文章编号:1671-4598(2015)01-0336-03　　中图分类号:TP393　　文献标识码:A

无线传感器网络内可疑节点的分析研究

刘文通，王　忠
（四川大学 电气信息学院，成都　610065）

摘要：在无线传感器网络中，传感器节点对信号采集传递的可靠性决定系统结果的准确程度，而对于应用于不同领域的 WSNs 而言，节点损坏、信息传递过程受到攻击的情况时有发生，为了保证结果的准确，及时准确的判断节点的工作情况至关重要；进而对传感器节点进行分析，介绍几种可疑节点判断方式，同时结合 WSNs 在母婴监控系统中的应用，通过信号强度及信号呈现的规律检测可疑节点的方案在母婴监控系统中的实用性，分析了母婴监控系统中是如何利用可疑节点来达到监控的效果。

关键词：无线传感器网络；可疑节点；母婴监控系统

Analysis and Study of Suspicious Nodes in Wireless Sensor Networks

Liu Wentong, Wang Zhong
(College of Electrical and Information Engineering, Sichuan University, Chengdu　610065, China)

Abstract: In wireless sensor networks (WSNs), the reliability of the signal acquisition transfer affects the accuracy of the system result, and for applied in different areas of the WSNs, the node can be damaged, the situation of the information transfer process is under attack, in order to guarantee the accuracy of the results, timely and accurate judgment nodes working condition is very important. Based on sensor node analysis, the paper introduces the suspicious nodes judging ways, at the same time combining the application of the WSNs on maternal and infant security system, By the law of the signal strength and signal presented to detect suspicious nodes solution in maternal and infant security system of practical, and analyzes the maternal and infant security system how to use the suspicious nodes to achieve the result of monitoring.

Keywords: wireless sensor network; suspicious node; maternal and infant security system

0　引言

无线传感器网络（wireless sensor networks，WSNs）WSNs 是由大量的低成本，自身具有感知能力、计算能力、无线通讯能力的传感器节点组成的网络。随着微电子技术、计算机技术和无线通信技术的快速发展，WSNs 的研究价值也越来越被人们重视。WSNs 作为媒介连通着物理世界、计算机世界及人类社会，为人类社会的发展提供了强有力的帮助，在军事国防、工农业、城市管理、生物医疗、环境监测、抢险救灾、防恐及反恐、危险区域远程控制等许多领域都体现了其研究价值。但在实际应用过程中，由于传感器节点存在易损坏、计算能力有限、存储能力及通信带宽有限等缺陷，造成 WSNs 对目标信息的采集在节点损坏等情况下存在极大误差，可能会严重影响实际需要结果，这种误差对于危险区域、医疗、国防等对结果要求严格的领域而言是不可忽视的。

1　传感器节点

传感器节点通常都由传感单元（信息的采集转化）、电源、嵌入式处理单元、存储器、通信单元及软件等部分构成[1]，其结构如图 1 所示，有时为满足应用领域的特殊需求而对部分结构加强，如添加电源自供电系统。

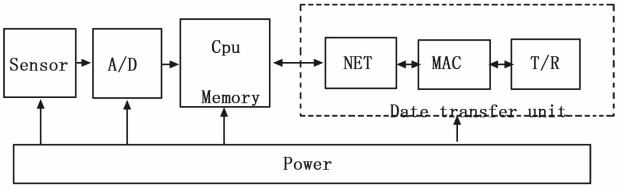

图 1　传感器节点的结构

从安全角度对 WSNs 内节点进行分类，可将 WSNs 节点分为正常节点、非正常节点，非正常节点可细分为恶意节点和自私节点[2]，传感器节点分类结构图如图 2 所示。

1）正常节点：能够按照网络部署事先配置完成相关任务的网络节点。

2）非正常节点：不能够按照网络部署事先配置完成相关任务的网络节点，然若非正常节点有窃取敏感数据和攻击网络造成瘫痪等行为则为恶意节点，而此外为了节省自身能量而不愿转发其他节点数据包的非正常节点被称为自私节点。

WSNs 节点具有分布性、独立性和移动性等特点[3]，传感器节点的局限及缺陷取决于自身的结构，当网络建立在无人区或是危险区域，更换节点电源付出的代价是得不偿失的；节点处理器和存储器的计算能力、容量有限，限制了网络的规模。

