基于物联网的计算机网络安全防护对策分析

黄鸿运

海南师范大学　海南海口　571127

摘　要：物联网（IoT）是一种以传感、通信为基础的新型网络体系结构，具有可分工、协调、组织性等诸多社会属性。所以，其被广泛地运用于现代工业生产中，并逐步延伸至当今智能家居。然而，随着物联网的快速发展，其安全隐患也日益突出，突出体现在终端节点安全、通信信息安全、感知层面等多个层面，已成为制约物联网技术推广与应用的瓶颈。因此，本文从物联网的角度出发，研究基于物联网的计算机网络安全防护对策，进一步提高物联网的安全性能。

关键词：物联网；计算机网络安全；防护对策

引言

在物联网环境下，计算机网络的安全是保障信息安全的重要一环。目前，随着物联网技术的发展，计算机网络的安全性存在很多问题。因此，在建立物联网系统时，研究者应当根据其表现和具体需求，采取行之有效的安全管控措施，提升物联网的安全性，例如应用防火墙技术、建立隐私保护机制等，从而降低物联网中存在的安全隐患，推动物联网的发展。

1. 物联网的定义

物联网是一种以人为基础、网络为基础，以必要的认知目标为基础的数据交流网络。利用所搭建的物联网，可以对所需的各类数据进行有效地收集和处理，充分地将互联网和真实的社会联系起来。物联网以互联网为基础，能把各种信息传感设备和互联网连接起来，构成一张巨大的网，使一切事物连在一起。目前，物联网已成为信息科技的一个重要组成部分，然而，物联网的本质仍然是互联网，是互联网的延伸与发展。能够实现高效的信息交流和技术支撑。物联网技术是一种新型的物联网技术，能够将物联网中的各类要素与网络相结合，提升信息交互与交流效率，实现对目标的智能识别，为下一步的跟踪、定位、管理等工作打下坚实的基础。这一概念最初由比尔·盖茨提出，但由于其自身的限制，如硬件、无线网络和感应装置等，并未受到太多重视。随着互联网等新兴技术的快速发展，各种感知技术得到快速发展，成为推动物联网发展的重要力量。其中，高频识别技术、云计算技术、M2M 系统架构技术以及传感技术是其中的核心技术。目前，物联网得到了广泛的应用，并对有关行业的发展起到了积极的推动作用，提升了智能程度，优化了资源分配，拓展了服务领域，具有广阔的发展前景和良好的应用前景。

2. 物联网背景下计算机网络安全概述

2.1. 计算机网络安全概念

计算机网络安全是指对计算机网络进行安全保护的软硬件体系。当计算机网络受到病毒或木马等威胁时，可以使用计算机网络安全技术进行修复，既能保证其正常工作，又能减少对其造成的危害。计算机网络的安全可以分为逻辑上的安全，物理上的安全，系统上的安全。所谓逻辑安全，就是在软件运行过程中，为保证数据的可用性、保密性和完整性而采取的一种手段。物理安全是指对计算机系统及与之有关的其他软、硬件设施所进行的物理保护，在日常工作中所用到的防火墙及防毒软件，都是在系统运作时所采用的安全策略之一。

2.2. 物联网背景下计算机网络安全的重要性

物联网是一种智能化物理设备网络，通过互联网技术采集并传输海量的信息，能够在各个元素间建立起某种联系，从而给使用者带来方便的服务。例如，共享单车，汽车自动驾驶，智能家居控制等。但是，在物联网对人类社会发展做出巨大贡献的同时，其安全隐患也日益突出。为保证数据的安全、有效，必须采用相应的技术保障。计算机网络安全就是在物联网环境下，通过与网络有关的技术对信息进行保护。但若不能有效保障计算机网络的安全，则会导致海量数据在物联网中被泄漏、被操控。所以，从长远的角度来看，加强对计算机网络安全的研究是十分必要的。

3. 基于物联网的计算机网络安全问题

3.1. 在通信方面存在的安全问题

在物联网实际运行中，由于通信端口的限制，导致物联网负载，从而对整个网络构成巨大的安全隐患。具体而言，主要有两点：一是网络运行超载。物联网中已存在大量的网络设备，没有这些设备的支撑，其稳定运行是无法实现的。但是，目前的认证分析手段不能对所有的网络数据进行有效地监控，从而不能与大部分终端或系统进行高效的互联，造成整个物联网运行超载。二是密钥管理方式不够合理。若要将物联网中的数据传输到通信终端，则需要通过系统的身份验证，并对其进行加密与管理。但是，在此过程中，常常需要接入其他的物联网设备，造成大量的资源浪费，使得密钥管理工作显得非常不合理。

