho_1)$时,$W_n(t)$与 $W_s(t)$的线性关系没那么显著,所以对于判断节点的安全性还需要进一步的分析讨论.这里引入总体能耗测评的方法来进行比较分析.即计算出 t_{packet}时间内节点的实际总能耗 E_n 和理论总能耗 E_s,分别为:

$$E_n=\int_{t_0}^{t_0+t_{\text{packet}}}W_n(t)\mathrm{d}t,\quad E_s=\int_{t_0}^{t_0+t_{\text{packet}}}W_s(t)\mathrm{d}t$$

得出 E_n 和 E_s 的差值 ΔE 为:

$$\Delta E=\int_{t_0}^{t_0+t_{\text{packet}}}W_n(t)-W_s(t)\mathrm{d}t \tag{5}$$

如果节点执行一个最小周期内的单个最小能耗任务所消耗的总能量为 $E'_{\min}$,当 $E'_{\min}\leqslant|\Delta E|$时,节点实际能耗跟理论能耗偏差较大,所以可认定节点处于非安全状态.当 $E'_{\min}>|\Delta E|$时,节点实际能耗与理论能耗偏差较小,认为节点处于暂时安全状态下,也即暂时可信任的,但需要对该节点保持观察.

(3)当 W_n 和 W_s 的互相关系数 $\rho_{ns}\in(0,1-\Delta\rho_1-\Delta\rho_2]$时,$W_n(t)$与 $W_s(t)$没有较好的线性关系,则认为节点的实际能耗情况与理论能耗情况偏差较大,可以判断出节点处于非安全状态下,即不可信任的.

3.3　非安全节点的状态估计

从 3.2 节的分析中可以判断出物联网传感层节点是否处于安全状态下,在此基础上进一步对节点进行分析研究,从而发现节点被攻击的时间和阶段,有利于做出相应的安全防护和安全应对措施.

当节点处于非安全状态下时,对节点的实际能耗功率和理论能耗功率进行一个作差取绝对值的计算,并将这个值与节点执行单个任务最小能耗功率 $W'_{\min}$进行比较.从而得出该节点执行非安全任务的具体起始时刻.具体计算方法如下:

$$|W_n(t)-W_s(t)|\geqslant\rho_{ns}W'_{\min},t\in(t_0,t_0+t_{\text{packet}}) \tag{6}$$

由式(6),可得知非安全状态下的节点起始恶意任务到结束该任务的整个时间信息.得到这样的时间信息有利于及时的安全警报和接下来的安全防护应对工作合理的进行.

整个信任评估流程如图 3,在安全评估阶段,本文引入了 $\Delta\rho_1$,$\Delta\rho_2$ 两个参数,并给出了取值范围.具体的取值则需要根据特定类型的传感器和传感网络的状况而定.在第 4 节中,我们分析了 $\Delta\rho_1$,$\Delta\rho_2$ 的取值情况和对评估结果的影响.

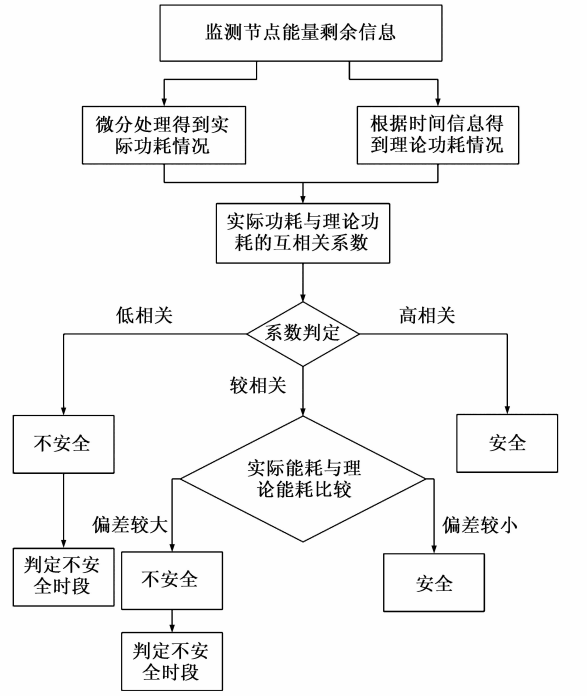


图3　基于能耗监测的信任评估流程图

4　仿真实验

本文采用的基于能量监测的信任评估方法主要是通过硬件方法来获得传感节点的剩余能量信息,通过对剩余能量信息进行处理得到节点的能耗功率函数,然后进行实际能耗功率与理论能耗功率的阶段互相关系数计算并比较分析节点的安全状态,最后对非安全的节点进行入侵估测.为了验证上述所提方法的有效性,下面主要通过仿真实验来对比验证.

