基于物联网技术的网络安全相关问题与应对策略

冯理明
（惠州城市职业学院，广东 惠州 516025）

摘要：随着我国计算机网络技术不断发展，它在很多领域得到了极为充分的应用，给人们的生活、生产提供了极大便利。但是，随着计算机网络技术使用场景的增加，很多安全问题也随之出现，若想保证网络系统的稳定运行，我们应重视对物联网技术的引入与优化，以此不断提升网络安全水平。鉴于此，本文将针对基于物联网技术的网络安全相关问题展开分析，并提出一些策略，仅供各位同仁参考。

关键词：物联网技术；网络安全；问题；策略

新时期以来，我国网络技术得到了进一步发展，实现了很多技术上的新突破，为各个行业的创新与发展提供了新的助力，这些行业也在网络技术的影响下得到了进一步发展。但是，在实际应用中，网络技术仍存在一些问题尚未解决，在物联网技术的支持下，网络数据流失逐渐成为影响网络安全问题的关键因素，为此，我们要不但提升基于物联网技术的网络安全水平，为社会发展提供助力。

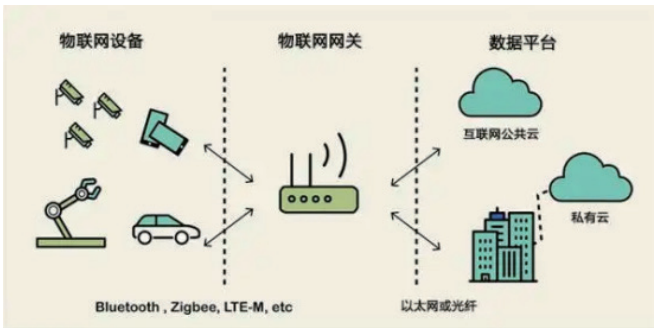
一、物联网技术概述分析

所谓的物联网技术通常是指以互联网技术为载体，以万物互联为目标的一种网络技术手段，其本质上可以看成是对互联网的进一步延伸和发函。物联网技术为很多行业应用互联网提供了一条新的道路，这对提升各产业的信息化综合水平有重要促进作用。

从技术层面分析，物联网技术主要可以分为如下三个层面，他们分别是网络层面、感知层和应用层。网络层主要是借助互联网、移动通讯网等技术，将各个设备连接起来，实现物品与网络的互联，在这一层级上，主要涉及承载网、专网等内容，为提升物联网使用效果，我们应强化网络架构涉及，这样方可更为高效地实现不同网络的融合。

在感知层，主要是对各类数据展开采集、处理。在采集数据的过程中，物联网能够借助各类传感器、射频技术、条形码、二维码等展开设备数据信息的采集，在对这些数据展开传输时，主要用到了高速短距离传输技术、协网信息处理技术、自组织组网技术等，这样能够实现物联网技术的信息高效处理。

从应用层上分析，当前物联网技术的应用范围得到了很大拓展，在智能电力、环境检测、智能交通、工业检测等方面都发挥了非常大的作用。物理网技术若想实现各类功能，需要很多公共支撑技术作为辅助，主要包括网络管理技术、标识解析技术、信息安全技术等。从这里我们可以看出，物理网技术有非常强的综合性特点。



二、基于物理网的网络安全相关问题分析

（一）通信安全问题

在处理物理网的大量信息时，很可能会出现端口超载的情况，若是这一问题未能得到有效解决，将可能出现严重的安全问题。

1. 网络系统运行不顺畅

物联网系统若想顺畅运行，需要诸多方面的共同支持。但是，在实际工作中，认证分析技术难以准确控制每个设备的工作状态。在这样的情况下，若想实现设备与互联网系统的有效连接，让物理网系统顺畅运行极为困难。

2. 秘钥管理方式不合理

一般来说，各类信息若想进入系统内部，需要经过一个网络通信端口，在此期间，这些信息需要经过系统认证方可实现信息加密管理。但是，在这个过程中，一些第三方的物联网设备计入，会严重影响网络安全水平，导致管理过程出现问题，还会在无形中造成大量资源浪费。

（二）安全隐私问题

一般来说，物联网技术以红外感知技术、射频识别技术和 GPS 定位技术等为主要载体，以此实现对各类数据资源的采集、分析、利用，从而完成对各类终端设备的实时监控。这些技术若是未能得到有效管理，各类信息资源很可能成为公开、透明的状态，这就导致人们很难实现对信息的控制与管理，在实践中出现信息流失的情况，不利于网络安全水平提升。

