CDMA EVDO 动态 VPDN 技术在 EPOS 缴费平台中的应用

杨云峰,李 健
(中国电信陕西公司,陕西 西安 710075)

摘 要:CDMA 增强型数据业务采用虚拟专用拨号网技术,为用户提供基于高速分组数据网络之上的 VPN 数据专网,VPDN 为分支点建立连接到企业内部的私密隧道,即两层隧道协议。基于隧道可以实现企业内部数据安全,高速、便捷的传输;从而使企业用户在任何地点都能够通过 CDMA 网络无缝和安全的连接到企业内网,实现信息共享、交互和相关业务应用的处理,节省了用户的通信成本,提高了企业管理运作效率。文中着重阐述了 EVDO 动态 VPDN 相关技术原理,组网方式,并对其安全性进行了分析,其次介绍了 EPOS 交费平台的系统组成以及如何利用 CDMA EVDO 动态 VPDN 技术实现在 EPOS 交费平台进行交费、充值、售卡等事务处理,主要目的是解决农村信息化的问题。

关键词:增强型数据业务;虚拟专用拨号网;两层隧道协议
中图分类号:TP39 **文献标识码**:A **文章编号**:1673-629X(2012)01-0182-05

Application in EPOS Fee Platform with CDMA EVDO and Dynamic VPDN Technology

YANG Yun-feng, LI Jian
(China Telecom Shaanxi Branch, Xi'an 710075, China)

Abstract: CDMA EVDO business is used VPDN technology to provide users with the VPN data private network based on high-speed packet data network. VPDN for branch point to enterprise internal connection is established by tunnel technology. Based on the tunnel, it can realize enterprise internal data security, high-speed, convenient transmission; Thus the enterprise users in any place through the CDMA network seamlessly and safely connected to the enterprise internal network, realize the information sharing and interactive and related business application processing, save the user's communication cost and improve enterprise management operation efficiency. It expounds the dynamic EVDO VPDN related technical principle and networking methods and adopted the technical scheme and implementation process in engineering practice. The main purpose is to solve the problem of rural informatization service in telecom domains.

Key words: EVDO; VPDN; L2TP

0 引 言

随着互联网和电子商务的快速发展,中国市场信息化程度的提高,VPN 在国内发展日益迅猛,VPN 已不再是跨国大企业的专利,越来越多的企事业单位和中小企业选择了 VPN,中国已经到了 VPN 技术应用的高速增长期。并且商用 3G 网络的日益成熟,用户对于 3G 无线的应用需求也越来越强烈,因为 3G 网络给用户带来极大的便利性,同时又是对有线通信方式及提高网络可靠性的很好补充。而 CDMA EVDO 作为目前 3G 移动用户的 VPN 接入手段,正扮演着越来越重要的角色。

收稿日期:2011-05-27;**修回日期**:2011-09-04
基金项目:中国电信 EPOS 缴费系统工程示范项目(08J1CB0001SNYXZ)
作者简介:杨云峰(1979-),男,研究方向为 IT 系统规划与实施。

1 码分多址 EVDO 动态 VPDN 技术

CDMA EVDO 是一种针对分组数据业务进行优化的、高频谱利用率的 CDMA 无线通信技术,可在 1.25MHz 带宽内提供峰值速率达 3.1Mbps 的高速数据传输服务[1]。

基于码分多址的 EVDO 动态 VPDN 技术的优点体现在以下几点:

1)数据传送速度快、效率高:CDMA EVDO 的传输速率原理上为 3.1Mbit/s,而实际在应用时的速率基本在 2.6Mbit/s 左右,但这也远远高于传统的 DDN,固话拨号等传输速度[2]。

2)可靠、安全的数据传输:CDMA2000 EVDO 网络 VPDN 业务具有五层安全保障:

第一级安全保证:CDMA 网络本身的安全性;

第二级安全保证:CDMA 无线宽带接入 AAA 认证;

第三级安全保证:CDMA 网络和客户网络之间的 L2TP 隧道;

第四级安全保证:客户网络侧的安全防火墙;

第五级安全保证:LNS AAA 鉴权认证。

3)行业应用广泛:在银行、政府、税务等行业已经采用这种技术组建自己的 VPDN 网络,应用前景十分广阔。终端用户通过无线 VPDN 接入到客户网络,对各类应用均可透明传送。适用多种终端形式,包括智能终端、具有 CDMA 拨号功能的网络设备和工控设备等。

