工业物联网安全态势分析报告 I

DTU 数据中心态势感知报告

灯塔实验室

http://plcscan.org/

目录

国内工业物联网发展迅速，无线数据采集与传输是工业物联网数据通信中重要的采集方式和组网方式，DTU 在无线数据采集所涉及到的供热、燃气、气象等市政重点工业领域应用及其广泛。最近灯塔实验室对国内暴露在互联网的 DTU 数据中心（DSC）进行了全网扫描，并对已发现的 DTU 中心站进行了深入的行业应用和用户所属单位分析。

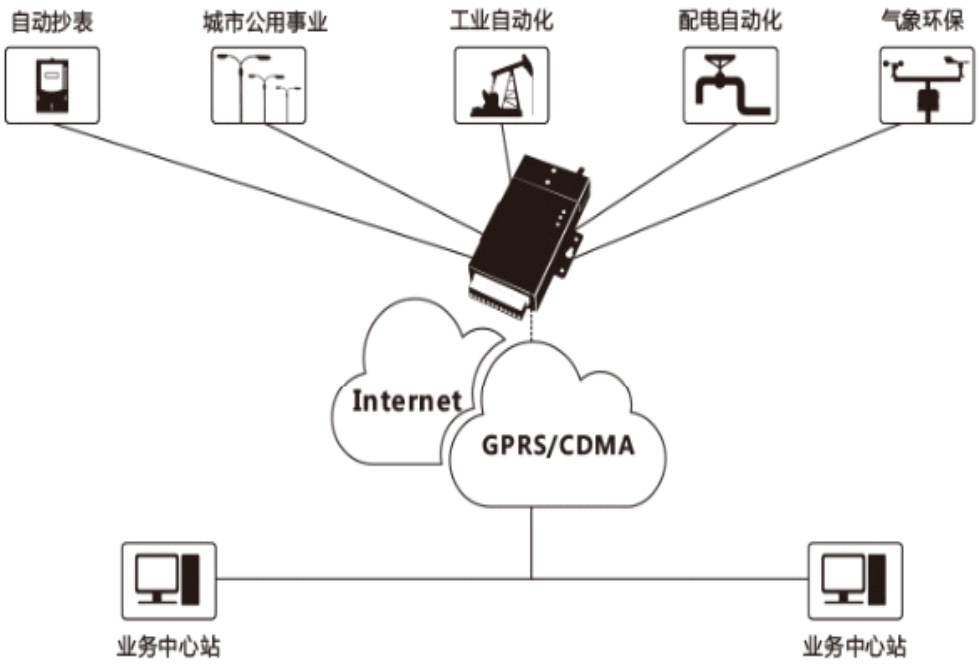
灯塔实验室长期致力于工控安全攻防技术研究和探索，后续我们会继续发布针对工业物联网设备、工控设备、协议、系统的风险报告，如果你对本研究报告的任何细节感兴趣，亦或技术交流，均可与我们取得联系，邮箱：labs@plcscan.org。

一、关键词定义

DTU：数据终端单元（Data Transfer unit）。

DSC：数据服务中心（Data Service Center），即 DTU 中心站，DTU 通过无线 GPRS/CDMA 网络将数据上传至中心站监听的某个端口。

DDP：DTU 和数据服务中心（DSC）之间的通讯协议。



二、应用场景

在工业现场中，存在许多现场是有线无法到达的场景，DTU 无线数据终端基于 GPRS/CDMA 数据通信网络，可专门用于将串口数据转换为 IP 数据或将 IP 数据转换为串口数据，并通过无线通信网络进行传输，目前广泛应用在电力、环保监测、车载、水利、金融、路灯监控、热力管网、煤矿、油田等行业。

三、DTU 数据中心指纹特征分析

DTU 与 DSC 中心站通信可使用 TCP/UDP 方式，DTU 会根据配置主动连接 DSC 中心站 IP 和开放的数据服务端口进行数据上传。

通信端口

根据厂家和应用的不同，DSC 开放的数据上传端口也不尽相同，我们根据厂商官方提供的一些解决方案和文档，搜集了一些知名厂商的默认端口，具体如下：

厂商	默认端口
宏电 DTU	5002
深证汉科泰	5003
厦门才茂通信科技	5001
济南有人物联网	5007
聚英电子	5004
拓普瑞 GPRS DTU	5000
TLINK	5006
厦门锐谷通信	8002
蓝斯通信	10000
鑫芯物联	2009
四信科技	5020
山东力创	3030