收稿日期:2014-06-01；　**修回日期**:2014-07-09；
基金项目:航空科学基金项目(20100119004)；国家级大学生创新创业训练计划项目(201310610109)。
作者简介:刘文通(1993-)，男，江西人，主要从事控制科学与工程方向的研究。
王　忠(1964-)，男，四川仪陇人，副教授、硕士生导师，主要从事 GPS 理论及应用、无线与移动通信关键技术、网络通信理论与技术等方向的研究。

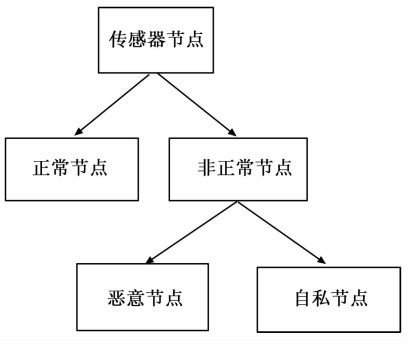

图 2　WSNs 节点分类图

2　可疑节点的影响

WSNs 建立在真实的物理世界，其服务与维护极其困难，网络的安全受到严峻的挑战，窃听、消息修改、消息注入、路由欺骗、拒绝服务、恶意代码等安全威胁都有可能发生。而节点信息的准确性是保证系统结果可靠准确的关键之一，节点信息的准确性决定于传感器节点本身的硬件设备及系统对节点信息有效合理的判断。

目前无线传感器网络的安全威胁主要来自如下六类攻击：Hello 洪泛攻击（hello flood attack）、陷阱攻击（sinkhole attack）、重放攻击（replay attack）、选择性转发攻击（selective forwarding attack）、女巫攻击（ssbil attack）、虫洞攻击（wormhole attack）[4]。

Hello 洪泛攻击：在许多传感器网络协议中节点都是通过广播 HELLO 数据包来发现其邻居节点，恶意节点以较高的发射功率向其他节点发送 Hello 消息，让其他正常节点误认该节点是其邻居节点，当误认的正常节点向攻击节点发送消息时，两者由于相距太远不能进行通信，就造成了传送数据包的丢失。

陷阱攻击：攻击者通常使用强大的处理器来伪装恶意节点，恶意节点表现出极高的传输质量，吸引网络中的其他节点将数据包通过恶意节点进行传送，在传送过程中恶意节点可转发、更改部分数据数据包内容达到攻击目的，而这些本应经过正常节点的数据包由于被吸引到了恶意节点而造成数据丢失。

重放攻击：通常接收节点会根据发送节点传递的消息而估算出节点之间的距离及发送节点的信号强度，而在重放攻击中，恶意节点会将本应传送的消息存储、延迟发送，这会造成接收节点对该节点的计算失误，且如果恶意节点重放的是路由消息，则会使网络中出现路由环路，会延长或者是缩短路由，影响网络的正常工作。

选择性转发攻击：恶意节点在传送数据包时概率性的转发或是丢弃某些消息，让数据包不能到达目的地，进而影响网络的正常工作。

女巫攻击：恶意节点声明自身的多重身份[5]，让其他正常工作的节点误认为有多个节点的存在，此时恶意节点就可以向网络中正常工作的节点发送错误消息。

虫洞攻击：一个远离基站的恶意节点声称自己可以和基站附近的节点建立低延迟、高带宽的链路，从而吸引附近的节点将数据包发送到它这里，同时攒通另一个靠近基站的恶意节点（Sinkhole 节点），这种攻击方式可与选择转发攻击、女巫攻击等结合起来影响网络的正常工作。

结合传感器节点自身会发生损坏及电源耗尽等情况，这些影响网络正常工作的攻击方式都有个共同的影响因素：节点可靠性。因而判断一个传感器节点可靠与否及排除可疑节点对于 WSNs 的安全是至关重要的。

3　可疑节点的检测方案

1）通过信号强度及信号呈现的规律检测可疑节点：

WSNs 在工作过程中，节点信号强度与节点正常工作时的信号强度进行比较，若信号强度不一致则视该节点为可疑节点[6]，节点正常工作时的信号强度作为给定的比较对象。对于节点检测信号有客观规律的无线传感器网络，通过一段时期的记录，由软件根据记录的信号数据拟合信号曲线作为比较对象，根据应用需求、实际结果制定判断标准，借此检测可疑节点，该检测方案的结构如图 3 所示。而针对追踪定位，杨峰[7]提出了一种基于标记的溯源追踪解决方案，可实现对可疑节点的追踪定位。