4)可移动、覆盖广:用户可以在移动的环境下进行无线数据传输,CDMA 独有的软切换技术使用户在高速移动中也能确保持续连接,真正地满足用户移动办公的需求。只要有 CDMA 信号的地方,用户就能使用 CDMA EVDO VPDN 业务。

1.1　组网元素介绍

(1)用户侧 VPDN 路由设备:简称 CPE,用户终端设备需要有路由和 VPDN 功能,置于客户机房本地,完成与上游的接入和路由选择以及通讯通道的建立。CPE 是 VPDN 呼叫发起和结束的地方,也是用户方需要设置的唯一 VPDN 硬件。

(2)网络接入服务器:简称 NAS,负责企业专网和外网的 VPN 对接,是实现 VPDN 接入的关键设备;该设备可兼容各种网络协议,支持隧道及其相关技术,具备安全管理和认证的功能。

(3)企业端认证服务器:用于用户一次认证,对认证通过的用户将其资料发送给相应的 LNS 设备的认证系统进行二次认证。

(4)用户终端:具备能使用 CDMA EVDO 上网的终端设备。

(5)认证服务器:主要对登录账号和信息传输进行 AAA 认证。

1.2　电信行业 VPDN 采用的隧道技术分析

目前隧道技术按照协议可划分为两类:第二层隧道协议和第三层隧道协议。

第二层隧道协议[3]:PPTP、L2F、L2TP。

第三层隧道协议:GRE、IPsec。

两种协议的根本区别在于穿透方式的不同,即第二层协议的穿透、第三层协议的穿透。

二层隧道协议 L2TP、二层转发协议 L2F、点到点隧道协议 PPTP 是三种主要的 VPDN 隧道协议。PPP 定义了一种封装技术,多种协议数据包可以在二层的 P2P 链路上传输,当 PPP 协议在用户与 NAS 之间运行时,在相同硬件设备上同时存在二层链路端点与 PPP 会话点。L2TP 是一种对 PPP 链路层数据报文进行隧道传输的技术,允许二层链路端点(LAC)和 PPP 会话点(LNS)驻留在通过分组交换网络连接的不同设备上,从而扩展了 PPP 模型,使得 PPP 会话可以跨越 IP 网络。

L2TP 结合了 L2F 和 PPTP 的各自优点,目前电信行业 VPDN 的隧道技术就是 L2TP。

其特点主要有下面几个方面[4]

(1)安全性高和身份验证机制灵活。

安全性的定义在 L2TP 协议本身并不存在,但 L2TP 却继承了 PPP 的所有安全特性,因为它是基于 PPP 提供的认证。数据安全的实现可以通过 L2TP 与 IPsec 相结合,数据通过 L2TP 传输更难被攻击。为了更进一步提高数据的安全性,可将端对端数据加密、隧道加密技术、以及应用层数据加密等技术运用于 L2TP 之上来实现[5]。

(2)多协议传输。

PPP 数据包通过 L2TP 传输,在 PPP 数据包内可以封装多种协议,L2TP 保证在任何 IP 网络上 IP、IPX 和其他协议包的安全性。

(3)支持 RADIUS 服务器的认证。

RADIUS 服务器对 LAC 和 LNS 发来的账号和密码进行验证,用户的验证请求通过 RADIUS 服务器完成。

(4)支持内部地址分配。

企业网的防火墙之后可以部署 LNS,远端用户的地址通过 LNS 进行动态的分配和管理,可支持私有地址应用。企业内部的私有地址被分配给远端用户,而不是 Internet 地址,这样方便了地址的管理并可以增加安全性。

(5)网络计费的灵活性。

计费信息可在 LAC 和 LNS 两处同时得到,帐单产生在 ISP 处,付费及审计在企业网关。出入包数、字节数以及连接的起始、结束时间等计费数据通过 L2TP 能够得到,网络计费根据这些数据可以方便地进行。

(6)可靠性。

L2TP 协议支持备份 LNS,LAC 与备份 LNS 在主 LNS 链路不可达或设备出现故障后建立连接, VPN 服务的可靠性和容错性得到增强[6]。

1.3　CDMA EVDO-VPDN 技术实现

VPDN 有两种实现方法:通过 NAS 与 VPDN 网关建立隧道;客户机与 VPN 网关直接建立隧道方式[7]。

(1)NAS 与 VPDN 网关建立隧道。

这种方式是 NAS 与 VPDN 网关建立通道是通过 Tunnel 协议进行的,企业网的网关上终结客户的 PPP 连接, L2F 和 L2TP 是比较常用的两种协议。