协议介绍

DDP 协议（DTU DSC Protocol）是 DTU 与 DSC 之间的通讯协议，DDP 是一种厂商定义的私有公开性质的通信协议，用于数据的传输和 DTU 管理，对于 DDP 协议厂商一般会提供协议文档和 SDK 开发包，用户可以通过组态软件或开发包，将数据中心集成到自己的平台软件中，国内的组态王、三维力控、昆仑通态、紫金桥等著名组态软件公司也均可以对接 DTU 实现数据采集。

以 DTU 市场占有量较高的宏电公司的 DTU 为例，宏电 DDP 协议官方提供了通信协议文档和数据中心 SDK 样例可供用户进行二次开发和集成。

宏电 DDP 协议数据帧格式

起始标志	包类型	包长度	DTU 身份识别	数据	结束标志
（1B）	（1B）	（2B）	（11B）	（0~1024B）	（1B）
0x7B					0x7B

宏电 DDP 协议 DTU 请求功能类型

包类型	包类型描述	传输类型
0x01	终端请求注册	GPRS
0x02	终端请求注销	GPRS
0x03	查询某一 DTU IP 地址	GPRS
0x04	无效命令或协议包（一般在查询或设置指令时使用）	GPRS
0x05	DSC 接收到用户数据的应答包	GPRS
0x09	DSC 发送给的用户数据包	GPRS

0x0B	DTU 查询参数的应答包	GPRS
0x0D	DTU 设置参数的应答包	GPRS/SMS
0x0E	DTU 提取日志的应答包	GPRS
0x0F	远程升级的回应包	GPRS/SMS

指纹构造

通过构造符合 DDP 协议的 DTU“注册”请求发送到 DSC 中心站，可以作为识别中心站的一种手段，如果目标应用的端口运行有中心站服务将会返回符合 DDP 协议标准的数据包。

四、安全隐患分析

DTU 与 DSC 中心站之间通信使用的 DDP 协议构造简单，通信时一般使用 DTU 中插入的 SIM 卡的 11 位手机号码作为“身份识别”的手段，DTU 主动链接 DSC 中心站开放的 TCP/UDP 端口上传数据，并且以明文方式传输，从目前 DTU 无线数据远传的通信模型上来看，最易受攻击的攻击面主要在 DSC 中心站上。

根据我们的本地分析与测试，暴露在互联网的 DTU 中心站易受到如下攻击：

终端伪造风险

根据 DTU 与 DSC 中心站的通信协议，攻击者可以构造任意手机号码（11 个字节的 DTU 身份识别标识）的“注册”请求，如果用户的应用逻辑上没有判断该手机号码是否可信，该设备将可以被注册到 DSC 中心站。

