第37卷 第10期
Vol.37 No.10

计 算 机 工 程
Computer Engineering

2011年5月
May 2011

·特邀论文· 文章编号：1000—3428(2011)10—0001—07 文献标识码：A 中图分类号：TP393

一种基于等级划分的物联网安全模型

孙知信[1,3]，骆冰清[1]，罗圣美[2]，朱洪波[1]

(1. 南京邮电大学物联网研究院，南京 210012；2. 中兴通讯股份有限公司，南京 210003；
3. 南京大学计算机软件新技术国家重点实验室，南京 210093)

摘 要：在对物联网安全进行研究的过程中，对于不同安全敏感度应用，通常是人为判断其所属的安全等级域。针对该问题，以等级划分为基础，提出一个物联网安全模型，利用该模型分析某一物联网应用的拓扑结构，预测其攻击来源与类型并判定其所属的安全等级域，从而对该应用进行合适的安全技术配置。将该模型用于某大学的智慧校园系统中，实践结果证明，其有利于学校更好地发展智慧校园应用，建立更加安全、稳定的智慧校园系统。

关键词：物联网；等级划分；安全模型；物联网拓扑；攻击模型

Security Model of Internet of Things Based on Hierarchy

SUN Zhi-xin[1,3], LUO Bing-qing[1], LUO Sheng-mei[2], ZHU Hong-bo[1]

(1. Institute of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210012, China; 2. ZTE Corporation, Nanjing 210003, China; 3. State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China)

【Abstract】 Different applications have different security sensitivities, which are determined by subjective judgment in the process of security research on Internet of Things(IOT). This paper presents a Security Model of IOT Based on Hierarchy(BHSM-IOT), which can be used to analyze the topology structure, predict the attack source and attack type and determine the application level of security domain, so that appropriate safety technical configuration can be made. The model is applied in a wisdom campus system of a university, and result proves that it is helpful for the managers to construct a more safe and stability system for the students and teachers with the model.

【Key words】 Internet of Things(IOT); hierarchy; security model; topology of IOT; attack model

DOI: 10.3969/j.issn.1000-3428.2011.14.001

基金项目：国家自然科学基金资助项目(60973140, 61003237)；国家“863”计划基金资助项目(2009AA01Z212)；江苏省自然科学资金资助项目(BK2009425)；江苏省青蓝工程基金资助项目；江苏省六大人才高峰及中兴通讯股分有限公司基金资助项目

作者简介：孙知信(1964－)，男，教授、博士生导师，1998年获南京航空航天大学博士学位，2001年~2002年在汉城国立大学进行博士后研究，现任南京邮电大学物联网研究院副院长、物联网学院副院长，主研方向：计算机网络与安全，多媒体通信，移动互联网计算等；骆冰清，南京邮电大学硕士研究生，主研方向：计算机网络与安全；罗圣美，博士、中兴通讯总工程师，主研方向：云计算，移动互联网；朱洪波，教授、博士生导师，现任南京邮电大学副校长、物联网研究院院长，主研方向：移动通信与宽带无线技术，无线通信与电磁兼容等

E-mail：sunzx@njupt.edu.cn

1 概述

根据国际电信联盟的定义[1]，物联网(Internet of Things, IOT)主要解决物品到物品(Things to Things, T2T)、人到物品(Human to Things, H2T)、人到人(Human to Human, H2H)之间的互连。而广泛意义上的理解，物联网即“物与物相连的互联网”，它包含2层意义：(1)物联网是在互联网的基础上延伸和扩展的网络，其核心仍然是互联网；(2)物联网的用户端延伸和扩展到任何物品之间进行信息交换和数据通信。物联网的推广使用能够给人们的生活带来便利，大大提高工作效率，改变人们的生活方式，但同时也必须注意到物联网的使用伴随着巨大的安全隐患。解决信息化与网络化带来的风险问题是物联网得以大规模使用的前提。目前适用于互联网的安全策略和算法在物联网时代并不能解决安全问题所面临的挑战，如何建立安全、可靠的物联网是一个迫切的问题。

考虑到物联网应用对安全的敏感度具备多样性，本文从等级划分这个特点出发，以互联网网络安全攻击为基础构建物联网攻击模型，以物联网实际应用为前提构建物联网拓扑模型，并在以上2个模型的基础上构建基于等级划分的物联网安全模型(Security Model of IOT Based on Hierarchy, BHSM-IOT)，利用结合三估计法的模糊评价模型对物联网应用进行等级划分，以此为基础对不同安全敏感度的应用进行区分配置。

2 相关研究

目前，物联网安全问题已经得到了学术界的广泛重视。文献[2-4]都从物联网的概念入手，分析物联网安全的重要性、物联网各逻辑层可能面临的安全问题以及能够采取的对应安全措施。但文献给出的均是概括性结论，并没有涉及到物联网安全的核心技术，而且未对相关技术能否适用于物联网给出分析评论。文献[5-7]研究了基于无线射频识别(Radio Frequency Identification Devices, RFID)的物联网安全，结合RFID自身特点研究物联网的安全需求，提出射频标签与阅读器之间的认证模型与加密策略。此类研究大多针对射频标签和阅读器间的安全策略，相对物联网整体来说，这部分研究只涉及到物联网前端的无线传感网安全部分。而目前针对物联网前端无线传感网和后端互联网安全的研究已相对成熟。