这种方式的优点:对用户是透明的,用户访问企业网的只发起一次登录,而整个过程的认证和内部地址分配都通过企业局域网内的安全设备管理,节约了公共地址;用户侧的上网接入平台多样化没有具体限制。但这种技术的实现是需要企业内部的 NAS 网络硬件必须支持 VPDN 协议。但缺点是安全性不高,一般多用于移动办公用户。适用的企业用户应大致有以下要求[8]:

A. 企业用户需要使用 CDMA EVDO 无线上网进行内部的工作事务处理;

B. 用户采用无线上网方式远程接入企业内网进行某些操作;

C. 安全性在于用户的网关本身,可以与互联网连接,当用户上网操作时,对数据安全性要求不高。

目前全国分组网 PDSN 均已支持此种方式,此方式较为成熟,相应的域名以及 LNS IP 地址等数据在分组网 AAA 进行设置。公网接入是比较成熟、快速部署、成本较低的一种方式,是运营商向一般 VPDN 客户推荐的首选接入方式。电信行业 EPOS 交费平台就采取这一种。

(2)隧道的建立实现了用户终端和 VPDN 网关的连接。

这种方式是首先用户采用宽带,光纤局域网等方式建立起与 Internet 的对接,然后用户则再通过专用的上网软件,使用 PPTP, IPSec 协议建立起与网关的通道[9]。

其优点在于:用户上网的方式地点随意,运营商不需要介入。缺点是需要在用户端主机上安装专用的系统平台软件;用户的认证过程需要两次,一次上运营商,一次接入私有企业网;但这种同时接入企业网和 Internet,会造成潜在的安全隐患。

1.4 VPDN 的安全技术

基于 Internet 的 VPDN 首先要考虑的就是安全问题[10]。能否保证 VPDN 的安全性,是 VPDN 网络能否实现的关键[6]。可以采用下列技术保证 VPDN 的安全:

- 口令保护;
- 用户认证技术;
- 一次性口令技术;
- 用户权限设置;
- 在传输中采用加密技术;
- 采用防火墙把用户网络中的对外服务器和对内服务器隔离开。

2 EPOS 交费平台简介

电信 EPOS 系统的组成。它主要包含 EPOS 支付电话终端、接入平台和具体应用前置机以及和计费中心相关的接口机等几部分。

EPOS 支付电话终端要求至少支持以下 3 种网络接入中的一种方式:

