无线传感器网络安全测评关键技术研究*

王曙光[1] 王庆升[1] 刘美丽[2] 公 伟[1] 甘杰夫[3] 许立前[1]
(1.山东省标准化研究院 济南 250014;2.山东微分电子科技有限公司 济南 250016;
3.中国信息安全认证中心 北京 100020)

摘 要:针对无线传感网面临的安全威胁,通过搭建无线传感网仿真环境,实验分析无线传感网在不同网络安全威胁和攻击下其安全状态变化,归纳分析影响无线传感网安全性典型因素,形成无线传感网安全性测评指标,针对每项测评指标,研究无线传感器网络安全性测评方法,通过运用无线传感网安全测评方法进行无线传感网安全测评实验,对无线传感网安全测评指标进行测评,从而从源头上降低无线传感网风险,保证了无线传感网安全。

关键词:无线通信技术;无线传感器网络;测评指标;测评方法
中图分类号:TP393 **文献标识码**:A **国家标准学科分类代码**:520.60

Research on the key techniques in security evaluation of wireless sensor networks

Wang Shuguang[1] Wang Qingsheng[1] Liu Meili[2] Gong Wei[1] Gan Jiefu[3] Xu Liqian[1]
(1. Shandong Institute of Standardization, Jinan 250014, China; 2. Shandong MicroSec Electronic Co. Jinan 250016, China;
3. China Information Security Certification Center, Beijing 100020, China)

Abstract: Based on the analysis of security threats faced by the WSN, typical factors which affect the security of WSN are analyzed by building a simulation environment of WSN, then the security status of WSN is analyzed in different variations of network security threats and attacks. For each of the security evaluation index of WSN, this paper studies the corresponding security evaluation methods. By using WSN security evaluation methods, the WSN security evaluation experiements are carried out, that is the security evaluation index of WSN are carried out. Thus the risk of WSN is reduced from source, and the security of WSN is ensured.

Keywords: wireless communication technology; wireless sensor network; evaluation index; evaluation method

1 引 言

无线传感器网络(也称:无线传感网)是指传感器节点通过近距离无线通信技术所构成的相互连接、传送传感数据的局域网络[1-2]。目前,无线传感网技术已在我国电力、环境监测、军事、国土安全、物流交通等国民经济重要领域得到广泛应用[3-5],应用模式逐步成熟。但在广泛应用的同时,其安全性已成为制约无线传感网技术更大范围推广的瓶颈[6]。众多无线传感网系统在没有进行安全性测评的情况下仓促上线,运行过程中带来巨大安全隐患,近年来发生的智能水表远程抄表系统数据篡改等信息安全事件表明在该领域尽快建立安全性测评工作机制是相当急迫的[7-8]。

在研究无线传感器网络面临的安全威胁和攻击的基础上,通过实验归纳分析,提出了无线传感网安全性测评指标和安全性测评方法。

2 无线传感网面临安全威胁

无线传感网虽然应用非常广泛,但在安全方面也面临着很多挑战,主要包括如下几个方面[9-10]:节点自身限制、节点数量大、节点故障率高等。

利用以上技术限制进行攻击,使得无线传感网面临很多安全威胁,主要包括不公正、资源耗尽、冲突、多重身份攻击、重放路由信息、选择转发、急行军攻击、虫洞攻击、确认欺骗攻击、洪拒绝服务攻击、同步攻击、重放攻击、数据篡改攻击等[11-12]。

3 无线传感网安全测评关键技术研究

3.1 概述

通过搭建无线传感网仿真平台,采集所监控的传感网

收稿日期:2015-03
*基金项目:国家质检总局质检公益性行业科研专项(201410037)项目

节点状态和链路状态数据，分析无线传感网在不同网络安全威胁和攻击下其安全状态变化，获取大量的测试实验数据，从而总结归纳出无线传感器网安全性测评指标，形成无线传感网安全性测评方法即形成无线传感网安全测评关键技术，如图 1 所示。