3.2. 感知层安全问题

一是安全隐私问题。将 RFID 等多种传感器件植入相应的物体中，并进行一维码或二维码的扫描、追踪和定位，并防止个人隐私被侵犯，标记对所有的要求作出反应，使追踪和查找变得容易。二是智能感知节点安全问题。一般使用物联网设备进行无人监测，但其所处的地域分布比较广，很可能会被黑客侵入，造成装置损坏或者被黑客操纵。三是信号干扰。由于采用无线接入方式，因此无线信号是开放的，易受多种干扰，不利于物联网终端间的通信。四是数据传输安全性问题。通常情况下，数据发送都是以广播的形式进行的，因为传感节点的容量是有限的，所以不能保证信息的安全性。若将其置于公众的无线网络中，那么会存在被攻击、破坏或窃听的危险，无法保证信息的安全。

3.3. 数据保护问题

在物联网环境下，传感器是获取信息的重要方式。在数据采集结束之后，还应按照具体的要求将数据传送出去。但是，由于信息传送的安全问题，如信息的保密不准确等，从而造成数据的损失。从物联网的体系结构上讲，其核心作用是为内部用户、设备和传感器等提供连接，使得数据信息可以在网络结构中稳定地传输，方便用户进行数据信息的传输。

3.4. 在终端节点方面存在的安全问题

随着物联网系统的迅速发展与普及，各种终端设备的种类与数量日益增多，其中包含无线与移动两种类型。但是，不管采用什么样的通信模式，大部分的通信终端都是自动化运行状态，这极大地增加了通信终端被破坏的风险，严重影响了物联网的正常运行。此外，由于网络中存在的恶意行为，使得网络中的用户无法正常工作。恶意模拟感知节点将导致错误消息泄漏或者有效信息资源被监听，从而威胁到用户的人身和财产安全。

4. 基于物联网的计算机网络安全防护对策

4.1. 构建全方位加密系统

4.1.1. 软件加密技术

在物联网领域，存在着各种各样的安全问题，其中，软件安全缺陷是导致计算机网络安全下降的一个重要原因。为防止因软件安全漏洞而导致的安全问题，可采用软件加密的方法。在计算机上安装性能优良、功能完善的杀毒软件，依赖杀毒软件对计算机系统进行定期性的扫描，一旦发现不正常的数据，应立即进行清理。利用杀毒软件防止计算机网路中的病毒与木马，是提升计算机网络安全效能的最佳途径。

4.1.2. 数据库加密技术

数据库作为“数据仓库”，负责对网络数据进行整理、存储，是一个非常重要的工作。在当今信息技术飞速发展的今天，数据库已成为物联网中必不可少的一种基本软件。所以，在物联网计算机网络中，数据库占据着最大的存储空间，因而显得尤为重要。当数据库存在安全性隐患时，网络故障就会增加，因此，为增强物联网计算机网络的安全性能，有效防范各类安全问题，需要将数据库加密技术引入到物联网计算机网络中，并对其权限进行管控。采用加密算法对数据库的权限进行管理，保证非授权用户不能对数据库进行访问，以达到数据保密的目的。相对于其它加密算法，数据库由于其密码算法更加复杂和难以破解而显得尤为重要，对提升物联网中的计算机网络数据库的安全性有很大的帮助。当未被授权的使用者侵入数据库中时，系统将会发出警报，以避免不法分子侵入计算机网络数据库，造成安全隐患。

4.1.3. 传输加密技术

这一技术主要是为了保证在物联网中的计算机网络中进行数据与信息的安全传输。该技术被广泛地运用于整个物联网计算机网络中。在物联网环境下，传输加密技术由数字签名技术、密钥加密技术以及数字文摘技术等组成。数字签名是指数据传送者利用无法模拟或伪造的数据序列，以确定数据传输的安全性。数字文摘就是把数据信息按照一定的长

度规格截取，然后将其转化成 128 位长度密文，从而达到对数据进行加密的目的。在接收者收到消息后，利用 128 位长度密文对其进行安全性检验，从而达到对物联网中计算机网络进行加密传输的目的。