文献[8]研究了适用于无线传感网的IEEE802.15.4协议

中消息封装和认证对实时通信的影响。文献[9]在802.15.4的基础上提出了一种混合适应安全框架，解决了节点能量消耗和安全防范之间的冲突。然而这类研究并没有解决802.15.4协议本身存在的一些问题，如许多802.15.4设备是通过电池或太阳能供电，在出现低能量操作或能量失效时，如果出现清空的ACL表，将会出现Nonce值重用而破坏机密性；协议中使用计数器加密模式的AES-CTR安全组件，并不使用认证码MIC，从而产生很多弱点；由于确认帧缺少加密和认证支持，攻击方可从原始帧中获取合适序列号创建伪造的确认帧，这种脆弱性导致当攻击方存在时确认帧的不可靠性。

文献[10]提出了如何保证在6LowPAN网络中点到点的网络数据的可靠性和真实性的问题。然而，该安全方案没有考虑网络应用行业的不同而带来的安全敏感度的不同，针对不同的安全级别给出不同级别的安全技术组合也是平衡节点能量消耗和安全性能的一种重要方法。

文献[11]提出的ZigBee协议广泛用于短距离的无线传感网络，其安全机制不仅保证了机密性，同时具有低能耗、低复杂度的轻量级优点。该文深入剖析了ZigBee协议中的安全系统、无线数据传输网络和数据的加密与解密，并提出将ZigBee协议与IPv6相结合的思想。然而，ZigBee设备为了实现信任管理，必须依赖于认证中心，而认证中心的设置增加了网络节点的负担，同时主密钥的生成存在安全漏洞，容易引发攻击。

文献[12]提出了基于需求等级的传感器网络安全策略模型，通过将需求和策略分解、关联、组合，实现总需求与总策略的对接。但是，由于物联网的组织方式和通信方式与传感网不尽相同，因此传感网中一些现有的解决方案在物联网环境中可能不再适用；同时，物联网所处理的数据量将比现在的互联网和移动网大得多。

模糊随机变量的概念于1978年由H.Kwakernaak[13]首次提出。随后国内外不少学者对模糊随机变量进行了研究[14-15]。文献[16]将模糊评价模型用于系统未来安全状况的评价，并采用多个实例证明该评价方法具备较高的精确度，这种模糊评价方法为确定物联网不同应用的安全等级提供了新思路。

从以上研究工作可以看出：(1)国内对物联网安全技术的研究以安全框架和探索研究居多，具体安全技术的研究较少。(2)目前，国内对物联网安全技术的具体研究大多集中在RFID系统上，对中继节点包括整个接入网的安全技术研究较少。(3)国内外目前较为流行的无线通信协议均采用为不同安全等级应用配置不同加密等级策略的思路，但针对如何为物联网应用划分安全等级的研究较少。

本文在研究国内外物联网安全技术发展的基础上进行了以下工作：(1)提出一个基于等级划分的物联网安全模型。(2)提出了物联网拓扑子模型和物联网攻击子模型架构。(3)利用模糊评价模型和简易的三估计法判定物联网应用安全等级。本文的研究目的在于将目前对物联网安全的研究内容进行有效整合，使研究者能够更加清晰地了解物联网安全；从新的角度研究物联网安全，解决物联网安全实际面临的等级划分问题，使物联网安全技术的应用更加准确、高效，并降低资源消耗。

3 基于等级划分的物联网安全模型

3.1 BHSM-IOT模型对象及相关定义

一个应用系统的运行是靠众多元素完成的，而应用系统中的相关元素同时也是构成该模型的重要对象。在整个应用系统的安全运行和维护中起主导作用的是应用系统管理员(Application System Administrator, ASA)和用户(User)。维护数据单元(Maintenance Data Unit, MDU)、系统硬件设备(System Hardware, SH)、应用涉及范围(Application Range, AR)、应用类型(Application Type, AT)和敏感数据单元(Sensitive Data Unit, SDU)等是被动(passive)的元素。为了区分这些元素，将元素定义为：(1)主体(Subject),即主动元素，如用户、应用系统管理员；(2)对象(Object)，即被动元素,有维护数据单元、系统硬件设备、应用涉及范围、应用类型和敏感数据单元。因此，可以得到：