数据伪造风险

攻击者可以构造任意手机号码（11 个字节的 DTU 身份识别标识）的“注册”请求，并在同一时间或一段时间内发送大量“注册”登录请求到 DSC 中心站，

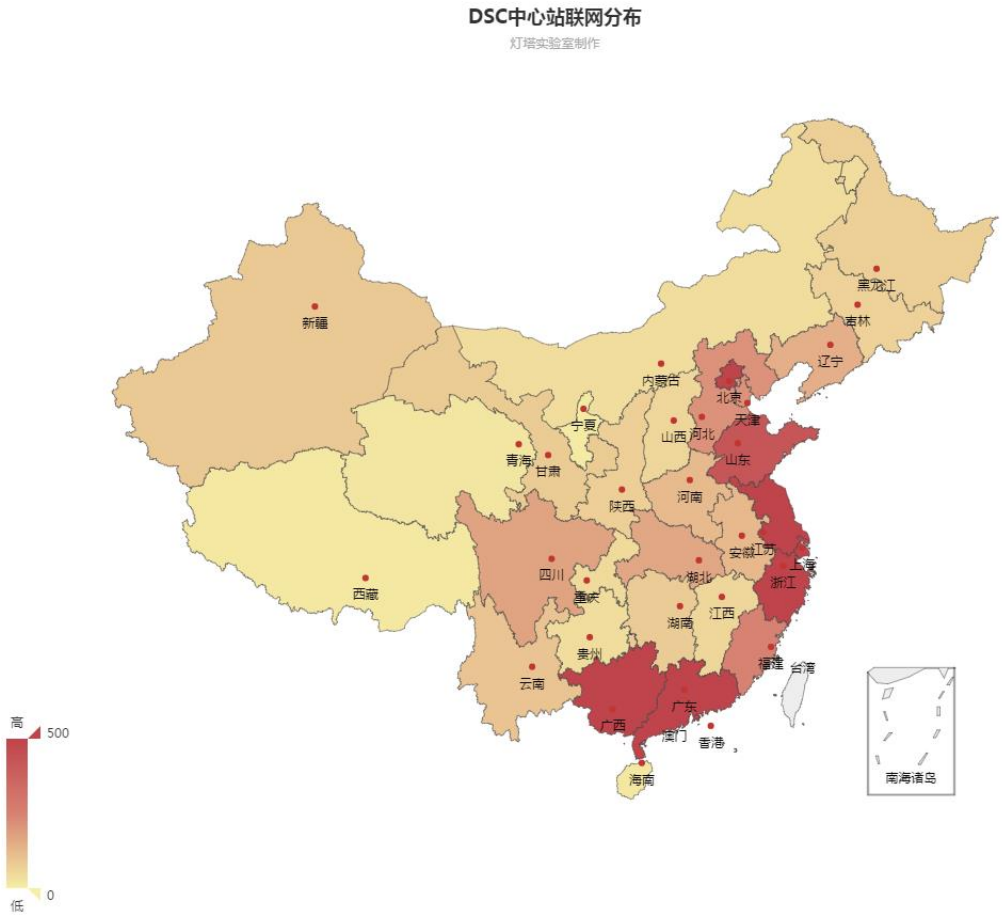
对于未做身份标识验证和判断的 DSC 中心站应用将会消耗大量系统资源，甚至导致中心站的采集应用崩溃，所有 DTU 设备无法链接至 DSC 中心站，使数据采集中断。

终端枚举风险

DTU 与 DSC 中心站之间使用 11 位手机号码作为“身份识别”，攻击者如果知道 DTU 终端的 11 位手机号码，即可以伪造对应的终端进行数据上传或将终端请求注销，如果确定了该应用场景或准确的地市区，针对终端号码的枚举或爆破将会缩小到较小的尝试范围。

五、DTU 数据中心联网分布

鉴于 DSC 中心站各家应用开放端口不一致的情况，我们实验室对国内 3 亿 IP 超过 160 个常用于发布 DDP 服务的端口进行了识别扫描，其中发现运行有 DDP 协议服务的主机超过了 8800 个，具体分布如下：



广东	1998
香港	1052
浙江	710
上海	676
北京	631
广西	556
江苏	500
山东	427
福建	251
河北	212
天津	208
四川	171
湖北	164

辽宁	144
安徽	125
河南	119
云南	99
新疆	88
中国	84
甘肃	81
湖南	80
陕西	73
黑龙江	71
吉林	66
江西	58
山西	57
重庆	48
内蒙古	41
贵州	41
青海	22
西藏	17
海南	17
宁夏	9
总计	8896