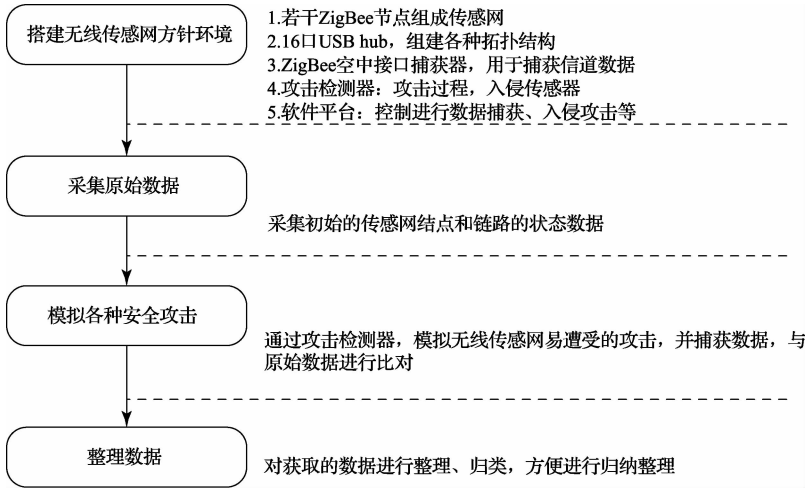

图 1　无线传感网安全测评关键技术研究

3.2　无线传感网安全测评指标

通过无线传感网安全测评关键技术研究得到无线传感网安全测评指标如图 2 所示。

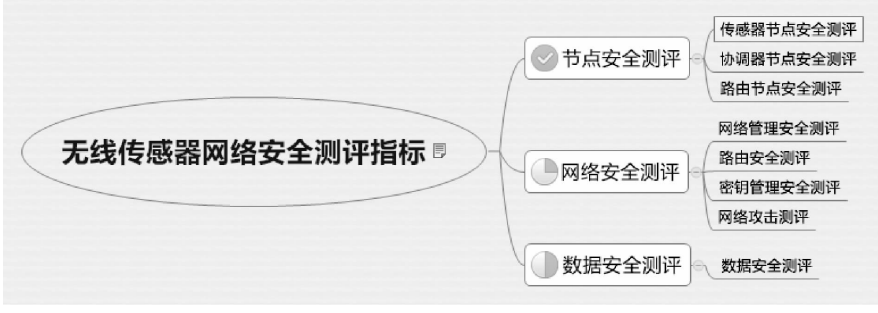

图 2　无线传感器网络安全测评指标

3.2.1　节点安全测评

本项测评主要包括传感器节点安全测评、协调器节点安全测评和路由节点安全测评 3 部分。

其中传感器节点和协调器节点安全测评又包括鲁棒性测评、节点保密性测评、节点完整性和验证测评、身份鉴别能力测评、访问控制能力测评、抗 DoS 攻击能力测评。路由节点安全测评包括鲁棒性测评、路由方向判断能力测评、路由结果判断能力测评、身份鉴别能力测评。