Subject = User ∪ ASA

Object = MDU ∪ SH ∪ AR ∪ AT ∪ SDU

Element = Subject ∪ Object

定义1 应用系统管理员指维护应用系统安全、为应用系统用户分配资源的主体。其自身的专业水平决定了其本身的安全等级。本文中其安全等级由高到低依次为：4，3，2，1。

定义2 维护数据单元指ASA在对应于系统的日常维护工作中涉及到的数据对象，包括安全检测时隔、故障维护延迟和数据备份间隔等。

定义3 应用系统硬件设备指该物联网应用的构建与实施过程中所需要的硬件设备，此对象包括硬件设备数量、硬件安全等级等。

定义4 应用涉及范围指该应用所涉及覆盖的物理和逻辑范围，包括网络覆盖范围、所涉及的人群类别。

定义5 应用类型指具体此物联网应用所属行业。

定义6 敏感数据单元指该物联网应用中可能涉及的敏感数据，包括数据量比率、数据影响度。

当然，应用系统的对象在实际中还有其他一些元素，如制度、IP地址、各种电子文档和操作手册，本文暂不做研究。

3.2 BHSM-IOT模型架构

BHSM-IOT架构如图1所示，包括应用需求分析、网络拓扑分析、攻击类型预测及应用安全等级判定4个部分。

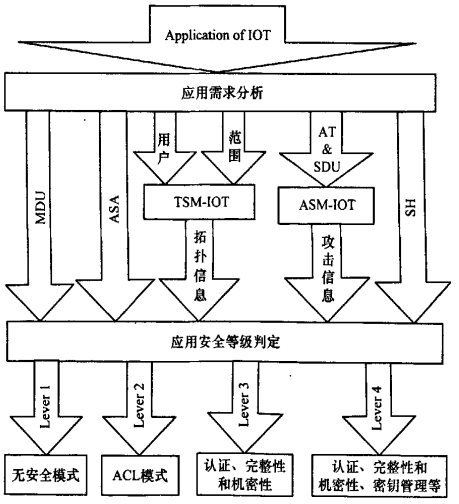

图1 基于等级划分的物联网安全模型

应用需求分析的功能是对某一物联网应用进行相关数据搜集，其中包括应用系统维护管理工作、维护人员专业水平、应用涉及物理范围、应用客户数量、应用类型和敏感数据量以及应用系统硬件安全水平。根据应用客户数量和使用范围

分析该应用规模，经由拓扑模型抽象出此应用服务的网络拓扑。同时根据应用类型和敏感数据量经由攻击预测模型预测攻击类型和所属逻辑层次。最后依据已有信息通过制定判定规则给出此类应用的安全防护等级以及相应的防护策略。

下面先对该模型涉及的对象和主体给出定义与相关属性，其次给出物联网拓扑子模型(Topological Sub-model of IOT, TSM-IOT)和物联网逻辑层攻击子模型(Attack Sub-model of IOT, ASM-IOT)，最后定义应用安全级别的判定原则，并给出应用安全等级的判定步骤以及安全应用技术。

3.3 TSM-IOT 架构

物联网的建立是在多网融合的基础上完成的，而物联网应用又涉及到各行各业，小到智能家居，大到电力、医疗行业应用。不同应用复杂度和应用需求对应的网络拓扑也不尽相同。本文在无线传感网络拓扑研究的基础上总结出以下3种物联网拓扑模型：

TSM-IOT I：广域或局域网—基站—分网—汇聚节点—感知节点；

TSM-IOT II：远程客户端—(移动通信网)—互联网—基站—汇聚节点—(簇首)—感知节点；

TSM-IOT III：远程客户端—(移动通信网)—互联网—物联网网关—物联网终端—(标签)。

模型 I 适合小型范围的行业应用，例如：环境应用，医疗应用；模型 II 适合物联网终端分布较广且移动性较强的应用，例如：物流跟踪，安全交通；模型 III 适合方便有线连接、终端移动性一般不突出的物联网应用，例如：智能家居，智能楼宇，工业检测。TSM-IOT 的总体架构如图 2 所示。

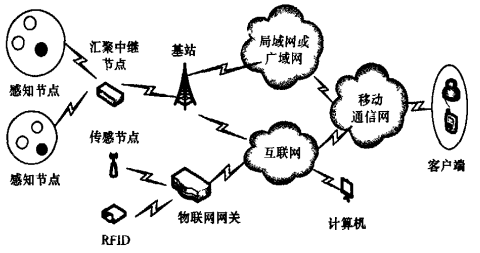

图 2 TSM-IOT 架构

不同的拓扑模型适用于不同的物联网应用需求，同时拓扑结构的安全性能也有所不同。因此，将物联网拓扑对安全的影响度作为判定该应用所属安全域的一个重要指标。

3.4 ASM-IOT 组成

根据功能的不同，物联网网络体系结构大致分为 3 个层次：用来进行数据采集功能的感知层，用来进行数据传输的网络层以及对数据进行处理和应用的应用层。通过分析物联网攻击模型，可以预测某一物联网应用可能遭受的网络攻击，由此提高应用系统的安全防御能力。

物联网的感知层由于网络本身的限制，在实际应用中显得十分脆弱，节点的特殊性和开放性使得无线传感网络的信息易受到监听、篡改、伪造和重播；并且物联网中大多数节点能量有限，攻击者可以通过连续发送无用的数据包消耗节点的能量，缩短节点的使用寿命，同时浪费了大量的网络带宽。具体攻击种类如表 1 所示。

表 1 感知层攻击类型

逻辑层	攻击类型
物理层	拥塞攻击、物理破坏、节点复制攻击
数据链路层	碰撞攻击、非公平竞争、耗尽攻击

物联网网络层所处的网络环境也存在安全隐患。由于不同架构的网络需要相互连通，因此在跨网络架构的安全认证等方面会面临更大挑战。本文通过研究互联网各层攻击模型和无线传感网可能存在的攻击类型，对物联网的网络层攻击种类进行了归纳与描述，物联网网络层将会遇到如表 2 所示的安全挑战。