（三）传输安全问题

在物联网的感知层，有很多种方法都可以实现数据的传输。但是，在实际应用中，每个传感器的节点容量是不同的，这些都会在很大程度上影响物联网的数据传输稳定性，还会增加数据传输过程中信息被损坏的概率，从而为整个网络安全体系带来隐患。若是不能对感知层的数据展开有效处理，很可能会导致数据处理错误，从而影响到整个物联网系统的安全性。

（四）虚假攻击问题

互联网背景下的智能终端设备和以往的普通网络设备在信息透明度、完整性上有很大区别，这样就很容易导致不法分子对网络数据进行攻击，这些数据还会被某些运营商利用，这样也会大幅影响物联网传感器节点运行的稳定性。

三、基于物联网技术的网络安全应对策略

（一）密钥管理技术

在物联网的安全预防措施中，加密算法是较为常见的一种有效方式，它能应用到信息交换的过程中，对维护网络安全有重要价值。一般来说，加密算法可以分为两个类型，对称加密和非对称加密。加密对称一般也被叫作公共秘钥数据库加密，它是指信息的发送者和接收信息的人都可以使用相同的秘钥对信息展开加密、解密处理，其优点是对数据进行加密、解密时速度较快，同时，这种秘钥形式能够对信息内容较多的数据库进行加密，其缺点在于，秘钥的管理较为困难。若是通信双方能够保证在交换秘钥的过程中，公共秘钥不会泄露，则可保证信息数据的相对安全。非

对称秘钥一般被叫作公钥数据库加密。一对秘钥可以用于加密数据，还可用在解密每个数据消息上。其中一个秘钥会被宣布出来，另一个则会被用户存储在自己手中。在交换信息的过程中，出价方可以将信息转化成秘钥，而后将这一秘钥进行公开，而后向其他交易方宣布。

（二）VPN 技术

1.VPN 技术

VPN 技术是一种基于公共非安全介质而创设的专用链接技术。借助 VPN 技术，能够让一些私密信息在公共环境中展开安全传输。通过将 VPN 技术应用到物联网中，能够大幅提升信息传输的安全性，它能够让数据在网络中更为可靠地传递。此外，结合 VPN 技术，我们还可创设一个安全连接通道，将不同的用户、机构、合作伙伴联系起来，从而实现对物联网的进一步拓展。

（1）借助 VPN 技术，可以让物联网变得更为安全，大幅提升它的安全系数，促使其稳定性和管理稳定性提升到一个新的高度。

（2）可以实现对网络结构的进一步拓展，让办公室和内部网有效连接，可以实现远程操作。

（3）可以连接 LOT 技术伙伴，为用户和分销商创设一个信息安全通道，从而进一步降低企业运营成本，提升用户满意度。

VPN 实现方法：

（4）硬件配置机器和设备：服务器防火墙，具有 VPN 程序模块的无线路由器，专用的 VPN 硬件配置机器和设备，例如 Cisco，Netyu Nebula，H3C，Tianrongxin 等。

（5）实现软件：Windows 内置的 PPTP 或 L2TP，第三方软件（如 CheckPoint，Wangyu Nebula 等）。

（6）服务提供商（ISP）：中国电信、中国联通、网通等。现阶段，一些 ISP 发布了 MPLS VPN，路由质量更加有保证，建议应用。

2. 入侵检测技术

入侵检测技术是指，结合计算机系统的安全日志、相关数据后者其他网络信息，对现有的系统展开虚拟入侵的尝试。入侵防御系统能够极大提升计算机的网络安全水平。一般来说，入侵检测技术能够对系统报告中的异常数据展开审核，对于一些未授权的行为，也会进行重点关注，它是一种避免出现网络安全问题的高水平技术手段。计算机的系统配置和入侵检测系统软件一同构成了计算机的入侵检测系统，它又被称为 IDS。为了保证物联网中，数据信息能够安全、有效传递，避免各类外界因素对信息安全造成影响，入侵检测系统需要对物理网上传递的而信息展开有效检测，保证其合法性、安全性。信息系统的主要构成部分是信息技术，它也是保证网络安全的重要基础。入侵检测技术通过对物联网上的信息展开检测，能够及时发现可以信息，帮助安全人员快速发现潜在问题，能够助力其将这些问题消弭于无形。通过搜集相应的攻击节点、外部入侵数据等信息，网络安全人员可以对相应的入侵行为展开及时应对。首先，入侵检测系统会利用传感器搜集相应的数据信息，而后将相应的信息传递给 A 盒，A 盒会结合现有的数据资料，对于传过来的信息展开检测，并对相应的内容展开分析。在分析完数据后，对于有问题的数据会进行隔离，没有问题的数据则可以通过。从这里我们可以看出，若想提升物联网下网络安全水平，入侵检测技术的应用有非常重要的作用。

