

集装箱码头无线网络环境下的 数据采集方法

刘 聪 徐 家

蛇口集装箱码头有限公司

摘 要: 阐述了集装箱码头 RCMS(remote crane monitoring system, 起重机远程监控系统) 系统在无线网络环境下数据采集所面临的问题, 并从集装箱码头网络安全及系统数据采集功能实现的角度出发, 有针对性地制定了一套服务器平台及起重机本地平台数据通讯方案, 以确保系统数据采集的安全高效。

关键词: 无线网络; RCMS; 数据采集

Data Acquisition Method based on Container Terminal Wireless Network Environment

Liu Cong Xu Jia

Shekou Container Terminals Ltd.

Abstract: This paper describes and analyses the problems of data acquisition of the remote crane monitoring system under the wireless network situation. And to develop a set of data communication solutions of the servers platform and the crane platforms, the solutions are developed from the aspects of the container terminal network safety and the implementation of the data acquisition, and it is targeted to ensure the safe and efficient operation of the data acquisition.

Key words: wireless network; remote crane monitoring system; data acquisition

1 引言

随着经济全球化和世界贸易总量的高速增长, 越来越多的货物运输依赖集装箱方式进行, 港口的吞吐总量高速增长的同时, 港口的大型设备及设施数量也越来越多, 港口企业面临着作业由劳动密集型向技术密集型转变、管理由粗放型向集约型转变的趋势^[1]。

为了适应发展趋势, 在保障高效生产的同时提升集装箱码头设备管理水平, 码头企业陆续引进了 RCMS 系统, 以实现起重机设备状态的远程实时管理。RCMS 系统通常采用无线网络的方式进行起重机设备状态数据的采集, 以满足集装箱码头内零散分布的起重机设备及流动作业机械的数据传输需求。但是, 由于无线网络带宽及稳定性限制, RCMS 系统的数据采集功能部署需综合考虑以下两方面因素:

(1) RCMS 系统的数据采集功能通常是基于 SCADA(supervisory control and data acquisition, 数据采集与监控) 等工业组态软件实现, 软硬件之间避

不可免的会采用广播方式进行通讯, 相应的广播信息如果不加以控制会造成无线网络的拥塞或者崩溃。

(2) 集装箱码头内的无线网络不仅需要承担 RCMS 系统数据的传输, 还需承担 CTOS(container terminal operation system, 集装箱码头操作系统) 等系统数据的传输, 因此数据采集功能的部署不仅需要符合企业网络安全的要求, 还需要尽量降低对企业整体网络资源的消耗, 以避免对网络内其它系统造成影响。

基于以上因素, 本文从集装箱码头网络安全角度出发, 以某集装箱码头部署的 GE Cimplicity 组态软件为例, 分析研究了在无线网络环境下 RCMS 系统数据采集所面临的问题及相应解决方案。