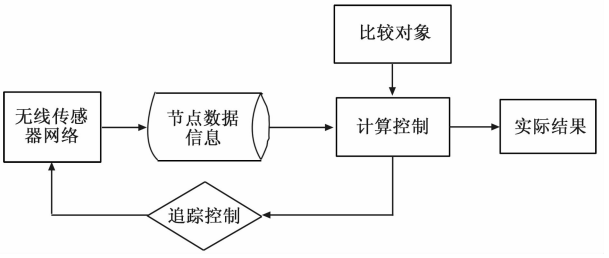

图 3　检测方案 1）的结构图

2）利用博弈模型分析检测节点：

而对于节点检测信号无客观规律的无线传感器网络，节点信号数据拟合的曲线无法设定成比较对象，严重影响可疑节点的判定。潘巨龙[2]等提出一种博弈的检测方法：采用多节点对可疑节点进行检测，同时采用博弈模型[2]分析检测节点和可疑节点的策略选择问题。该方法通过检测节点对可疑节点先行判断，避免了比较对象的设定。

3）利用确认信息时延检测可疑节点：

对于任何收到消息的节点，方法要求需向发送消息的节点返回一个确认信息。发送消息的节点在收到确认信息之前将消息暂时保存在缓冲区，当在确定时间段内收到确认信息，则认为接收消息节点可信，否则认为是恶意节点，该方案结构原理如图 4 所示。然而这种判断方法有不利因素：恶意节点由于距离较远，传回确认信息所需时间较长。测试表明该方法能够检测出恶意节点，但耗费的资源比较多[7]。

4　WSNs 在母婴监控系统中的应用

在现实生活中，节点检测信号存在客观规律的无线传感器网络应用非常广泛，然通常可疑节点都会给实际结果带来巨大影响，而 WSNs 在母婴监控系统上的应用恰好是反其道而行之，即利用可疑节点的存在来监测母婴的情况。

母婴监控系统的理论原理是基于射频识别（radio frequency identification，RFID）技术[8]，是一种非接触式的自动识别技术，它通过射频信号自动识别目标对象并获取相关数据，识

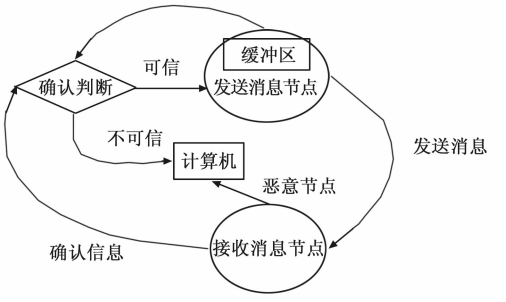

图 4 检测方案 2）的结构原理图

别工作无须人工干预，可工作于各种恶劣环境[9]。

母婴监控系统的基本架构：通过选用 MICROCHIP 公司的 ENC28J60 芯片用于组建 10 Mbps 局域网，选用 Nordic 公司的 nRF24LE1D 作为系统的标签及监控节点，监控节点将标签信息通过总线实时的反馈到服务器以达到监控的目的。整个监控系统将对母婴的监控简化为对标签的监控，服务器通过对监控反馈信息的分析处理对事件做出相应的处理，当发现可疑节点，医务人员可及时查看该节点的情况，进行有效的监护母婴，防止婴儿被盗的情况发生，母婴监控网络系统的结构框图如图 5 所示。

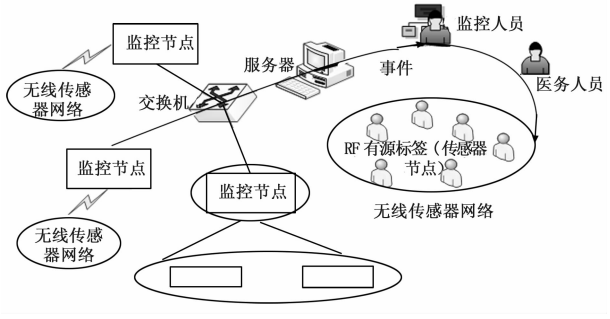

图 5 母婴监控网络系统的结构框图

系统以母婴标签发出的信号作为所需检测信号，以标签作为系统的传感器节点，各传感器节点的软、硬件条件相同（下图为简化以天线作为监控节点），并借助局域网构建一个个小规模的无线传感器网络，进而组合成一个监控网络，其网络结构如图 6 所示。