4.1　实验建立

仿真环境建立的 PC 机配置为:CPU T7250 2.00GHz,RAM = 1GB,Windows XP 操作系统.所采用的仿真环境为 matlab7.1.

本文采用的信任评估机制可用于大部分无线传感器中,对传感器本身的应用特点并没有特殊的要求.虽然不同节点在各自功率数值上会有所差别,但对于大多数传感器节点而言,能耗分布总的特征是一致的,图 4 所示,即:第一,传感器模块和处理器模块的能耗要远小于通信模块的能耗;第二,通信模块在发送数据、接收数据以及闲置时消耗了大量的能量,而通信模块在

休眠模式下的能耗要小的多[16].

实验中,我们采用 Freescale 公司的 MMA7660FC 作为获取参数和研究对象,该传感器主要应用于纵向或者横向的运动、振动和敲击检测.工作功率参数有:待机休眠模式下为 7.2μW;检测模块工作时为 14.4μW;处理模块工作时为 14.4μW;发送数据时为 72μW;接收数据时为 64.8μW;闲置时为 64.8μW.

对该节点设定一周期内的工作任务,为方便计算,认为起始时刻为 0 点整.任务周期为 30min,即从 0:00 到 0:30.设定的节点任务为:从 0:00 到 0:05 处于接收数据状态,0:05 到 0:10 处于待机状态下,0:10 到 0:25 进行检测并处理数据,0:25 到 0:28 发送数据到基站,0:28到 0:30 处于待机休眠状态下.图 5,6 分别为传感节点理论功耗情况和实际功耗情况.

4.2 攻击模拟

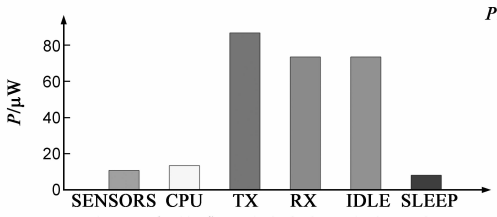


图4 一般传感器节点各部分能耗分布

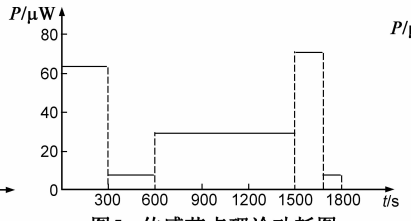


图5 传感节点理论功耗图

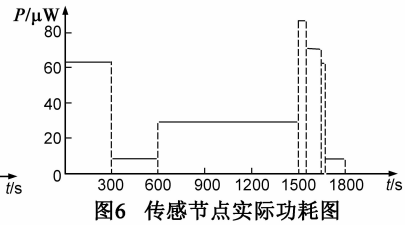


图6 传感节点实际功耗图

由理论功耗情况和实际功耗情况得到它们的互相关系数为 0.993809,很显然在没有受到任何攻击的情况下,实际功耗跟理论功耗高线性相关.在上面任务的基础上,分别对传感器进行仿真的敌手控制后传送伪数据和虫洞攻击.得到受攻击后的传感器实际功耗情况分别如图 7,8 所示.

4.3 对比分析

由上面受到攻击传感节点的实际功耗情况,得到在受控情况下和受到虫洞攻击的情况下,实际功耗与理论功耗的互相关系数分别为 0.379975 和 0.794643,如图 9.在通常情况下如果 $|\rho_{ns}|\geqslant 0.8$,则认为它们之间存在较强的线性关系,由于能耗情况的相关系数只可能是正数,即有 $\rho_{ns}\geqslant 0.8$ 时实际能耗与理论能耗存在较强的线性关系.在 3.3 节中所提到 $\Delta\rho_1$,$\Delta\rho_2$ 参数的确定,经过上述分析可知,如果 $\Delta\rho_1$ 和 $\Delta\rho_2$ 取值偏小的话,评估过程中容易将节点的信任度降低,但如果 $\Delta\rho_1$ 和 $\Delta\rho_2$ 取值偏大的话,评估过程中容易将节点的信任度升高,使得恶意节点不容易判断出来.实验结果显示,安全节点跟非安全节点所计算出来的相关系数有较强的分界线,对于节点安全性的判定具有很高的准确性.在综合一些实际情况下,$\Delta\rho_1$ 可以取值在 0.1 附近,$\Delta\rho_2$ 可以取值在 0.05 附近.