2 数据采集功能主体架构

本文所述的数据采集功能是 RCMS 系统的核心构成部分, 其网络架构包含服务器平台、企业交换网、无线网络及起重机本地平台, 见图 1。

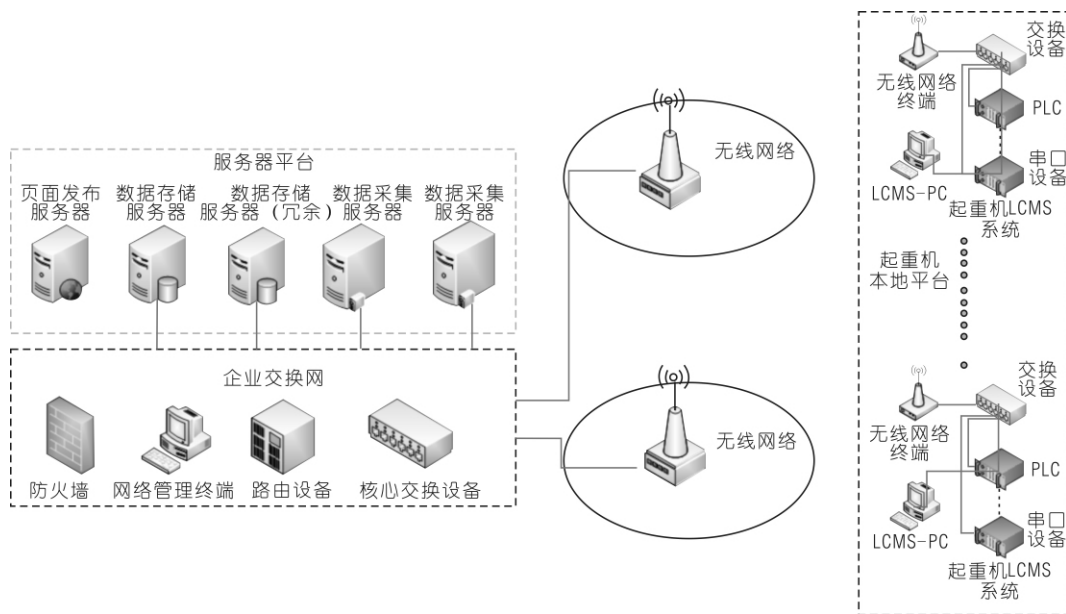


图1 数据采集功能架构图

服务器平台是数据采集系统的上位平台,该平台通过部署的 SCADA 软件实现起重机设备实时状态数据的采集、存储及监控页面发布,各项功能分别通过独立的数据采集服务器、数据存储服务器及页面发布服务器实现。

企业交换网是码头企业网络安全架构的一部分,也是数据采集系统需要遵从的网络安全要求。企业交换网通过部署安全策略将不同类型、不同重要程度的数据限定于特定的网段内进行数据交互,以避免不同数据之间的干扰。本实例中的企业交换网将数据采集系统划分至 2 个不同的网段,其中数据采集服务器及起重机本地平台运行于生产网网段,数据存储服务器及页面发布服务器运行于办公网网段。

起重机本地平台是数据采集系统的下位平台,也是数据采集系统的数据源。该平台通过搭建起重机本地通讯链路并配置网络通讯接口设备,实现操作指令数据、PLC 控制数据、串口通讯数据及起重机 LCMS(local crane monitoring system) 系统等数据的传输。

以上网络架构是基于企业整体网络规划的基础上进行的应用部署,架构内数据的传输不仅需要符合企业网络安全的要求,还需要尽量降低对企业整体网络资源的消耗。但是,在实际应用部署过程中会存在以下两方面的问题:

(1) 服务器平台运行的数据采集服务器需要周期性的通过 UDP(User datagram protocol, 用户数据报协议) 广播包的方式与数据存储服务器及页面发布服务器进行通讯,以实现服务器上各 SCADA 软

件工程的访问。但是由于数据采集服务器位于生产网网段内,广播包在无线网络内传输可能会导致网络拥塞,影响无线网络内各应用程序平台的正常使用。

(2) 起重机本地平台需接入无线网络内的控制设备数量多、数据类型复杂,如将各控制设备直接接入无线网络不仅会大量增加 IP 地址等网络资源的消耗,而且会形成大量 ARP(address resolution protocol, 地址解析协议) 广播包,导致无线网络拥塞。

针对以上问题,本文从数据采集功能主体架构出发,有针对性地制定一套服务器平台及起重机本地平台数据通讯方案,以确保数据采集功能的安全高效运行。

3 服务器平台通讯方案

服务器平台包含数据采集服务器、数据存储服务器及页面发布服务器,其中数据采集服务器通常采用热备冗余设计,正常情况下由主服务器负责数据采集,冗余服务器处于热备状态并保持与主服务器的实时通讯,一旦主服务器出现异常,冗余服务器会自动切换投用,以确保数据采集的连续性。