表 2 网络层攻击种类描述

攻击种类	描述
IP 碎片攻击	修改或重构报文中的分片或重组，从而引起意外重组、重组溢出、重组乱序等问题
选择性传递攻击	恶意节点随机选择或者选择性丢弃含有重要信息的数据包，从而破坏路由协议
Sybil 攻击	恶意节点伪造身份或俘获合法节点从而获取数据
污水池攻击	提供虚假高质量路由信息从而破坏路由负载均衡
虫洞攻击	利用虫洞产生污水池，再进行选择性转发或者改变数据包的内容
虚假路由信息	攻击者通过提供虚假的路由信息，造成资源浪费、改变路由路径或者造成回路
跨异构网络的网络攻击	攻击异构网络的信息交换过程

物联网应用层的重要特征是智能，但自动化处理对恶意指令信息的判断能力有限，智能也仅限于按照一定规则进行过滤和判断，攻击者很容易避开这些规则，因此，应用层的非法人为干预、设备丢失和隐私数据窃取问题都很可能导致智能变低能、自动变为失控。由此可见，网络攻击无处不在，攻击类型各异。针对不同的物联网应用，攻击者的出发点也会有所不同。通过分析某一类物联网应用的应用类型、应用场合和敏感数据源，能够有效发现攻击者的合理攻击目标，进而可以预测此类应用可能遭受攻击的概率以及强度，以此为依据推测该应用的安全等级域。

3.5 应用安全等级判定

目前，一些较为流行的无线通信协议如 ZigBee、6Lowpan 以及 802.15.4 中的安全协议都通过划分应用安全等级来减少网络节点的能量消耗。然而对如何划分物联网应用业务安全等级的研究却相对较少，其中很重要的一个原因就是对安全评定标准的不确定性。物联网应用安全等级本身具有模糊性，对安全的敏感程度没有量化的标准，更无法获取精确的数据，因此，本文利用结合三估计法[17]的模糊评价方法来判定物联网应用的安全等级。

3.5.1 判定原则

判定主体是某一物联网应用的安全等级。

判定因素由本文提出的 BHSM-IOT 模型可以搜集到某一物联网应用的分析数据，包括定义 1~定义 6 以及拓扑信息和攻击信息。这里定义如下 5 个元素作为判定因素：

元素 1(ASA)：应用系统管理人员水平。

元素 2(MDU)：应用系统安全维护。

元素 3(SH)：应用系统硬件水平。

元素 4(TI)：网络拓扑影响度。

元素 5(AI)：攻击强度预测。

判定原则包括：

(1)管理人员专业水平越高，应用系统安全度越高。

(2)应用系统维护情况越良好，该应用安全度越高。

(3)应用系统硬件安全水平越高，该应用安全度越高。

(4)网络拓扑影响安全能力越低，该应用安全度越高。

(5)攻击预测越详细，该应用安全度越高。

3.5.2 判定方法

应用安全等级判定方法步骤如下：

Step1 确定评价指标 $u_i(i=1,2,\cdots,5)$，其中的 u_i 就是

3.5.1节的5个评价元素。

Step2 确定评语等级论域$V=\{v_1,v_2,v_3,v_4\}$，其中，v_1为1级，即安全等级最低；v_2为2级，以此类推；4级的安全等级最高。

Step3 建立因素与评语之间的模糊关系矩阵。

逐个对被评事物从每个因素$u_i(i=1,2,\cdots,5)$上进行量化，即确定从单因素来看被评事物对等级模糊子集的隶属度$(\boldsymbol{R}\mid u_i)$，进而得到模糊关系矩阵：

$$\boldsymbol{R}=\begin{bmatrix}\boldsymbol{R}\mid u_1\\ \boldsymbol{R}\mid u_2\\ \vdots\\ \boldsymbol{R}\mid u_5\end{bmatrix}=\begin{bmatrix}r_{11} & r_{12} & \cdots & r_{14}\\ r_{21} & r_{22} & \cdots & r_{24}\\ \vdots & \vdots & & \vdots\\ r_{51} & r_{52} & \cdots & r_{54}\end{bmatrix}_{5\times 4}$$

矩阵$\boldsymbol{R}$中第i行第j列元素r_{ij}表示某个被评事物从因素u_i来看对v_j等级模糊子集的隶属度。

Step4 确定评价因素的权向量，即对每个因素的重视程度。

在模糊综合评价中，确定评价因素的权向量：$\boldsymbol{A}=(a_1,a_2,\cdots,a_5)$。权向量$\boldsymbol{A}$中的元素$a_i$本质上是因素$u_i$对模糊子集的隶属度。这里使用三点估计法来确定评价指标间的相对重要性次序。由此确定权系数，并且在合成之前归一化。即$\sum_{i=1}^{5}a_i=1,a_i\geqslant 0,i=1,2,\cdots,5$。

