目录

[Modbus Tcp协议分析 1](#_Toc495994170)

[1、Modbus传输方式 2](#_Toc495994171)

[1.1 ASCII模式 2](#_Toc495994172)

[1.2 RTU模式 3](#_Toc495994173)

[1.3 Modbus消息帧 3](#_Toc495994174)

[2、Modbus TCP协议分析 4](#_Toc495994175)

[2.1 Modbus TCP协议 5](#_Toc495994176)

[2.1.1 Modbus TCP安全性分析 9](#_Toc495994177)

Modbus Tcp协议分析

# 1、Modbus传输方式

控制器能设置为两种传输模式（ASCII或RTU）中的任何一种在标准的Modbus网络通信。用户选择想要的模式，包括串口通信参数（波特率、校验方式等），在配置每个控制器的时候，在一个Modbus网络上的所有设备都必须选择相同的传输模式和串口参数。

所选的ASCII或RTU方式仅适用于标准的Modbus网络，它定义了在这些网络上连续传输的消息段的每一位，以及决定怎样将信息打包成消息域和如何解码。在其它网络上（像MAP和Modbus Plus）Modbus消息被转成与串行传输无关的帧。

## 1.1 ASCII模式

当控制器设为在Modbus网络上以ASCII（美国标准信息交换代码）模式通信，在消息中的每个8Bit字节都作为两个ASCII字符发送。这种方式的主要优点是字符发送的时间间隔可达到1秒而不产生错误。

代码系统：

· 十六进制，ASCII字符0...9，A...F

· 消息中的每个ASCII字符都是一个十六进制字符组成

每个字节的位：

· 1个起始位

· 7个数据位，最小的有效位先发送

· 1个奇偶校验位，无校验则无

· 1个停止位（有校验时），2个Bit（无校验时）

错误检测域：

· LRC(纵向冗长检测)

## 1.2 RTU模式

当控制器设为在Modbus网络上以RTU（远程终端单元）模式通信，在消息中的每个8Bit字节包含两个4Bit的十六进制字符。这种方式的主要优点是：在同样的波特率下，可比ASCII方式传送更多的数据。  
代码系统：  
· 8位二进制，十六进制数0...9，A...F   
· 消息中的每个8位域都是一个两个十六进制字符组成  
每个字节的位：  
· 1个起始位  
· 8个数据位，最小的有效位先发送  
· 1个奇偶校验位，无校验则无  
· 1个停止位（有校验时），2个Bit（无校验时）  
错误检测域：  
· CRC(循环冗长检测)

## 1.3 Modbus消息帧

两种传输模式中（ASCII或RTU），传输设备以将Modbus消息转为有起点和终点的帧，这就允许接收的设备在消息起始处开始工作，读地址分配信息，判断哪一个设备被选中（广播方式则传给所有设备），判知何时信息已完成。部分的消息也能侦测到并且错误能设置为返回结果。  
1、ASCII帧  
使用ASCII模式，消息以冒号（:）字符（ASCII码 3AH）开始，以回车换行符结束（ASCII码 0DH,0AH）。其它域可以使用的传输字符是十六进制的0...9,A...F。网络上的设备不断侦测“:”字符，当有一个冒号接收到时，每个设备都解码下个域（地址域）来判断是否发给自己的。消息中字符间发送的时间间隔最长不能超过1秒，否则接收的设备将认为传输错误。一个典型消息帧如下所示：

2、RTU帧  
使用RTU模式，消息发送至少要以3.5个字符时间的停顿间隔开始。在网络波特率下多样的字符时间，这是最容易实现的(如下图的T1-T2-T3-T4所示)。传输的第一个域是设备地址。可以使用的传输字符是十六进制的0...9,A...F。网络设备不断侦测网络总线，包括停顿间隔时间内。当第一个域（地址域）接收到，每个设备都进行解码以判断是否发往自己的。在最后一个传输字符之后，一个至少3.5个字符时间的停顿标定了消息的结束。一个新的消息可在此停顿后开始。整个消息帧必须作为一连续的流转输。如果在帧完成之前有超过1.5个字符时间的停顿时间，接收设备将刷新不完整的消息并假定下一字节是一个新消息的地址域。同样地，如果一个新消息在小于3.5个字符时间内接着前个消息开始，接收的设备将认为它是前一消息的延续。这将导致一个错误，因为在最后的CRC域的值不可能是正确的。

# 2、Modbus TCP协议分析

Modbus通讯协议包括在RS232和RS485等串行链路上传输的Modbus和在以太网上传输的Modbus。下面介绍在以太网TCP/IP上传输的Modbus，即Modbus TCP协议。

Modbus TCP（Modbus协议系列）是将Modbus帧嵌入到TCP帧中，从而实现Modbus协议的网络传输。对于原现场总线设备，通过专用的Modbus TCP网关使其与工业以太网相连，完成透明和高速的信息传输。Modbus控制网络结构如图2-1所示。该网络将现场总线设备连到Modbus TCP工业以太网中，实现了现场设备、仪器仪表的联网，从而实现现场设备的远程访问和控制。