在图 7,8 受攻击后能耗情况的基础上,通过 3.3 中提出的方法进行非安全入侵时刻检测,在受控攻击下得到受攻击时间段为 0:12:30 至 0:20 以及 0:28 至 0:30.在受虫洞攻击下得到的受攻击时间段为 0:25 至 0:26:20以及 0:28 至 0:30.

采用了硬件方法来监测传感节点的能耗信息,会额外的增加传感器少部分的成本,但在获得精确的能耗信息后,只需要通过一次微分计算和相关系数计算便可获得节点的信任度,大大减小了复杂算法信任评估机制的复杂度.而且计算出的节点信任值非常具有区分性,可较准确地估算出节点受攻击的时间段.

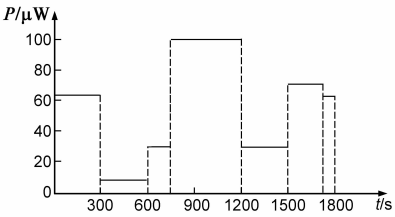


图7 受控传感节点实际功耗图

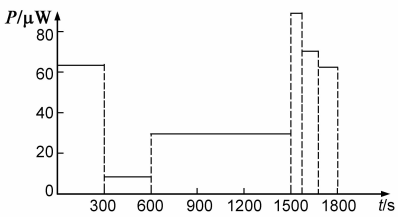


图8 受虫洞攻击传感节点实际功耗图

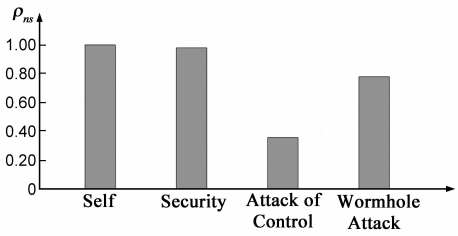


图9 理论能耗与几种实际能耗的互相关系数

5 结束语

本文提出的评估方法是基于监测传感节点能量信息的,该方法首先通过电路监测模块来获取节点剩余能量信息,然后通过实际功耗情况与理论功耗情况之间的互相关系数来建立评估方案,判断节点的几种信任度,最后估算出非安全状态下节点遭受攻击的时间段.实验结果表明,该方法可以在物联网多样化所带来节点应用各异,所需的安全策略也各不相同的情况下,在不需要复杂算法支持下对所有节点进行准确的安全评估和受攻击时段估算.但由于能量信息是分阶段发送到服务器端进行计算评估的,所以安全评估信息并

不是绝对实时的,当节点遭遇洪泛攻击时可能会造成大区域节点被判断处于非安全状态[17],造成区域内节点普遍失效.如果敌手控制了节点并截获任务中心数据,根据任务数据修改能量消耗信息返回给监测中心,会使得节点逃脱信任评估排除.并且在大量物联网传感器部署的情况下,大量监测数据发回到监测中心会一定程度上影响到网络的效能,监测中心对大数据量的处理也会存在效率上的问题.这些将是我们下一阶段需要解决的问题.

参考文献

[1] 杨庚,王江涛,等.基于身份加密的无线传感器网络密钥分配方法[J].电子学报,2007,35(1):180 – 184.
Yang Geng, Wang Jiang-tao, et al. A key establish scheme for WSN based on IBE and difie-hellman algorithms[J]. Acta Electronica Sinica, 2007, 35(1): 180 – 184. (in Chinese)

[2] Rui Sushmita, Nayak Amiya, Stojmenovic Ivan. Fully secure pairwise and triple key distribution in wireless sensor networks using combinatorial designs[A]. Proceedings IEEE INFOCOM[C]. USA: IEEE Press, 2011. 326 – 330.

