物联网计算机网络安全与控制策略分析

张智毓

河北大学附属医院

[摘　要]近年来，随着我国社会的不断发展，互联网技术在国民生产和生活中得到了广泛的应用。物联网计算机作为辅助互联网技术应用的关键设备，在实际运行过程中可能会存在网络安全问题，威胁客户的经济权益和个人信息安全。为了提高物联网计算机设备使用的安全性，必须要针对其安全问题采取合理的控制措施，进而保证我国物联网计算机网络能够为国民生产生活提供更多帮助。基于此，本文通过对物联网进行分析，探究在物联网计算机网络运行过程中存在的安全问题以及相应的解决措施。

[关键词]物联网；计算机；网络安全；控制策略

【DOI】10.12252/j.issn.2096-627X.2020.02.1874

引言：

在科学技术不断发展的背景下，互联网技术产生了越来越多的分支，并且在人们日常生产生活中得到广泛应用。在国家发展建设的过程中应用互联网技术，可以加快建设进程；在人们日常生活中应用互联网技术，可以阅览丰富的网络资源，满足精神需求，因此，现阶段互联网技术已实现在我国的全面覆盖。而物联网作为互联网的重要组成部分，其技术水平越来越高，并且在日常生活中也得到了广泛的应用，但是物联网安全问题是当前一直影响互联网使用效率的重要因素，一旦发生个人信息泄露，不仅会侵犯个人隐私，还会影响国民的权益，所以保证网络安全，是当前网络维护人员的重要责任和义务。同时，物联网技术的研发人员也应该在保障相关技术稳定运行的前提下，提高网络安全性能。

一、物联网技术分析

随着互联网技术的不断渗透，物联网技术的应用越发广泛，物联网技术是在互联网技术的基础上发展而来的，可以与人们生产生活中的实际物体相连的系统应用技术。利用物联网技术，既可以保证互联网中的相关信息能够应用在实际生产设备上，又可以将生产设备与网络进行连接，提升生产设备的生产效率。同时物联网技术也使用了全球定位技术、红外线传感器技术以及无线射频识别技术等，将这些技术与互联网技术进行有机融合，可以提高物联网技术的使用效率。

当前我国常用的物联网系统主要包含信息感知系统、信息传输系统、信息处理系统，以及信息控制系统等，通过各系统进行有机结合，不仅能够使物联网系统的运行规模急剧扩大，还能够提高其运行质量，在信息感知层中，可以利用智能技术和传感器技术对相关信息进行获取，然后将获取到的信息通过相关设备，传输给信息处理层和控制层中，进而实现信息使用价值的提升。物联网技术处理层的主要目的是对于大规模的数据能够完成高效的处理，并且利用智能计算系统提高数据处理效率，而数据的应用层和控制层的主要作用是能够将信息进行合理的分配和使用，进而保证信息的使用效率和使用价值均能够得到提升，同时在信息控制层方面，还能够根据用户的不同需求提供针对性的服务，进而使物体和人类需求之间能够互通，提高物联网技术的应用价值。

二、物联网计算机存在的网络安全问题分析

（一）通信安全问题分析

当前在物联网计算机系统应用的过程中，存在很多网络安全问题，影响其使用的安全性和可靠性，所以为了保障个人隐私不被侵犯，必须要在信息通信的过程中对其进行相应的控制，并且采取合理的控制措施，提高物联网计算机设备使用的安全性。当前在物联网计算机技术应用的过程中，存在的通信安全问题主要体现在以下几个方面，第1个方面是目前在互联网技术应用的过程中，可能由于使用的用户规模相对较大，造成网络出现拥堵的现象，由于物联网设备会和大量的网络线路相连接，因此导致网络系统的规模急剧扩大，而物联网设备如果没有进行更新或者扩容，可能会导致其信息处理效率与庞大的网络系统之间出现不匹配的问题。而工作人员在针对关联性进行解决的过程中，可能会出现通信安全问题。

第2个方面是目前在物联网计算机系统使用的过程中，一般都会使用密钥技术。利用密钥，既能够提高相关信息的隐秘性，又能够发挥互联网设备终端的作用，但是在物联网技术应用的过程中，对其认证环节没有进行科学合理的管理，导致在设备和个人进行连接的过程中，密钥信息泄露或者出现资源浪费的问题。