（三）优化网络安全风险数据库

若想让网络安全有所发展，需要建立更加科学、有效的网络风险数据库。一般来说，网络风险数据库中存储的信息能够为网络风险评估提供重要的评测基础，若是未能建立完善的网络安全风险数据库，评测结果将在很大程度上丧失实际意义。在进行网络安全风险评估时，以往的评估数据也会产生一定作用。但是，很少有人会对这部分数据提起重视，未能建立一个正规的数据库来存储、分析和整理相应的数据内容，这样进行的网络风险评估将存在较大的失真性。因此，风险评测人员要进行数据库优化时，可以采用 B/S 三层模式建立。这个数据库可以从浏览器、应用服务器、网页服务器以及数据服务器四个方面进行数据收集，这样可在最大程度上实现数据共享，确保网络安全风险评估数据库具有较强的可拓展性，也能在很大程度上增加数据库内容的灵活性。

（四）建立网络安全风险评估模块

通过全面优化网络安全风险评估数据库，可为之后更有效地发展网络安全打下坚实的基础，这离不开建立更加有效的网络安全风险评估模块。通过对数据库内的信息进行取样，危险评估模块可以调用系统内专业的风险评测系统对相应数据进行解读，而后将得出的信息与 IDS 系统的历史入侵数据库进行比对，从而分析出那些具有较高危险性的数据内容，最后得出网络安全风险评估结果。评估人员可以将评估结果与之前遭受攻击的记录进行比对，而后结合自身经验、专业技术等，对未来可能发生的不法攻击进行合理规避。风险评估模块的内层系统设置了一些定量、定性的评估方法，它会对网络运营服务器、LAN、网络主系统中心以及网络主机进行全面的风险评估分析，最终将评估结果以数据报表的形式直观地呈现出来。

（五）发展网络云安全检测技术

云安全检测技术作为物联网下最具代表性的数据技术，能在很大程度上助力网络安全的发展。所谓云安全检测技术通常是指借助云计算，将网络安全风险数据库中的信息进行处理，并对相应结果进行综合分析，找到潜在的安全隐患。此外，通过云安全检测技术，能切实提升网络安全风险评估系统对未知病毒的检测效率。在物联网下，云安全检测技术能够对网络安全风险评估系统所涉及到的每个节点进行监察，发现异常行为后可对其进行较为及时、准确地处理。在以往的网络安全数据分析中，人们通常只能分析一个测算标准，但云安全检测技术能对病毒、恶意网络软件的数据进行一定程度拆解，这在很大程度上降低了网络安全风险的威胁性，突出了云安全检测技术在网络安全风险评估技术中的重要意义。

四、利用物联网实现网络安全的成功案例

在我国，浦东机场是最为繁忙的机场之一，为保证飞行安全，飞行区内通常会依靠人工巡逻、物理围栏等方式展开安全防护工作。为此，中科院上海微系统和上海机场集团展开了深入合作，结合传感器技术等手段，创设了一个防入侵系统，实现了机场周边防卫的突破性进展。在机场内的地面、栅栏等地，设置了多个监测点，并利用传感器检测人员偷渡、恶意攻击等情况，大幅提升了网络安全技术水平。传感器网络技术有非常强的抗干扰能力，能够满足全天候的监测需要，这对提升机场安全水平意义重大。

参考文献：

[1] 黄铖生 . 物联网技术下的网络安全问题与应对方案分析 [J]. 计算机产品与流通，2020（06）：40.

[2] 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.

[3] 梁龙春 . 探究物联网技术的网络安全问题及应对策略 [J]. 大众标准化，2020（02）：118+120.