4.2. 开发防火墙技术

物联网的环境和正常的网络体系有较大区别，当使用这种技术提高网络安全性的时候，需要根据物联网计算机网络的特点，制定出合适的防火墙技术，并根据计算机的实际情况，建立完整的数据传送机制。另外，针对不同的系统，应根据需求，建立合理的网络防火墙系统，提高网络安全存取程度，以达到有效地隔离与提高安全性。另外，将入侵检测技术引入到物联网的各个应用层，使使用者能够迅速发现并确认入侵行为，并对入侵行为进行解析，并对其进行修补。

4.3. 融合应用区块链技术

物联网节点分布广、数据量大、应用环境复杂，为其带来了巨大的安全隐患，成为制约其推广应用的主要瓶颈。本项目以其去中心化、不变性、加密算法及链式结构等特性，为提升物联网安全水平提供一种全新的思路。区块链认证与一致性机制能够强化终端的身份认证与追踪，防范非法或未授权程序的介入，能够有效防范恶意入侵造成的网络瘫痪，保障物联网的安全。区块链的技术优势也将进一步完善物联网信任机制，推动物联网智能应用的拓展，促进物联网的技术和应用方式的创新。

4.4. 完善隐私保护系统

在物联网中，隐私保护一直是人们关注的焦点和难点，为此，有必要对物联网环境下的隐私保护系统进行改进，以更好地保障网络中的隐私保护。首先，可以在技术上进一步改进物联网环境下的隐私保护系统。在物联网实际运作中，通过对每个节点进行身份验证和授权，可以有效地防止恶意软件的侵入，保障使用者的隐私。另外，还可以从网络安全的角度出发，进一步提高网络环境下的安全保障水平。可以由专业的网络管理人员维持使用者的个人隐私，并借助相应的设备保障数据信息的安全。同时，也可以设定对应的信息保护代码，提高使用者信息的隐私性。

4.5. 设置 VPN 虚拟专用网络

虚拟专用网络技术（VPN）是一种通过公开的、不安全的媒介，通过互联网等公开的、不安全的媒体来建立具体的连接技术，加强物联网环境下的计算机网络的安全性。利用 VPN 的虚拟专用网络技术，既能保证非安全介质的安全传输，又能保证公开介质传输。VPN 是一种应用非常广泛的物联网安全技术，能够为物联网的安全运行提供可靠的保障。在 VPN 技术的实际应用中，通过建立安全信道与连接，将物联网、用户、设备三者有机地结合在一起，构成了一种新型的物联网架构。PN 技术具有较高的安全性能和较好的物联网稳定性。另外，VPN 虚拟专用网络的内部架构可随需扩充，使使用者能在网际网络中高效地连结。在搭建虚拟专用网络的过程中，可以根据用户的需求，灵活地设置服务器防火墙、无线路由器和 VPN 设备（如 H3C、Cisco 等），并在系统中安装 CheckPoint,L2TP,PPTP 等软件。保证虚拟专用网络的有效运行，能够有效地提升物联网系统的安全性。

5. 结束语

综上所述，近几年来，随着物联网技术的迅猛发展，人们在享受便捷的同时，也对其安全性提出了更高的要求。针对目前我国网络安全存在的各种隐患，需要对其进行深入的分析，并借鉴相关的网络安全提高其安全防护。在物联网的环境中，要实现对数据的安全管理，必须要与现代的网络安全技术相融合，从而制定防护措施，将安全风险与损失降到最低，保证计算机网络稳定与安全。

参考文献

[1] 张婧 . 物联网计算机网络安全与远程控制技术研究 [J]. 软件 ,2021,42(11):166-168.

[2] 游海英 , 方锐 . 物联网环境下计算机网络安全技术影响因素及防范措施 [J]. 电子测试 ,2021,(20):57-59.

[3] 赵宏凯 . 物联网计算机网络安全与远程控制技术分析 [J]. 中国新通信 ,2021,23(13):5-6.

[4] 张蒙恩 , 郭萌萌 . 基于物联网的计算机网络安全分析 [J]. 电脑知识与技术 ,2021,17(07):34-35.

[5] 张莉 . 基于物联网技术的计算机网络安全问题及应对策略研究 [J]. 信息与电脑 (理论版),2020,32(13):203-204.

[6] 刘锋 . 物联网环境下对计算机网络安全的分析 [J]. 农家参谋 ,2020,(16):257.