第3个方面是在通信过程中，如果传输的信息没有采取合理的防护措施，可能会导致个人隐私出现泄漏现象。物联网环境越来越复杂，在其处理数据的过程中，可能会将数据直接暴露在复杂的网络环境中，因此在一些黑客或者不法分子的眼中，暴露的信息则会使其有机可乘，进而导致个人隐私受到侵害。网络攻击行为一般会针对互联网设备的端口进行入侵，而如果物联网计算机设备的安全性能相对较低，极有可能对用户的重要信息及隐私信息等造成威胁。同时还有一些技术水平相对较高的黑客，会通过小程序作为相应的跳板，对网络中的相关信息进行恶意攻击。此行为不仅会影响物联网计算机的应用效率，还会对用户的网络使用效率造成影响。通信安全问题是当前物联网计算机存在的主要网络安全问题，在通信过程中，因为需要对个人隐私信息以及重要的计算机信息等进行传输，所以在传输过程中难免会出现黑客攻击现象，进而导致信息保护的安全性较低。

（二）信息感知层方面存在的安全风险因素分析

在物联网技术应用的过程中，感知层是容易出现安全风险的主要环节，其主要包含以下几个方面。第1个方面是安全隐私存在的问题。当前为了提高物联网技术应用水平，研发人员针对物联网的感知层设置了很多智能感知系统，利用这些智能感知系统，可以快速准确地获取相关信息，同时也能够对相关信息完成自动处理过程。但是在此过程中虽然有助于工作人员提升工作效率，但是对一些不法分子来说，可能会因为信息的暴露，而使个人隐私受到威胁。例如在物流行业中，物流工作人员可以通过扫描物品上的条形码，对相关物品进行定位，进而可以为用户提供物品的具体位置，这些信息在扫描的过程中会经过信息感知层和信息传输层，通过以上分析可以明确在信息传输的过程中可能会出现暴露问

题，而在信息感知层也经常会出现信息被公开的问题。在物流系统应用的过程中，相关标签对任何问答均会给予满足，由于不会自主甄别信息获取用户，因此可能会导致物品中的个人隐私被跟踪或定位。

第2个方面是可能会存在信号干扰的问题。当前物联网技术在应用的过程中，感知层起到了非常重要的作用，利用感知层可以获取物联网技术需要处理的相关信息。目前随着物联网技术水平的不断提高，在信息获取的过程中，已由传统的有线连接方式转变为无线连接方式，而无线连接方式增加了信息的共享性能和公开性能，因此导致信号在传输和感知的过程中，经常会受到外界网络的影响，降低了其传输的效率。同时在外界网络信号的干扰作用下，还可能会导致感知层获取的信息有误，进而影响其正常通信功能。信息干扰现象是当前在物联网技术应用过程中的主要问题，降低物联网信息之间的干扰因素，能够使通信效果得到显著提升，进而能够解决信息传输不准确的问题。

第3个方面是在智能感知的过程中也会存在一定的安全隐患，由于物联网系统包含的设备相对较多，很多设备均会处于无人监控的状态下进行自主运行，而在此工作状态的下，可能会导致很多不法分子通过相关技术手段获取监控信息内容。同时在设备运行过程中，一般会将其进行分散化的处理，在不同的地理位置均包含物联网系统中的通信设备，因此在针对其进行管理的过程中，无法实现集中性管理，导致很多网络攻击对象能够轻松地获取相应的秘密信息。同时也可能会对信息造成破坏。被破坏和篡改后的信息在传输到通信网络上，会形成伪造数据程序，进而导致出现严重的后果。在智能传感设备应用的过程中，由于其端口具有一定的开放性，可能会出现假冒攻击的问题，一些黑客在针对开放的端口进行操作的过程中，可能会将不良程序植入其中，进而导致物联网内部的信息传输受到影响。一旦传输的信号错误，对传感器的正常运行会造成严重的威胁，进而导致整个物联网系统的协调性能和系统性遭到破坏。