三点估计法[17]步骤如下：把因素的权重看成随机变量，它的分布近似于正态分布。根据专家打分，得到每一个因素权重序列，将其平均得到序列的平均值m。将大于和小于m的权重序列再平均得到a和b。正态分布在m处为单峰；m的可能性2倍于a，则m与a的平均值为$(a+2m)/3$；m的可能性2倍于b，则m与b的平均值为$(b+2m)/3$。以上两点平均值为$X_j=\dfrac{(a+b+4m)}{6}$，方差为$\sigma=\dfrac{b-a}{6}$。

将根据上述a、m、b3点得到的估计量X_j作为因素权重的估计值并进行归一化处理后，可得到因素指标的权重分配。

Step5 合成模糊综合评价结果向量。

利用合适的算子将$\boldsymbol{A}$与各被评事物的$\boldsymbol{R}$进行合成，得到各被评事物的模糊综合评价结果向量$\boldsymbol{B}$，即：

$$\boldsymbol{A}\circ\boldsymbol{R}=(a_1,a_2,a_3,a_4,a_5)\circ\begin{bmatrix}r_{11} & r_{12} & \cdots & r_{14}\\ r_{21} & r_{22} & \cdots & r_{24}\\ \vdots & \vdots & & \vdots\\ r_{51} & r_{52} & \cdots & r_{54}\end{bmatrix}=(b_1,b_2,b_3,b_4)=\boldsymbol{B}$$

其中，b_1是由$\boldsymbol{A}$与$\boldsymbol{R}$的第j列运算得到的，它表示被评事物从整体上看对v_j等级模糊子集的隶属程度。

Step6 对模糊综合评价结果向量进行分析。

根据实际情况分析此物联网应用所得到的模糊综合评价是否准确，一般也可以采用最大隶属度原则进行判定。

3.6 安全技术应用

某一物联网应用通过BHSM-IOT模型的训练后可以判定此应用安全所属级别，得知应用安全等级信息有助于为此应用配置相应的安全技术，减少不必要的资源消耗。如图1所示，BHSM-IOT模型为所属安全等级为1的应用配置无安全模式，为安全等级为2的应用配置ACL模式，安全等级达到3和4的应用配置机密性保护、完整性保护和认证等其他安全策略。

在无安全模式下，应用系统包括其数据和设备均不需要配置安全保护策略。这种配置涉及的应用较少，例如环境生物监测。该应用的数据通常只在长时间监测下才有效，小范围时间内的监测数据一般变化微弱，少量数据窃取对此类应用来说没有任何意义。因此，此类应用经过分析和判定，基本数据安全等级为1的安全域，为其配置无安全模式即可。

ACL模式即访问控制模式，此策略配置在安全等级为2的应用中。一般在数据链路层进行此模式的安全技术应用。ACL工作模式也不对MAC帧做任何加密或修改操作，仅提供给设备一种按帧中源/目的地址进行过滤的机制，并将结果指示给高层。安全等级为2的应用较多，例如家庭应用、工业质量检测、商务应用。

模型中为等级3和等级4的应用配置了认证、机密性保护和完整性保护措施等常用策略。物联网的大部分应用都隶属于该等级域，物联网安全技术的研究也大多是针对这2个安全等级域中的应用而讨论的。而等级3和等级4之间的安全配置差别并不是特别明显，可以根据具体的应用配置不同的安全策略。以本文提出的BHSM-IOT模型为基础，亦可以对等级3、4中的物联网应用进行更加详细的分析。物联网应用安全是物联网大规模发展的前提，但物联网网络终端和中继节点由于其自身特点都不适合过于复杂的安全保护策略。因此，轻量级的安全技术是需要进一步深入研究的课题之一。

4 BHSM-IOT模型的应用

根据以上模型，可以对某大学智慧校园应用的安全等级进行如下分析与判定：(1)对智慧校园的维护情况、系统管理员专业水平情况、网络覆盖范围、涉及的学生人数、教师人数、食堂、图书馆和校园商店的使用情况、涉及存储的数据单元以及硬件配置情况进行了解和核查。(2)根据搜集到的信息，分析学校智慧校园网络的拓扑模型。(3)根据应用环境，分析该系统和网络可能受到的攻击行为。(4)根据模糊评价模型判定此智慧校园应用的安全应用等级，为其配置合理的安全技术策略。

4.1 应用环境

实验对象是某大学校园的“智慧校园”工程，该大学分为A、B 2个校区。网络覆盖范围包括2个校区的大部分楼宇。涉及的师生共计35 768人，其中，教职工2 292人；研究生7 714人；本科生25 762人。数据模式共205项，其中，基本信息模式25项；人力资源子集23项；科研子集37项等。部署实施栏目176个。基础平台包含：信息门户服务，数据集成服务，身份集成服务，协同工作平台，综合监控服务平台，数据与信息标准建设，相关网络及服务器硬件设备。智慧校园涉及的服务应用如图3所示，其网络拓扑如图4所示。