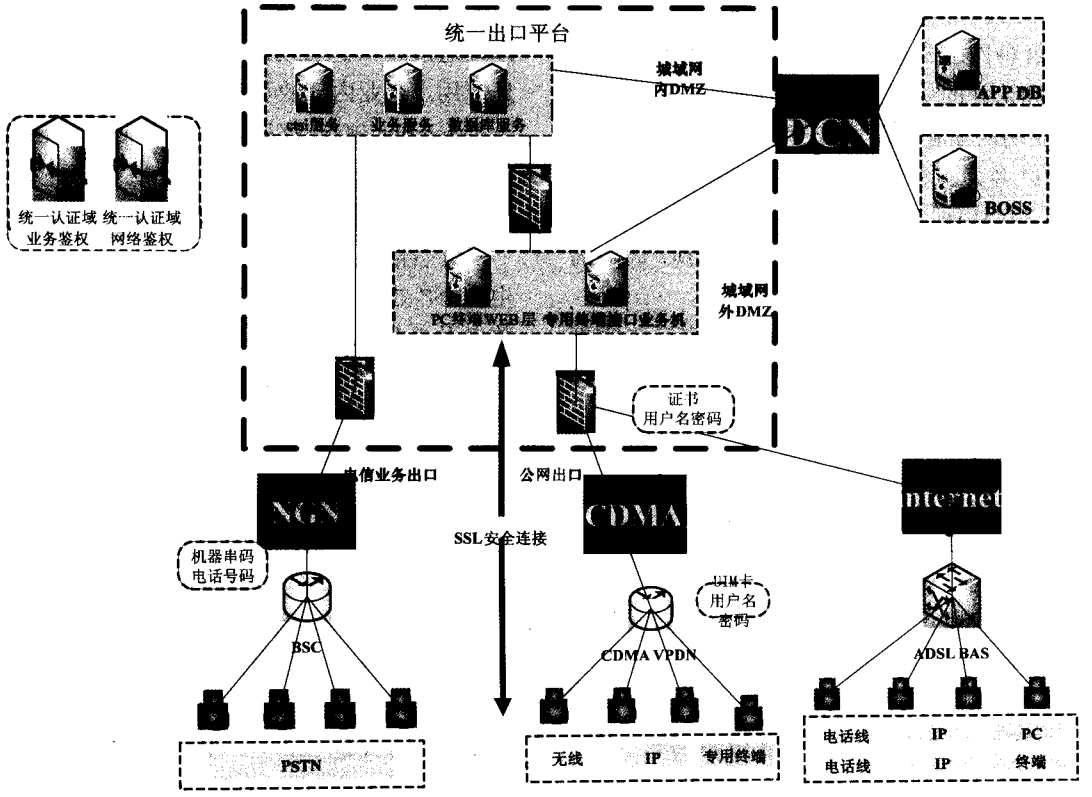

图 1 EPOS 交费平台物理结构

(1)具备 RJ11 电话线接入接口,并具备 PPPOE 拨号功能;

(2)具备 RJ45 标准网络接入接口;

(3)具备 CDMA1×或者 EVDO 的接入模块(可以插入 SIM 卡后通过无线接入网络)。

网络接入可以选择 NGN、CDMA、INTERNET,下面是三种方式比较:

(1)NGN:终端采取 FSK 调制方式,终端与系统之间信息交互协议标准为 CTSI 协议,速率低、误码高、交易处理时间长;

(2)CDMA:终端采取 EVDO 接入方式,速率高,误码低,交易处理时间短;

(3)INTERNET:终端采取 ADSL 接入方式,速率高、误码低、交易处理时间短。

后二者网络协议采取 TCP/IP ,通信方式为 SOCKET 流方式。终端与交易平台通过 SOCKET 流方式通讯,交易平台为 SERVER 端,终端为 CLIENT 端。由 CLIENT 端发出请求包发起交易,SERVER 端对各请求回送响应. 通过建立 VPN 经过防火墙接入应用服务器,经过交易中心业务解析处理后通过 TUXEDO 接口与计费中心交互[11]。

3　CDMA EVDO 动态 VPDN 技术在电信行业 EPOS 交费平台中应用

如图 2 所示,基于 CDMA EVDO 动态 VPDN 技术的 EPOS 交费平台使用非常方便,终端用户就像平时用 EVDO 上网一样,只输入专用的用户名和密码就能建立起与后台交费平台的连接。网络中用来建立 3G 网和分组数据网的接入网关由 PDSN 设备即分组业务数据节点实现,它为 3G 无线用户提供点对点的连接(PPP 协议)来完成 IP 分组数据业务的接入,从而确保了 IP 数据包在无线 3G 网与 IP 网间的安全传输; DCN 内的 RADIUS 服务器实现了 AAA 认证等功能, EPOS 系统的账号、密码如果被 RADIUS 检测到,就建立 PDSN 和 LNS 的连接,这个连接内部使用 L2TP 协议,我们将其称之为隧道连接,通过该隧道连接使数据传输的安全得以确保。一个 session 会随着 L2TP 的建立在 LNS 中出现,这个新会话的 IP 临时地址将从 IP Pool 中动态分配得到[12],最终 EPOS 终端用户可以登陆交费平台进行交费。在 CDMA EVDO 客户端的接入方案中,EDM500 防火墙(LNS)是关键设备,它既完成网络的连接,同时还作为 VPDN 的网关使用,目前全省 PDSN 有六台设备,EDM500 终结 6 条 L2TP 的隧道,将远端的 VPDN 拨号用户接入到 VPDN 专网网络中,完成交费过程。

L2TP 的建立过程是:

①远端用户采用 EPOS 终端拨入 LAC(PDSN),拨打号码为#777,并输入 username@ ctdsxt. vpdn. sn 和密码。

②PDSN 将 username@ ctdsxt. vpdn. sn 送到分组网 AAA 服务器,EDM500(LNS)信息,包括 LNS IP 地址等信息由 AAA 服务器向 LAC(PDSN)提供。