三、物联网计算机网络安全控制措施分析

（一）建立完善的加密机制

目前针对物联网计算机在运行过程中存在的网络不安全问题，必须要采取合理的控制措施，当前很多技术人员会选择利用加密机制提高网络信息的隐秘性。在加密的过程中，其主要方式分为端口对端口的加密以及逐条加密。使用逐条加密的方式，能够保证针对需要传输的信息进行全程加密，进而提高其加密的准确性，但是使用这种加密方法所需要的加密时间相对较长，并且因为在后期解密的过程中需要对应大量的密钥，所以可能会导致信息使用效率下降。在针对不同节点进行加密的过程中，也可能会导致信息的暴露危险增加，所以逐条加密的方式一般无法在用户信息传输过程中使用。在网络层中逐条加密方式得到了广泛的应用，因为逐条加密方式对网络层中的信息具有较强的适用性，所以能够根据公司在业务处理过程中的不同类型，选择合理的加密方式，进而提高其安全性能。与个人信息相比，企业中的机密信息则显得更为重要，所以即使在加密的过程中，信息使用效率下降，也应该使用先进的加密技术，提高信息的安全性能和隐蔽性能。目前逐条加密方式能够使用链接保护的措施，所以可以应用于提高企业信息保护效率的过程中。

而端口对端口的加密方式与逐条加密方式相比，虽然其保密性能相对较差，但是在实际应用过程中，因为操作相对简单，所以在传出一些普通信息时，可以使用端口对端口的加密方式，只需要一次解密密码，即可以完成相关信息的查阅和传输。与逐条加密的方式相比，端口对端口的加密方式受到危险攻击的可能性更大，因此在进行加密的过程中，必须要提高密码等级，尽量选择具有大小写以及数字和标点符号的密码组成结构。同时端口对端口的加密方式还无法针对信息的目的地进行相应的加密，因此也可能对收件者的个人信息造成泄露问题。如果有人进行恶意攻击，可能会使相关信息以及收件人地址的个人隐私暴露。在选择不同加密方式的过程中，用户应该根据自己的实际需求进行合理的选择，如果要提高信息的使用效率，并且信息的保密性要求相对较低，则可以使用端对端加密方式，而如果信息保密性要求相对较高，则应该使用逐条加密方式。

（二）签订安全网络通信协议

当前物联网技术主要包含感知网络与通信网络两部分，物联网通信需要使用路由器，并且要针对不同类型的网络结构匹配相应的IP地址。当前物联网路由器IP地址在使用的过程中需要签署相应的路由协议，因此路由协议成了保护IP地址隐秘性的重要措施。所以可以通过签订安全网络通信协议，提高IP地址的安全性能，并且要保证互联网信息在传输的过程中针对其不同节点签订不同的安全网络通信协议，利用各节点的多变性不断改变数据传输路径使黑客无法获取节点的准确信息。利用无线传感器签订的安全路由协议，能够使信息传输过程受到法律保护，但是这种方法也存在一定的缺陷，例如在组网状态下，安全路由协议起不到保护作用，所以还应该配合使用密钥机制，提高路由器的安全运行效率。

（三）防火墙技术的应用

目前在物联网系统运行的过程中，防火墙技术得到了广泛的应用，打造网络信息的安全防火墙，是当前在计算机设备和互联网技术应用过程中的常见方法，利用防火墙技术可以对相关信息进行保护，并且在黑客入侵的过程中也可以进行抵挡。防火墙技术还具有一定的提醒功能，当计算机设备检测到入侵信息时，防火墙则会弹出异常信号进而给工作人员提醒。但是这种常规的方法仍然存在一定的漏洞，还需要对终端设备进行全方面检测，保证能够使防火墙技术实现实时监测和防护功能。

结束语：

综上所述，现阶段我国物联网计算机网络安全问题较为严重，不仅影响了互联网技术水平的提升，还暴露了国民的个人隐私，所以必须要利用防火墙技术、签订安全路由协议、建立加密机制等，提高网络安全性能。

参考文献：

[1]代婉秋.物联网计算机网络安全及控制的研究[J].数码世界,2019,(12):274.

[2]潘山.物联网计算机网络安全及控制[J].计算机产品与流通,2019,(11):56.

[3]田明亮.物联网计算机网络安全与控制的探究[J].数码世界,2019,(11):256.