物联网计算机网络安全技术

王益忠

（潍坊科技学院 山东 寿光 262700）

［摘 要］从某方面来讲，应用物联网计算机网络安全技术可以满足系统风险评估要求，并伴随着系统建设过程满足实时监控要求，将各类风险评估数据进行准确分析与记录，形成具有科学性与合理性的系统风险评估体系，并得出相应的评估报告，供给操作人员进行参考与决策，最大限度地降低风险损失。因而，本文主要分析探讨了物联网计算机网络安全技术，以供参阅。

［关键词］物联网；计算机；网络；安全技术

引言

1999 年，麻省理工学院（Massachusetts Instituteof Technology，MIT）提出了物联网的概念，其目的在于提高企业货物管理水平，实现自动化、智能化管理和控制“物”的目的。物联网技术的不断发展，为生产生活带来了极大的便利，但物联网安全问题也成为物联网技术发展的一个重要制约因素。企业在构建物联网系统的同时，还需要建立安全机制，采取有效措施，确保物联网系统运行的安全性与稳定性。现代网络技术的快速推进超过了网络安全技术的发展速度，技术、运用、信息、数据及管理等问题仍然亟需解决，以促进物联技术、系统和产品的应用与发展。

1 物联网概述

目前，学术界尚未对物联网形成统一的定义，从实质上来讲，物联网具体包括两层含义：一是物联网以互联网为基础，通过互联网实现物物相连，实现网络扩展与延伸；二是物联网利用识别技术、智能感知技术、普适计算等通信技术，进行物品之间的信息交流。在实际应用中，需将物联网与互联网、移动通信网整合起来，通过在建筑、电网、公路、供水系统、油气管道、道路照明等物体中嵌入感应器，从而构建起业务控制平台，实现对基础设施、设备等集中管控，促使人类的管理活动可以向更加智能化、精细化的方向发展，提高生产力水平。

2 物联网计算机网络安全技术

2.1 加密机制

加密方式包括逐跳加密与端对端加密两种。逐跳加密的传输过程是以加密方式完成的，但在加密时需要不断地对每个传输经过的节点进行解密与加密，每个加点上的信息均是明文形式。逐跳加密是在网络层中完成加密，可适用于各种业务需要，保证了安全机制在业务中的透明化，具有延时低、可扩展、效率高的特点，能够加密受保护链接，需要传送节点有较高的可信度。端对端加密则能够根据业务类型选择合适的安全策略和加密算法，进而为业务领域提供端到端安全加密措施，确保业务安全性。该加密方式不能对消息目的地址加密，无法掩盖信息传输的起点与终点，受到恶意攻击的可能性较高。因此，在物联网中，可以采取逐跳加密，端对端加密可以作为一种安全选项，用户安全需求较高时，可启用这种加密方式，以提供端到端安全保护。在加密算法中，哈希锁是一种主要方法，以此为基础，可以对加密技术进行改进，以适用于不同领域要求。

2.2 个人隐私保护

物联网网络中，并不需要依靠人工的力量进行设备维护，如此就造成网络被恶意攻击之后，个人隐私信息容易被泄露。在 RFID 系统内部，系统入侵者能够自动扫描出带有电子标签的私人信息，并且对这些信息进行恶意窃取与非法盗用，甚至定位与跟踪这些信息，以此挖掘用户更多的私人信息，造成物品所有者身份信息的外泄。对此，应该进一步做好物联网个人隐私保护工作，从技术和管理等方面，提升保护力度。首先，从技术层面而言，可以通过对授权认证与加密等技术的引入，增强网络的安全性能，确保用户的个人隐私不被轻易泄露。从管理层面而言，需要限定物联网终端设备数据管理权限，完善管理制度，有效保护用户的个人隐私。

2.3 对终端设备进行实时监测

为避免物联网终端设备遭到破坏，可以在相应的设备上建立起网络监测系统，从而实现对物联网终端设备进行有效的监管保护。当设备受到一定程度的损坏时，网络系统即会向服务器发出预警消息，并且能够记录下对服务器破坏的全过程，以方便相关负责人员对破坏者进行责任追究。如此以来，自然能够有效的对物联网终端设备进行保护与检测。从而避免终端设备受到破坏而对信息的传输造成影响。

2.4 安全路由

由于物联网中包含了感知和通信两大网络体系，从而使得物联网路由需要跨越多类网络，如基于 IP 地址的路由协议、基于标识的传感网路由算法等等，在这一前提下，为保证路由的安全，需要解决如下两个方面的问题：多网络融合后的路由安全和传感网的路由安全。对于前者而言，需要重点考虑的是将身份标识映射成与 IP 地址相类似的信息，由此便可构建起基于 IP 地址的统一路由体系。对于后者而言，传感器网络的计算资源较为局限，并且容易受到网络攻击，因此，必须设计出一套合理可行的安全路由算法，从而有效抵抗入侵者对路由的攻击。从现有的技术手段上看，实现安全路由的方法有两类，一类是借助密钥构建安全的通信环境，为路由信息的交换提供安全保证；另一类是借助冗余路由对数据包进行传递。无论采用何种方法确保路由的安全，都应当在设计之初予以考虑，并结合物联网的应用特点对路由进行安全设计。

2.5 防火墙与入侵检测技术

为加强传输安全，可基于物联网组网特征与性能要求，研制专用的特殊防火墙，以制定安全性更高的访问控制策略，对类型不同的网络进行隔离，以确保整个传输层的安全。在应用层可采用入侵检测技术，及时发现并检测入侵和入侵企图，并采取有效措施修复漏洞。一方面，可检测异常入侵，结合异常行为与计算机资源情况对入侵行为进行检测，通过定量分析方法设定可接受的网络行为特征，与非正常的和潜在的非法入侵行为进行区分。另一方面可检测误用入侵，通过系统与应用软件的已知弱点攻击方法检测入侵行为。要结合物联网特征，构建一套和物联网系统相适应的高效的入侵检测技术，提高物联网系统安全性。

结束语

总而言之，在计算机物与联网系统中，做好数据信息安全管理工作的重要性不言而喻。为了确保各项信息的安全性和个人隐私不轻易泄露，就需要对计算机物联网网络安全问题进行全面把握，并且结合实际的需求，给予有效的保护，增强计算机物联网网络的安全性，促使计算机物联网网络稳定运行，为广大用户提供便利，促进物联网网络的可持续发展。

参考文献

[1] 李磊．物联网计算机网络安全与控制策略研究 [J]. 无线互联科技 .2018(11)

[2] 李缘圆，胡军，叶炳．计算机与物联网网络安全与控制 [J]. 电脑迷 .2018(21)

[3] 王士鑫．物联网计算机网络安全与远程控制技术初探 [J]. 电子技术与软件工程 .2018(02)