③若 username@ ctdsxt. vpdn. sn 信息为正确的 VPDN 用户信息,则 LNS 信息,通过 AAA 服务器送给

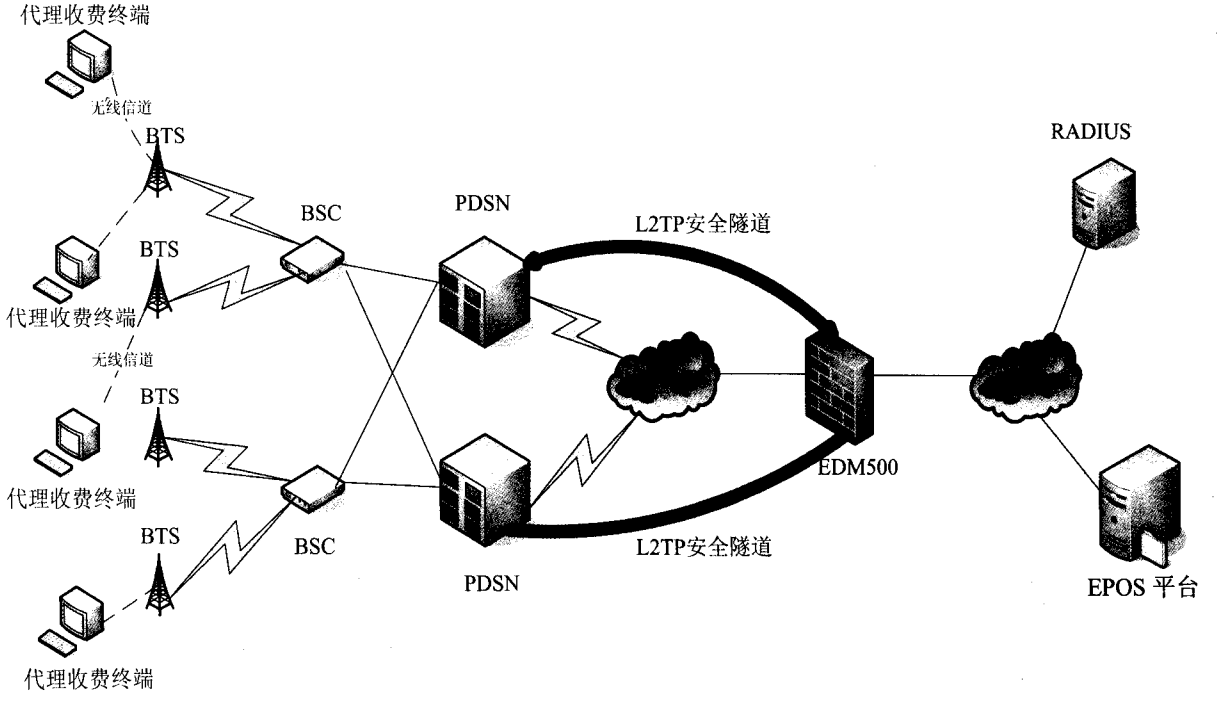

图 2　EVDO 动态 VPDN 在 EPOS 交费平台中应用

LAC。

④L2TP 隧道建立在 PDSN 与 EDM500 之间进行，并将 username@ ctdsxt. vpdn. sn 全部送给 EDM500，由它进行认证。

⑤DCN 内部的 RADIUS 服务器(认证服务器)从 EDM500 获得 uusername@ ctdsxt. vpdn. sn 认证信息。

⑥如果认证通过则允许接入并保持 L2TP 隧道，EPOS 终端将获得合法的 IP 地址。

⑦完成 VPDN 操作，端到端的数据，从 EPOS 终端传到 EDM500，从而进入 DCN，完成缴费交易[13]。

为了加强系统的安全性，还需把 UIM 卡上的 IMSI 信息与@ ctdsxt. vpdn. sn 进行捆绑，防止 EPOS 终端使用 CARD 帐户进行公网登录。