在不考虑无线网络影响的情况下,服务器平台的工作原理如下:数据采集服务器通过 UDP 广播的方式周期向各连接终端广播服务器上运行的 SCADA 软件工程名,数据存储服务器及页面发布服务器根据接收的广播信息在主数据采集服务器发生故障时进行切换,起重机本地平台上的通讯终端通过 TCP/IP 协议与数据采集服务器进行数据交换。

由于数据采集服务器与起重机本地平台上的通

讯终端均在无线网络内,UDP 广播包会传输至无线网络并内导致网络拥塞,影响网络内各应用程序的正常使用。为了保障无线网络的安全,需要对无线网络内的 UDP 广播包进行拦截。该类型广播包的拦截可以通过服务器平台外部增设路由器或服务器网络架构优化 2 种方式实现。

3.1 基于路由器的广播包拦截

路由器作为网络通讯的重要节点设备之一,不仅可以实现不同网络之间的数据转发,还可配置实现 UDP 广播数据的拦截。结合路由器设备的特点,可以采用图 2 的方式实现特定网段内的数据转发及广播包的拦截,其工作原理如下:

(1) 建立服务器局域网,将服务器平台内的各服务器置于同一网段内,确保服务器之间的通讯及 UDP 广播数据正常传输。

(2) 服务器局域网与生产网及办公网之间增设路由器。数据采集服务器通过路由器的转发功能进行起重机本地平台数据的采集,同时,借助路由器的 UDP 广播包拦截功能杜绝服务器局域网内的广播包数据进入无线网络;办公网内用户通过路由器转发功能实现跨网段访问页面发布服务器。

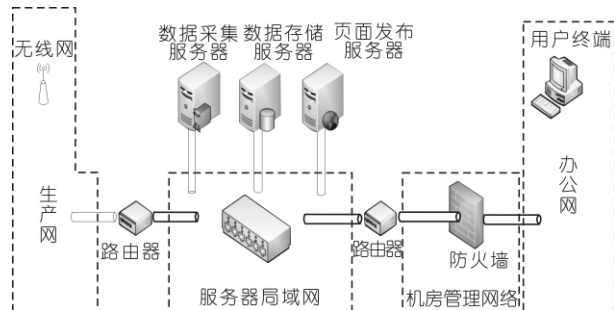


图 2 基于路由器的广播包拦截方式

该方案虽然可以有效杜绝广播包数据进入无线网络,但是由于路由器处于 OSI(open system inter-connect,开放式系统互联) 参考模型的网络层,其数据转发过程不是简单的数据交换,期间还要进行数据过滤、数据包压缩、协议转换、路由表维护、路由计算以及防火墙防护等繁杂作业,这些作业一方面会大量消耗路由器的 CPU 资源,导致路由器传输效率低,吞吐能力受限,甚至成为网络瓶颈,另一方面符合需求的路由器设备价格昂贵,管理复杂^[2]。

3.2 基于服务器双网卡的广播包拦截

利用服务器的双网卡配置来实现广播包的拦截,将同一服务器的不同网卡置于不同网络以实现数据传输的同时,隔离广播包信息,其实现方式如图 3。该方式的工作原理如下:

(1) 将数据采集服务器的 1 个网口、数据存储

服务器的 1 个网口以及页面服务器的 1 个网口(使用服务器的双网卡功能) 组成服务器局域网,确保服务器之间的通讯及 UDP 广播数据正常传输。

(2) 数据采集服务器的网口 1 置于无线网络网段内(生产网),通过无线网络采集起重机本地平台数据;数据采集服务器的网口 2 接入服务器局域网,利用此接口为数据存储服务器及页面发布服务器提供数据连接服务。

(3) 页面发布服务器的网口 1 置于服务器局域网内,接收数据采集服务器的广播包数据,以满足服务器冗余通信及工程访问的需求;网口 2 通过机房管理网络及防火墙接入到办公网,供用户计算机访问。