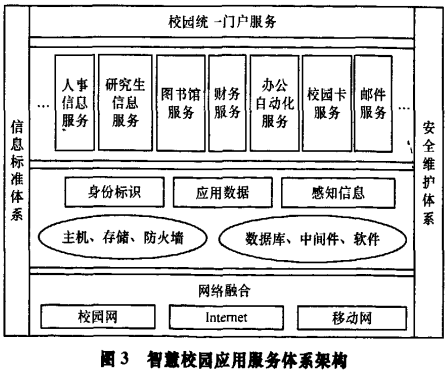

图3 智慧校园应用服务体系架构

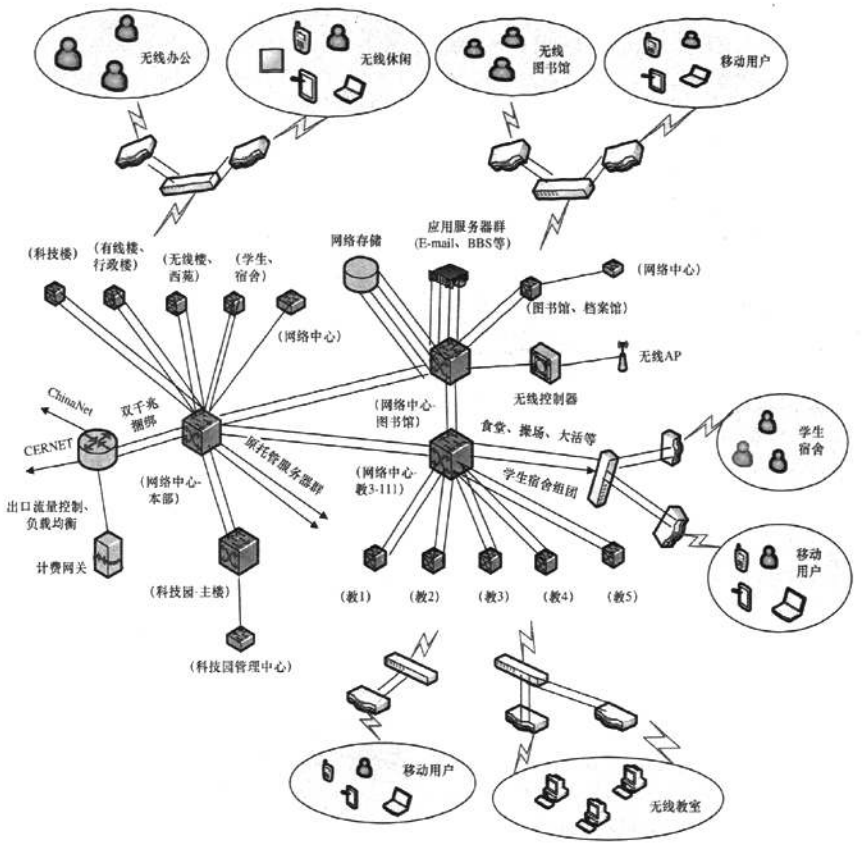

图4 智慧校园网络拓扑

4.2 应用分析

根据模型对“智慧校园”应用进行了信息查询与整理，利用已知信息由TSM-IOT和ASM-IOT进一步对该物联网应用做分析与处理可以获得其抽象物联网拓扑模型和预测攻击模型，最后根据其拓扑信息、维护管理信息、硬件信息及攻击信息等构成模糊评价模型的判定元素，由专家打分后根据模糊评价计算模型对该物联网应用进行安全等级域的评定，从而为其制定相应的安全防护策略。

4.2.1 拓扑研究

根据图4以及3.3节的TSM-IOT架构可以分析得出智慧校园网络的抽象拓扑。由图4可以发现，智慧校园应用根据其地域对无线区域进行了功能划分，例如无线教室、无线图书馆、无线休闲区域、移动区域和无线办公区域。其终端的移动性较小，门禁与一卡通应用服务的感知终端大多是固定属性。根据3.3节的TSM-IOT架构中的3个拓扑模型，可以很清楚地看出，该“智慧校园”应用的抽象拓扑属于TSM-IOT III的形式，即：

远程客户端—(移动通信网)—互联网—物联网网关—物联网终端—(标签)

以上结果符合3.3节中对3个拓扑模型各自常用应用的特点分析。

4.2.2 攻击模型分析

由图3所示的“智慧校园”应用服务体系架构和3.4节的ASM-IOT组成，可以对“智慧校园”可能面临的攻击做出预测。由图3可知，该应用服务涉及的敏感数据集中在财务系统和教务系统中，其他系统中的学生及教师的个人隐私信息也是敏感数据之一。另外，该物联网应用的无线覆盖范围广，无线硬件设备分布地区广、数量多，不排除这些设备会受到物理攻击和盗窃的可能。

根据ATS-IOT组成可以为该应用服务做出如表3所示的攻击预测。

表3 “智慧校园”攻击预测

逻辑层	攻击类型
感知层	拥塞攻击、物理攻击、耗尽攻击
网络层	Sybil攻击、污水池攻击、跨异构攻击
应用层	非法人为干预、设备丢失

4.2.3 安全应用等级判定

根据BHSM-IOT模型的数据流，在得到“智慧校园”应用的各类数据信息以及经过拓扑和攻击模型分析后，可以对其进行安全等级配置的评价，根据3.5节的安全等级判定过程，利用模糊评价方法做出如下判定：