4 结束语

伴随着现代通讯技术的飞速发展，POS 技术开始从有线走向无线。采用码分多址分组数据传输技术的 CDMA 无线 POS 由于辐射低、线路稳定、保密性强、高速等特点已成为无线技术中应用前景最为广阔的一种。CDMA EVDO VPDN 系统实现了 EPOS 交费系统的有效延伸。可以利用 CDMA EVDO 随时随地上网的特点，进一步优化网络构架，以渠道建设为起点，方便代理点的交费、充值、售卡等工作，同时加强了代办员的实时管控，有效减少了欠费。基于 EPOS 系统的“随 e 付”在电信行业的应用，展现了信息化对行业发展和社会进步的深远影响。一方面，它协助电信稳步的开展行业发展转型，提供了更多其展示服务与产品的空间，两者在功能发挥上融合互通，相得益彰。另一方面，随着 EPOS 在各个行业应用的深化，信息科技的魅力充分展现，它将为人们创造舒适、便捷、安全生活，在我国社会经济全面快速步入信息化高速公路上发挥越来越重要的作用。

参考文献：

[1] 张 骏. CDMA 1X 动态 VPDN 技术在税务系统中的应用[J]. 通信世界网，2005(25)：32-34.

[2] 宁孟丽，李 颖. 基于 VPDN 技术的无线数据传输系统[J]. 中国科技信息，2005(13)：45-46.

[3] 程 思，程家兴. VPN 中的隧道技术研究[J]. 计算机技术与发展，2010，20(2)：156-159.

[4] 张智江，刘申建. CDMA2000 1x EV-DO 网络技术[M]. 北京：机械工业出版社，2005：60-64.

[5] 林曙光. CDMA2000 分组域网络技术[M]. 北京：北京邮电大学出版社，2006.

[6] 王 达. 虚拟专用网(VPN)精解[M]. 北京：清华大学出版社，2004：123-125.

[7] 陈淑荣. 拨号虚拟专用采用的 L2TP 及其相关技术分析[J]. 数据通信，1999(4)：37-39.

[8] 贾永杰，周秋剑，李 刚. VPN 隧道协议比较与分析[J]. 空军雷达学院学报，2003(2)：28-31.

[9] 杨静雯. CDMA 1X 分组域 VPDN 业务解决方案[J]. 通信世界，2004(7)：52-55.

[10] 李明铎，任立刚. CDMA2000 1x 分组域 VPDN 的安全性分析[J]. 电信技术，2004(12)：72-75.

[11] Hills S，McGlaughlin D，Hanafi N. IP Virtual Private Networks [J]. BT Technology Journal，2000，18(3)：151-161.

[12] Bollapragada V，Khalid M，Wainner S. IPSec VPN 设计[M]. 北京：人民邮电出版社，2006：60-63.

[13] Doraswamy N，Harkins D. IPSec 新一代因特网安全标准[M]. 京京工作室，译. 北京：机械工业出版社，2000：40-42.

(上接第 181 页)

伺服电机分布式控制 CAN 总线通讯系统[J]. 工业控制与应用，2006，25(2)：24-26.

[3] Ran Ping，Wang Baoqiang. The Design of Communication Convertor Based on CAN Bus[C]//International Conference on Industrial Technology. [s. l.]：IEEE，2008.

[4] Li Xiaoming，Li Mingxiong. An Embedded CAN-BUS Communication Module for Measurement and Control System[C]// Internationan Conference on ICEEE. [s. l.]：IEEE，2010.

[5] 钟 斌，程文明，唐连生. 起重机吊重智能防摇 CAN 控制系统的设计[J]. 起重机运输机械，2007(6)：38-40.

[6] Zhang Lihong，Sun Lei，Han Shufen，et al. Measurement and Control System of Soil Moisture of Large Greenhouse Group Based on Double CAN Bus[C]//Third International Conference on Measuring Technology and Mechatronics Automation. [s. l.]：[s. n.]，2011.

[7] 王宜怀，刘晓升. 嵌入式系统-使用 HCS12 微控制器的设计与应用[M]. 北京：北京航空航天大学出版社，2008：257-258.

[8] 刘宇婕，张保平. 基于 P87C591 构成 CAN 总线节点的设计[J]. 微处理机，2008，29(3)：156-159.

[9] Philips Semiconductors. Data Sheet TJA1040 High Speed CAN Transceiver[S]. 2000.

[10] 智 鹏，杨 进. 基于 CAN 总线的分布式设备数据采集与监控系统的研究与应用[J]. 中国仪器仪表，2005(11)：75-77.

[11] 邱 晟，向 欣，汪秉文. 基于 CAN 总线的分布式监控系统[J]. 工业控制计算机，2008，21(6)：72-73.

[12] 刘维弋，金远平. 基于 CAN 总线的通信系统的设计与实现[J]. 计算机技术与发展，2007，17(12)：207-209.