(4) 配置数据采集服务器的“路由和远程访问”选项,禁止服务器网口 1 的 UDP 发送功能,使广播包只能通过网口 2 发出。

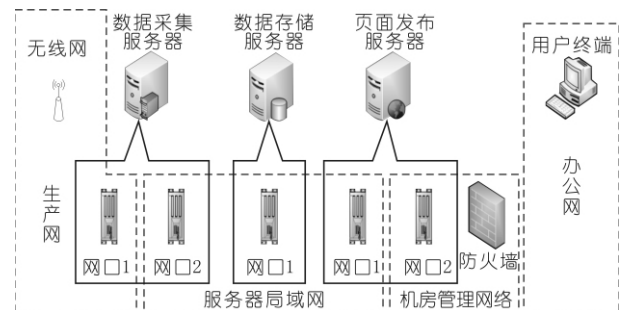


图 3 基于服务器双网卡的广播包拦截方式

该方案采用服务器的 2 个网卡分别实现生产网起重机本地平台数据的采集和广播包数据在服务器局域网内的传输。网卡处于 OSI 参考模型的数据链路层,其只需承担通讯链路上的数据分帧及连接控制,无需承担过多数据处理作业,因此其数据传输效率相对较高。

4 起重机本地平台通讯方案

起重机本地平台为数据采集系统的核心数据源,其覆盖的设备包含 PLC 控制器、串口设备及 LC-MS 电脑设备等,各设备通过 TCP/IP 协议与数据采集服务器通讯。按常规局域网设备工作方式,起重机本地平台上的控制设备将通过定时发送 ARP 广播包的方式来更新各控制设备的 MAC 地址缓存,以建立数据采集服务器与起重机本地控制设备的连接,ARP 广播包会在网络内所有接入终端进行传输和接收应答,当接入设备数量过多时容易在局域网内造成广播风暴,导致网络拥塞^[3]。为了降低 ARP 广播包对无线网络的影响,需要严格控制无线网络投用的 IP 地址数量。在确保数据采集系统正

常工作的前提下,可以通过无线网络终端或路由器的 NAT(Network Address Translation, 网络地址转换) 功能实现 IP 地址的扩展。

4.1 基于无线网络终端 NAT 功能的 IP 地址扩展

利用无线网络终端 NAT 功能实现 IP 地址的扩展主要通过以下 2 个步骤:

(1) 通过工业交换机在起重机本地平台上组建小型局域网,分别接入 PLC、串口设备及 LCMS 电脑等,接入设备 IP 采用本地局域网地址。

(2) 配置无线网络终端(含无线网络接入终端、无线网络数据转发终端等)的 NAT 功能,实现针对交换机各接入设备的端口映射,将无线网络终端 IP 与交换机内接入设备的多个 IP 进行映射,实现 IP 地址的扩展,同时避免局域网内的 ARP 广播包传送到无线网络中。具体架构见图 4。

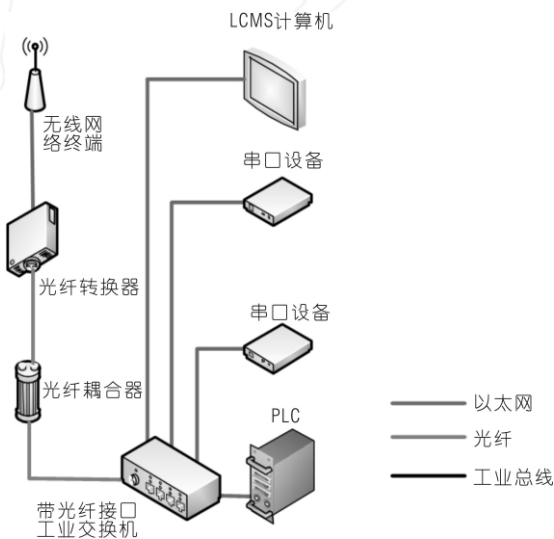


图4 基于无线网络终端的 IP 地址扩展架构

由于无线网络终端设备一般为 OSI 参考模型数据链路层接入设备,通常不具备 NAT 功能,因此该方案虽然在技术上可行,但是具体实施的可行性取决于无线终端设备的选型。