1)鲁棒性测评

本指标主要对节点鲁棒性进行测评，以测评是否能正常收发数据。

2)节点数据保密性测评

本指标主要对节点数据加解密能力进行测评，以测评是否具有加密和解密能力。

3)节点数据完整性和验证测评

本指标主要对节点数据完整性保护和验证能力进行测评，以测评是否具有数据完整性保护和验证能力。

4)身份鉴别能力测评

本指标主要是无线传感网节点对用户的鉴别进行测评，以测评是否只有通过鉴别的节点之间才能传递信息，通过鉴别的用户才能收集节点的数据。

5)访问控制能力测评

本指标主要对无线传感网访问控制机制进行测评，以防止未授权用户对传感网节点和数据的非授权访问。

6)抗 DoS 攻击能力测评

本指标主要对节点抗拒绝服务攻击能力进行测评，以测评是否具有抗 DoS 攻击能力。

7)路由方向判断能力测评

本指标主要对路由节点对转发的指令和数据判断传输方向的能力进行测评。

8)路由结果判断能力测评

本指标主要对路由节点对转发的指令和数据是否成功进行判断的能力进行测评。

3.2.2 网络安全测评

本项测评主要包括网络管理安全测评、路由安全测评、密钥安全管理测评和网络攻击测评4部分。

网络管理安全测评主要包括网络可靠性测评、网络健壮性测评、网络标识测评、网络传输抗碰测试、动态拓扑结构测评、网络拓扑结构变化警示测评、组网时限测评;路由安全测评包括路由连通性测评、抗惰性路由攻击测评;密钥安全管理测评主要包括密钥设置测评、密钥更新测评、密钥建立测评、密钥扩展测评和密钥撤销测评;网络攻击测评主要包括网络可靠性测评、重放攻击测评、修改重放攻击测评、Sybil攻击测评、hello flood攻击测评和资源耗尽攻击测评等。

3.2.3 数据安全测评

本项测评主要包括数据对网络的独立性测评、数据可靠性测评、数据保密性测评、数据完整性测评、数据可用性测评、数据新鲜性测评以及身份隐私性测评。

1)数据对网络的独立性测评

本测评指标主要对数据格式是否依赖于传感网的结构和传输模式进行测评。

2)数据可靠性测评

本测评指标主要对数据在传输中发生错误的概率进行测评。

3)数据保密性测评

本指标主要对无线传感网数据的保密性进行测评,主要包括了保密性存在测评和保密性正确性测评。

4)数据完整性测评

本指标主要对无线传感网数据的完整性进行测评,主要包括完整性存在测评和和完整性正确性测评。

5)数据可用性测评

本测评指标主要对数据能否正确接收、非法数据能否被过滤掉进行测评。

6)数据新鲜性测评

本指标主要对无线传感网数据的新鲜性进行测评,主要包括新鲜性存在测评和新鲜性真实性测评。

3.3 无线传感网安全测评方法研究

对无线传感网进行安全性测评,需要借助于安全性测评方法,对安全性测评指标进行检测,以查看其是否符合要求,目前,无线传感网安全测评方法主要有如下4种:

1)特定信道数据捕获方法

通过捕获器设备捕获特定一路信道数据,并将设定信道的所有节点信息接受并传送的方法。

2)传感网传输协议解析方法

对捕获器获取的数据进行解析,重点对MAC/NWK/APS帧格式进行解析,以实现实时存储、管理和展示和网络拓扑生成的方法。

3)渗透性测试方法

运用攻击检测器,进行入侵、仿冒等攻击,并通过多次测试获取结果进行安全性分析的方法。

4)检查方法

模拟协议或算法的运行过程,检查协议或算法的运行结果是否正确的方法。

4 无线传感网安全测评实验

通过搭建无线传感网仿真平台上,模拟远程抄表系统,对无线传感网安全测评进行了应用示范,以验证远程抄表系统是否采用了相应的安全机制。测评环境[12-13]如图3所示。