母婴监控系统工作情况：标签以高频率发送信号，监控节点接收不同标签的信号传递到服务器，服务器对传递的标签信号判断分析，当出现非正常情况则派医务人员对该标签母婴进行检查，防止发生婴儿被盗。

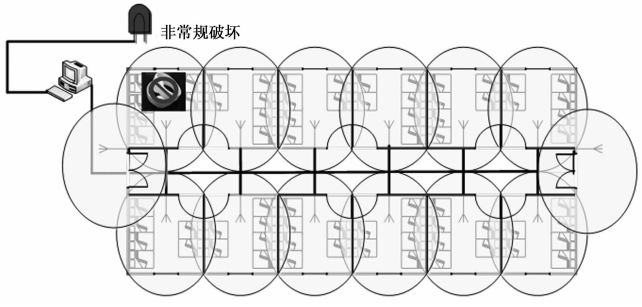

图 6 母婴防盗系统的 WSNs 结构

母婴监控系统中可疑节点的检测方案采用上述检测方案：对母婴标签初始化，录入个人信息，并将正常工作情况下标签返回的信息记录以作为比较对象。系统工作时，标签被非常规破坏、标签电源耗尽等情况的产生，造成节点信号强度的改变，服务器比较判断该标签节点为可疑节点，进而采取相关措施。

通常的 WSNs，可疑节点的出现很可能对系统实际的结果产生较大的影响，然在母婴监控系统中，却是利用可疑节点的出现间接反馈母婴的现状，以达到监控效果。

在此系统中，构建的 WSNs 规模虽然很小，节点传递的信息也很简单，但其应用极大简化了医院对母婴的监护流程，并一定程度降低了婴儿被盗、抱错事件发生的概率。

5 结束语

传感器节点传递信息的可靠、准确性是无线传感器网络性能的一个重要的评判标准。然往往针对 WSNs 的安全威胁是建立在信息的传递上，通过对正常节点工作情况的记录分析及节点的信号强度用以判断节点是否为可疑节点，这种方法对于结果存在规律的网络而言是实用的，其在母婴监控系统的应用简化了医院对母婴的监护流程，有效地减少了婴儿被盗事件的发生。通过利用可疑节点间接达到对母婴监控的效果，这种思考方式上的转变进一步扩宽了 WSNs 的应用空间。随着电子技术、计算机技术、通信技术的飞快发展，传感器节点其能源有限的问题也将会得到有效改善，传感器网络如何在破坏或干扰情况下可靠的执行任务，也将是一个重要的研究课题[10]。

参考文献：

[1] 石琴琴. 无线传感器网络节点自定位系统及其算法研究 [D]. 上海：上海交通大学，2009.

[2] 潘巨龙，李善平，张道远. 无线传感器网络簇内可疑节点的博弈检测方法 [J]. 浙江大学学报，2012，46 (1)：72－78.

[3] 汪 洋，林 闯，李泉林，等. 基于非合作博弈的无线网络路由机制研究 [J]. 计算机学报，2009，32 (1)：54－68.

[4] Kalith H K，Kar A. Wireless sensor network security analysis [J]. International Journal of Next－Generation Networks，2009，1 (1)：1－10.

[5] 付志威，叶晓慧，张海波. 无线传感器网络安全威胁及对策 [J]. 网络安全技术与应用，2008 (11)：6－8.

[6] 杨建强，方 磊. 无线传感器网络的安全威胁及防范措施 [J]. 襄樊学院学报，2011，32 (8)：41－44.

[7] 杨 峰，周学海，张起元，等. 无线传感器网络恶意节点溯源追踪方法研究 [J]. 电子学报，2009 (1)：202－206.

[8] 顾 希. 自行研制 RFID 母婴识别及婴儿防盗系统 [J]. 中国医疗设备，2011，26 (6)：37－38.

[9] 王 伟. 射频识别 (RFID) 技术及其应用的研究 [J]. 安徽师范大学学报，2008，31 (2)：139－141.

[10] 王卫平. 浅谈无线传感器网络的研究现状与发展趋势 [J]. 科技视界，2012 (28)：253.