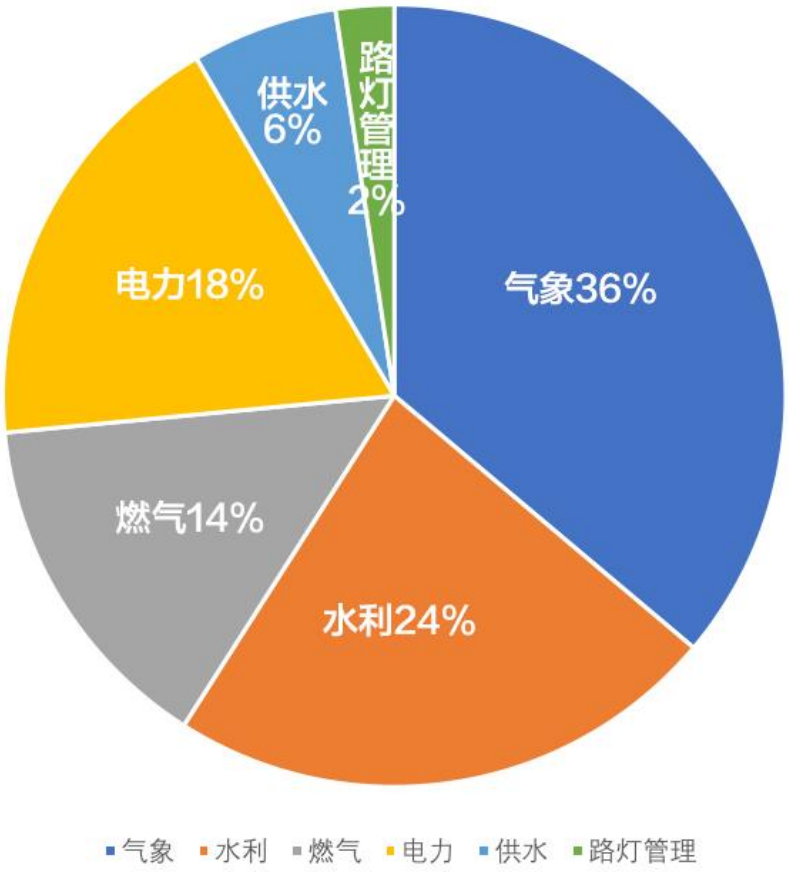
发布 DDP 服务最多的前 30 个端口：

排行	端口	暴露数量
1	5060	1302
2	9999	1248
3	5002	802
4	60000	575

5	55555	547
6	50123	537
7	51960	418
8	65000	392
9	61697	385
10	2000	296
11	3000	234
12	8000	204
13	6000	108
14	1025	92
15	5001	88
16	6004	87
17	33333	81
18	10001	76
19	5000	75
20	60001	69
21	5007	67
22	5003	61
23	5005	61
24	8001	60
25	4000	56
26	6002	45
27	7001	41
28	7000	40
29	5004	39
30	8888	32

六、联网企业与应用分析

根据对扫描到的数据，我们实验室通过 IP 开放服务、IP 位置，分析验证了运行公网的 DSC 中心站所属的企业和单位，具体行业分布如下，我们目前已经准确验证了超过 300 家公司和单位的 DDP 服务暴露情况，详细报告获取联系：labs@plcscan.org。



七、解决方案与应对策略

在本次针对DSC数据中心站的安全分析的过程中，像终端使用GPRS/CDMA直接经过互联网与中心站的固定/动态 IP 进行通信，这种快捷、廉价的组网应用广泛，目前虽然没有出现专门针对此类系统公开的攻击事件，但根据我们的判断，对于 DDP 协议这种 ICS 协议暴露将缩短攻击者发现重要工业控制系统入口的时间，随着 DDP 服务的开放易导致该 IP 目标成为针对性的被攻击对象，我们建议

使用此类组网的用户，尤其应该做好边界入口的安全防护、应用服务（Web、Telnet、SSH）的安全加固、主机安全配置。

灯塔实验室依据工信部《工业控制系统信息安全防护指南》以及相关国家标准，给出如下具体应对建议：

身份认证

我们建议在互联网开放 DDP 服务的用户，应检查除 DDP 服务以外，如 Telnet、SSH、Web 服务等服务配置的安全性，避免使用默认口令或弱口令，合理分类设置账户权限，以最小特权原则分配账户权限，对于关键系统和平台的访问采用多因素认证。

远程访问安全

我们推荐有条件的用户在中心与终端之间使用电信运营商提供的 APN 专网进行组网，DTU 的 SIM 卡开通专用 APN 接入，使用 APN 专线后所有终端及数据中心分配的 IP 地址均为电信运营商的内网 IP 地址，通过 APN 专网终端与数据中心的数据通信无需通过公网进行传输，专网实现了端到端加密，避免了中心在互联网开放网络端口。