Step1 确定U={系统管理人员水平,系统安全维护,系统硬件水平,网络拓扑影响度,攻击强度预测}。

Step2 确定应用安全度评价V={较低,一般,中等,较高}。

Step3 确定权重。

这里由专家组对每一个特征元素进行打分，然后使用三估计法得到 X_j，再对 X_j 进行归一化处理。假设专家打分由三估计法得到的归一化结果为：

$A=\{0.2,0.1,0.4,0.1,0.2\}$

Step4 建立隶属度模糊矩阵：

$$R=\begin{bmatrix}0.2 & 0.4 & 0.3 & 0.1\\ 0.0 & 0.2 & 0.5 & 0.3\\ 0.3 & 0.4 & 0.2 & 0.1\\ 0.1 & 0.3 & 0.4 & 0.2\\ 0.0 & 0.1 & 0.5 & 0.4\end{bmatrix}$$

Step5 合成模糊综合评价结果向量。

为了判断该应用系统的级别，将特征向量 U 构成模糊关系矩阵 R 与模糊子集 A 进行模糊复合运算。本文采用“·”和“+”模糊算子，记为模型 $M(\cdot,+)$。

设复合运算的结果为 B，则 B 中的元素为：

$$B_{ij}=\sum_{k}(a_{ik}\cdot r_{ij})=(a_{i1}\cdot r_{1j})+(a_{i2}\cdot r_{2j})+\cdots+(a_{ik}\cdot r_{kj})$$

其中，$a\cdot b=ab$，是乘积算子(代数积)；$a+b=(a+b)\wedge 1$，是闭合加法算子(代数和)；Σ 表示对 k 个数在“+”下求和。

$$B=A\circ R=$$

$$[0.2,0.1,0.4,0.1,0.2]\circ\begin{bmatrix}0.2 & 0.4 & 0.3 & 0.1\\ 0.0 & 0.2 & 0.5 & 0.3\\ 0.3 & 0.4 & 0.2 & 0.1\\ 0.1 & 0.3 & 0.4 & 0.2\\ 0.0 & 0.1 & 0.5 & 0.4\end{bmatrix}=$$

$$[0.17,0.31,0.33,0.19]$$

Step6 由最大隶属度原则可以看出，该“智慧校园”服务应用的安全等级为 3 级，即其安全等级域属于“中等”，在各类物联网应用中隶属安全需求较高的范围，因此，“智慧校园”的建设者和管理者需要高度重视其应用系统及网络的安全防护工作，为其配置认证、加密、密钥管理、路由聚合、数据完整性鉴别等多项安全措施，为该物联网应用的安全、可靠、稳定运行打好基础。