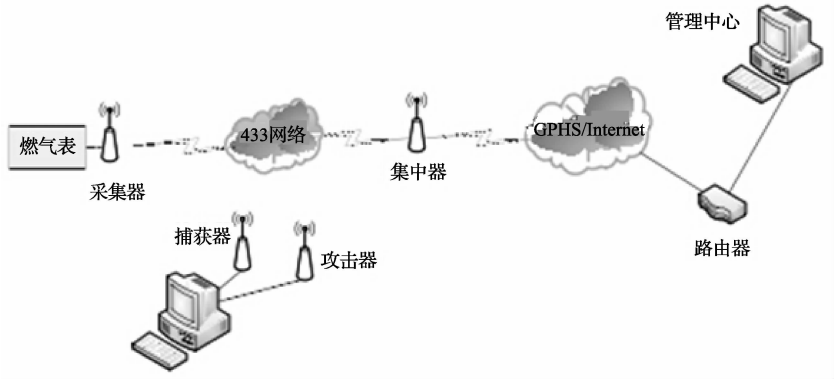

图3 无线传感网安全测评环境

为提高试验效果,实验过程中选取传感节点的保密性、身份鉴别能力、抗DOS攻击重点进行实验。

1)保密性:通过Packet Sniffer利用特定信道数据捕获方法,观察捕获的数据,发现其第6位加密标识位为1,证

明其保密性通过测评；

2)身份鉴别能力：攻击器模拟合法的感知节点，并假冒这个合法节点进入无线传感网，发现不能进入网络，证明其身份鉴别能力也通过测评；

3)抗 DOS 攻击：利用攻击器把捕获器捕获的数据包进行替换，通过攻击器进行重新发送，观察管理中心数据显示区，开始不显示，当攻击不断加大时，开始显示，证明其可以抵抗一定的抗 DOS 攻击，但当抗 DOS 攻击不断增大时，就被攻破了。

实验中，进行测试的远程抄表系统 3 项指标都通过了测评，类似的可进行其他的各项测评指标，同时根据应用的具体需求，确定通过多少指标即可进行应用。

5　结　　论

在分析无线传感网面临安全威胁基础上，通过搭建无线传感网仿真平台，采集所监控的传感网节点状态和链路状态数据，提出了无线传感网安全测评指标和测评方法，通过运用无线传感网安全测评方法进行无线传感网安全测评实验，对无线传感网安全测评指标进行测评，从而保障无线传感网安全。下一步将在无线传感网安全测评指标和测评方法基础上，通过应用无线传感器网络安全性评估系统，大规模开展无线传感网系统安全测评工作，从而为无线传感网乃至物联网大规模推广应用和智慧城市的建设提供安全依据。

参考文献

[1] 尚兴宏. 无线传感器网络若干关键技术的研究[D]. 南京：南京理工大学，2013：1.

[2] 李建中，李金宝. 无线传感网及其数据管理的概念、问题与进展[J]. 软件学报，2013，14(10)：1717-1727.

[3] 焦尚彬，宋丹，张青，等. 基于 ZigBee 无线传感器网络的煤矿监测系统[J]. 电子测量与仪器学报，2013，27(5)：436-442.

[4] 张世一，黄华，刘永平. 基于 ZigBee 和 LabVIEW 的智能照明监控系统设计[J]. 国外电子测量技术，2014，33(5)：63-66.

[5] 鲍贤亮，陈年海，徐一凡，等. 基于 ZigBee 技术的无线脉搏传感网[J]. 电子测量技术，2015，38(2)：105-108.

[6] 赵章界，刘海峰. 无线传感网中的安全问题[J]. 计算机安全，2010(6)：1-4.

[7] 郭江鸿. 无线传感网若干安全问题研究[D]. 西安：西安电子科技大学，2013：4.

[8] 王曙光，公伟，王庆升，等. 无线传感器网络安全性研究综述[J]. 信息技术与信息化，2014(7)：12-14.

[9] 陈智勇. 无线传感器网络安全若干关键技术研究与应用[D]. 南京：南京大学，2011：5.

[10] 汪燕，李玲娟. 无线传感网数据安全采集方案研究[J]. 计算机技术与发展，2013，23(2)：229-232.

[11] 王艺琳. 基于无线传感器网络的安全技术研究[J]. 太原：太原理工大学，2011：5.

[12] 代晓丽. 物联网安全技术研究[D]. 北京：北京邮电大学，2012：5.

[13] 颜丙洋. 基于 433MHz 模块的远程抄表安全系统设计与实现[D]. 济南：山东师范大学，2014：5.

作者简介

王曙光，1977 年出生，高级工程师，硕士研究生。主要研究方向为信息标准化。

王庆升，工程师，硕士研究生。主要研究方向为信息安全标准化与无线传感网信息安全。

刘美丽，高级工程师。主要研究方向为物联网信息安全测评。

公伟，工程师，硕士研究生。主要研究方向为信息安全标准化与无线传感网信息安全。

甘杰夫，高级工程师，博士。主要研究方向为信息安全认证。

许立前，本科，工程师。主要研究方向为信息标准化。