[3] Zhao Xin, Wang Xiaodong, Yu Wanrong, et al. An efficient broadcast authentication protocol in wireless sensor networks[J]. Chinese Journal of Electronics, 2009, 18(2): 368 – 372.

[4] Ning P, Liu A, Du WL. Mitigating DoS attacks against broadcast authentication in wireless sensor networks[J]. ACM Transactions on Sensor Networks, 2008, 4(1): 1 – 35.

[5] Kim J, Baek J, Shon T. An efficient and scalable re-authentication protocol over wireless sensor network[J]. IEEE Transactions on Consumer Electronics, 2011, 57(2): 516 – 522.

[6] Samir G, Tomasz I. Prediction-based monitoring in sensor networks: Taking lessons from MPEG[J]. ACM SIGCOMM Computer Communication Review, 2001, 31(5): 82 – 98.

[7] Edward C, Song Han. Energy efficient residual energy monitoring in wireless sensor networks[J]. International Journal of Distributed Sensor Networks, 2009, (5): 748 – 770.

[8] 艾春丽,张凤登,等.无线传感网能量监测方法研究[J].自动化仪表,2007,28(12):5 – 7.
Ai Chunli, Zhang Fengdeng, et al. Research on energy monitoring method for wireless sensing network[J]. Process Automation Instrumentation, 2007, 28(12): 5 – 7. (in Chinese)

[9] 成小良,等.基于无线通信和计算特征分析的能耗模型[J].计算机研究与发展,2009,46(12):1985 – 1993.
Cheng XiaoLiang, et al. A model of energy consumption based on characteristic analysis of wireless communication and computation[J]. Journal of Computer Research and Development, 2009, 46(12): 1985 – 1993. (in Chinese)

[10] Choongill Yeh, Hyoungsoo Lim, Dongseung Kwon. IEEE C802.16d-03/92. RSSI Measurements[S]. 2003.

[11] Bao Tie, et al. Research on trustworthiness evaluation method for domain software based on actual evidence[J]. Chinese Journal of Electronics, 2011, 20(2): 195 – 199.

[12] Delaet S, Mandal P, Rokicki M, et al. Deterministic secure positioning in wireless sensor networks[J]. Theoretical Computer Science, 2011, 412(35): 4471 – 4481.

[13] Krasniewski MD, Varadharajan P, Rabeler B, et al. TIBFIT: Trust index based fault tolerance for ability data faults in sensor[A]. Proceedings of the International Conference on Dependable Systems and Networks (DSN)[C]. Piscataway: IEEE Computer Society, 2005. 672 – 681.

[14] Tanachaiwiwat S, Dave P, Bhindwale R, et al. Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks[A]. IEEE Workshop on Energy-Efficient Wireless Communications and Networks (EWCN), in conjunction with IEEE IPCCC[C]. Piscataway: IEEE Computer Society, 2004. 463 – 469.

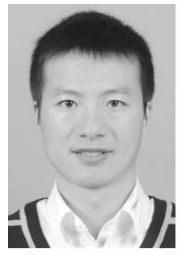
[15] 霍宏伟,等.基于室内无线传感器网络射频信号的老年人跌倒检测研究[J].电子学报,2011,39(1):195 – 200.
Huo Hong-wei, et al. Fall detection using radio signals of home wireless sensor networks[J]. Acta Electronica Sinica, 2011, 39(1): 195 – 200. (in Chinese)

[16] Pedram, Massoud, Rabaey, Jan M. Power Aware Design Methodologies[M]. Springer, 2002.

[17] Shangguang Wang, Qibo Sun, et al. Detecting SYN flooding attacks based on traffic prediction[J/OL]. Security and Communication Networks, http://onlinelibrary.wiley.com/doi/10.1002/sec.428/abstract, 24 FEB 2012, DOI: 10.1002/c.428.

作者简介

范存群　男,1986 年出生,江苏南通人.北京邮电大学网络技术研究院博士研究生.主要研究方向为融合网络、物联网安全和车联网技术.
E-mail: fancunqun@bupt.edu.cn



王尚广(通讯作者)　男,1982 年出生,河南周口人.2011 年毕业于北京邮电大学,获得计算机科学与技术专业博士学位.目前主要研究领域为服务计算、车联网技术及网络安全.
E-mail: sgwang@bupt.edu.cn