4.3 应用效果

目前该智慧校园的建设正逐步完善，学生服务应用的运行使学生查询成绩、选择课程、查看科研成果、一卡通使用情况等众多应用更加便捷。

智慧校园的学生服务系统页面如图 5 所示。

图 5 学生服务系统页面

图 6 展示了学生服务中的成绩查询页面。

图 6 学生成绩表页面

监控系统的运行保障了学生的人身财产安全和学校的公共设施与秩序安全。如图 7 和图 8 所示。

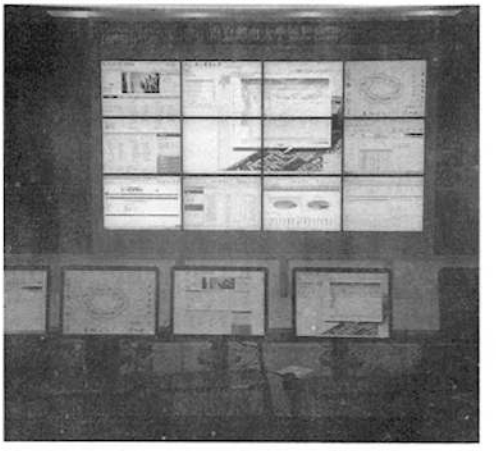

图 7 智慧校园监控室

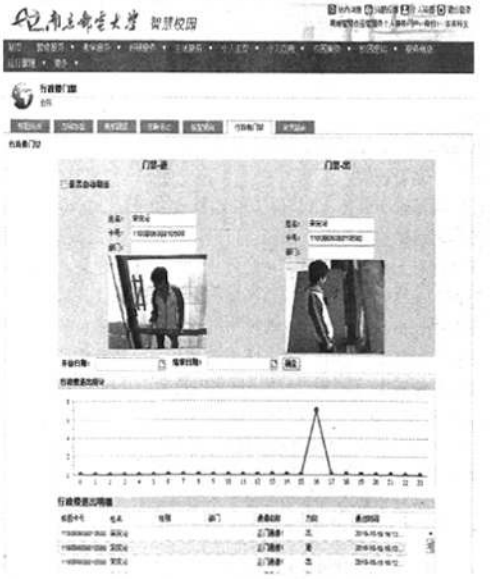

图 8 行政楼门禁监控与统计

智慧校园服务商店应用包括仓储服务、物流跟踪、校园感知、智慧旅游等，如图9、图10所示。

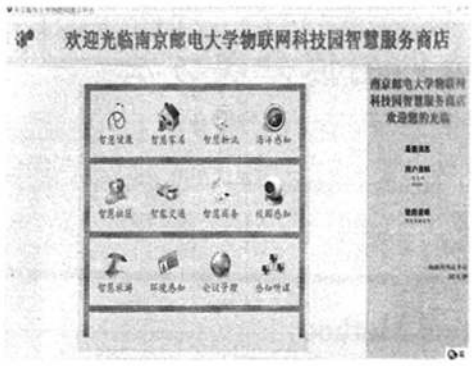

图9 智慧校园服务商店

图10 智慧校园服务商店会员中心页面

智慧校园的建立需要一定的发展阶段，通过本文提出的BHSM-IOT模型的分析有助于建立一个更加安全、稳定、可靠的智慧校园。在智慧校园的建设过程中，随着硬件设备的增加，面向信息服务的应用系统越来越多，数据存储量也越来越大，因此，可以不断地使用BHSM-IOT模型对当前应用服务建立的安全等级进行评定，及时修正必需与不必要的安全技术配置，减少不必要的资源消耗，同时建立更加完善安全的服务应用。

5 结束语

本文提出了一种基于等级判定的物联网安全模型BHSM-IOT，通过该模型中的物联网拓扑模型TSM-IOT，可以有效地抽象出各个物联网大型应用的网络拓扑，分析其结构数据与结构利弊；通过物联网攻击模型ASM-IOT，可以有效地分析物联网应用的攻击来源与攻击类型，为安全应用防御提供参考；通过模糊评价模型的判定方法，能够有效地为该物联网应用评定其安全等级，提供相应的物联网安全技术配置。

与目前国内其他物联网安全的研究相比，本文从一个较新的角度审视物联网安全，所提出的模型既整合了目前学者对物联网安全的思考，又另辟蹊径为未来物联网安全技术配置提供了参考。该模型的应用同时解决了众多物联网应用安全无法评定等级的难题。在此基础上，对轻量级物联网安全技术的研究是需要进一步探索的课题。只有将安全技术与该模型相结合，才能更好地体现该模型的价值与实用性。

参考文献

[1] ITU Internet Reports 2005: The Internet of Things[Z]. International Telecommunication Union, 2005.

[2] 李振油. 物联网安全问题研究[J]. 信息网络安全, 2010, (12): 1-3.

[3] Chen Xiangqian, Makki K, Yen Kang, et al. Sensor Network Security: A Survey[J]. IEEE Communications Surveys & Tutorials, 2009, 11(2): 52-73.

[4] 武传坤. 物联网安全架构初探[J]. 中国科学院院刊, 2010, 25(4): 411-419.

[5] 彭 朋, 韩伟力, 赵一鸣, 等. 基于RFID的物联网安全需求研究[J]. 计算机安全, 2011, (1): 75-79.

[6] 王后珍, 张焕国. 新型的轻量级数字签名方案[J]. 通信学报, 2010, 31(11): 25-29.

[7] 谷 峪, 于 戈, 李晓静, 等. 基于动态概率路径事件模型的RFID数据填补算法[J]. 软件学报, 2010, 21(3): 438-451.

[8] Chen Feng, Yin Xiaolong, German R, et al. Performance Impact of and Protocol Interdependencies of IEEE 802.15.4 Security Mechanisms[C]//Proc. of the 6th International Conference on Mobile Ad Hoc and Sensor Systems. Macau, China: IEEE Press, 2009: 1036-1041.

[9] Shon T, Koo B, Choi H, et al. Security Architecture for IEEE 802.15.4-based Wireless Sensor Network[C]//Proc. of the 4th International Symposium on Wireless Pervasive Computing. Melbourne, Australia: [s. n.], 2009: 1-5.

[10] Barker R. Security Aspects in 6lowPan Networks[C]//Proc. of Design, Automation & Test in Europe Conference & Exhibition. Dresden, Germany: [s. n.], 2010.

[11] Li Chunqing, Zhang Jiancheng. Research of ZigBee's Data Security and Protection[C]//Proc. of International Forum on Computer Science Technology and Applications. Chongqing, China: [s. n.], 2009: 298-302.

[12] 张鸿亮, 刘文予, 符明丽. 基于需求等级的传感器网络安全策略模型[J]. 微计算机信息, 2008, 24(13): 134-136.

[13] Kwakernaak H. An Algorithm for Rating Multiple-aspect Alternatives Using Fuzzy Sets[J]. Automatica, 1979, 15(5): 615-616.

[14] 张 跃. 模糊随机变量[J]. 哈尔滨建筑工程学院学报, 1989, 22(3): 12-20.

[15] Wang Guangyuan, Zhang Yue. The Theory of Fuzzy Stochastic Processes[J]. Fuzzy Set and System, 1992, 51(2): 161-178.

[16] 许开立, 陈宝智, 陈 全. 安全等级特征量及其计算方法[J]. 中国安全科学学报, 1999, 9(6): 6-12.

[17] 孙林柱, 杨 芳. 非确定信息评价的变权模糊方法[J]. 数学的实践与认识, 2009, 39(6): 12-17.

编辑 张 帆