4.2 基于路由器 NAT 功能的 IP 地址扩展

路由器处于 OSI 参考模型的网络层,具有良好的 IP 分配、路由寻址及地址映射性能,因此可以通过在起重机本地平台部署路由器的方式实现 IP 地址的扩展。具体步骤如下:

(1) 通过路由器在起重机本地平台上组建小型局域网,路由器的局域网网口分别接入 PLC、串口设备及 LCMS 电脑等,接入设备 IP 采用本地局域网地址(如图 5 中的 192.168.0.x)。

(2) 路由器的广域网接口采用无线网络规划的 IP 地址(如图 5 中的 18.25.4.x),通过路由器的静态 NAT 功能将外网 IP 与局域网内各控制设备的 IP 地

址进行映射,实现 IP 地址的扩展,同时避免局域网内由 ARP 导致的广播包传送到无线网络中。

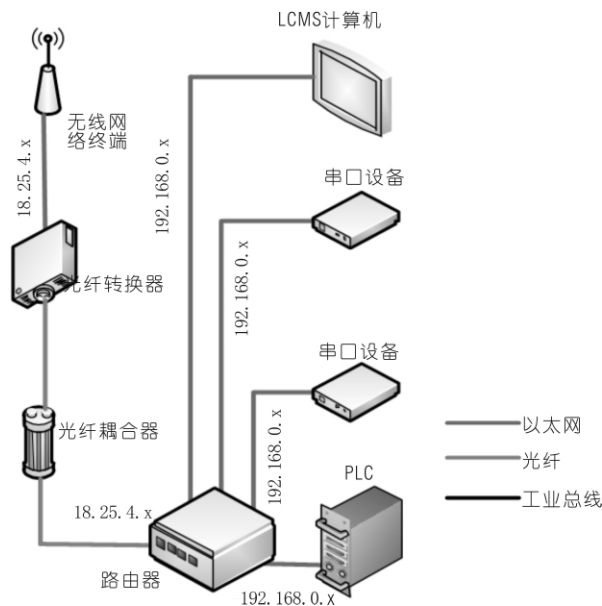


图5 基于路由器的 IP 地址扩展架构

本方案不仅可通过路由器的 NAT 功能实现起重机本地局域网内各控制设备的 IP 地址映射,还可通过路由器的管理功能实现起重机本地平台各控制设备数据的规范化管理及扩展管理。

5 结语

从集装箱码头网络安全角度出发,分析了在无线网络环境下 RCMS 系统数据采集所面临的广播包问题,并有针对性地提出了一套基于服务器平台及起重机本地平台数据通讯链路优化的解决方案。通过在某集装箱码头的实践经验来看,此方案切实可行。但是,由于不同集装箱码头之间网络规划及安全管理策略会存在差异,因此在类似项目实施过程中项目实施人员需结合实际要求进行调整,以实现 RCMS 系统的安全高效运行。

参考文献

- [1] 陈羽. 2015 年我国港口集装箱发展现状及趋势 [J]. 中国港口, 2016(4): 5-10.
- [2] 严雷, 胡华平, 简洁. 基于分层分析法的安全评估参数模型研究 [J]. 计算机工程与应用, 2006(25): 16-19.
- [3] 赵鹏. 计算机网络系统中基于 ARP 协议的攻击与保护 [J]. 网络安全技术与应用, 2005(1): 35-36.

刘聪: 518069, 深圳市蛇口港湾大道第三突堤

收稿日期: 2017-05-17

DOI: 10.3963/j.issn.1000-8969.2017.04.020