图2-1 Modbus网络体系结构实例

## 2.1 Modbus TCP协议

Modbus是一个请求/应答协议，图2-2描述了Modbus请求响应模型。主设备是主动方，在实际工业控制系统环境中应为控制器端，发送控制指令；从设备是被动方，在实际工业控制系统环境中应为执行器或者传感器，执行控制器的控制指令并返回检测数值给控制器。



图2-2 Modbus请求/响应模型

TCP/IP协议自20世纪80年代诞生以来，由于其灵活性、经济性以及适用性而取得巨大成功。TCP/IP简化了OSI的7层模型，省略了表示层和会话层，图2-3所示Modbus TCP使用TCP/IP以太网的5层结构。



图2-3 TCP/IP通信模型

Modbus TCP协议嵌在TCP数据包中，使用502端口进行数据通信。如图2-4所示描述了Modbus TCP协议在TCP/IP协议栈中的位置，可以看出，Modbus TCP协议是应用层协议，嵌在传输层TCP数据包的传输层数据部分。



图2-4 Modbus TCP数据包结构图

图2-5描述了通用的Modbus帧结构，Modbus协议定义了

PDU：协议数据单元

ADU：应用数据单元

PDU包括功能码和数据部分，它与基础通信层无关。ADU在PDU的基础上添加了地址域和差错校验，不同总线和网络上的Modbus协议在ADU上会添加不同的信息。图2-6描述了TCP/IP上Modbus帧的结构，由于TCP/IP协议中的数据链路层已有数据校验，所以Modbus TCP帧中没有差错校验。



图2-5 通用MODBUS帧



图2-6 Modbus在TCP/IP上的帧

如图2-6描述了Modbus TCP协议的格式，Modbus TCP帧包括MBAP报文头、功能码和数据部分。

一、MBAP报文头

MBAP报文头包括事务处理标识符、协议标志符、长度和单元标识符。事务处理标识符用来标识请求数据包和对应的响应数据包，避免当主设备发送多个请求数据包时请求数据包和响应数据包无法匹配的问题；协议标志符用来表明应用层协议类型，此标志位为0x0000代表此协议是Modbus TCP协议；长度标识的是单元标识符、功能码以及数据三部分的长度，不是协议的总长度；单元标识符用来指明和主设备相连接的从设备的识别码。

表2-1 MBAP头部信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 区域 | 所占长度 | 内容 | 客户端 | 服务器 |
| 事务处理标识符 | 2字节 | 标识请求数据包和对应的响应数据包的序列号 | 主机生成 | 从机应答时复制该值 |
| 协议  标识符 | 2字节 | Modbus协议为  0x0000 | 主机生成 | 从机应答时复制该值 |
| 长度 | 2字节 | 剩余部分数据的长度 | 主机生成 | 从机应答时由从机端生成 |
| 单元标  识符 | 1字节 | 从机地址 | 主机生成 | 从机应答时复制该值 |

二、功能码

功能码是主设备向从设备发送控制指令的关键，每个特定的功能码代表不同的控制执行操作。功能码一旦被恶意修改，执行器会受到错误的控制指令而执行错误的操作。功能码占一个字节的长度，转化为十进制的有效范围是1-255。



图2-7 功能码分类

Modbus的功能码可以分为三类：公共功能码、用户自定义功能码和异常响应保留功能码。其中128-255为异常响应保留功能码，它是一些公司对其特定产品所使用的功能码，用来判断响应的异常类型，一般很少使用。公共功能码与自定义功能码的范围为1-127。公共功能码是已被较好定义的功能码，并且是唯一的、公开的、一致的。自定义功能码是指用户在65-72和100-110这两个范围内可自行选择和定义操作的功能码，但是该功能码的使用不是唯一的。图2-7显示了公共功能码和用户自定义功能码的划分区间。

三、数据

Modbus有四种基本的数据类型，分别为离散量输入、线圈、输入寄存器和保持寄存器。其中，离散量输入和输入寄存器为只读类型的数据，主要由I/O系统提供，线圈和保持寄存器为读写类型的数据，主要通过应用程序来更改。数据部分主要包括各类数据类型的起始地址，操作的数量以及需要写入的数值，响应数据包中会包含数据的长度信息。数据部分的长度可以为0，即数据部分不存在，此时只进行功能码定义的操作。Modbus具有4种基本的数据类型，如表2-2所示。

表2-2 Modbus数据类型

|  |  |  |  |
| --- | --- | --- | --- |
| 数据类型 | 对象类型 | 访问类型 | 内容 |
| 离散量输入 | 1比特 | 只读 | I/O系统提供 |
| 线圈 | 1比特 | 读写 | 应用程序读写 |
| 输入寄存器 | 16比特 | 只读 | I/O系统提供 |
| 保持寄存器 | 16比特 | 读写 | 应用程序读写 |

对于表2-2中的每一种数据类型，其物理地址范围都是16位的2进制数（十进制为0-65535）。数据存储的方式有大端存储和小端存储两种模式，Modbus使用大端存储表示物理地址和数据项，即传输数据时先发送高位数据。例如一个16位数据0x1234，在传输时首先发送0x12，然后发送0x34。

### 2.1.1 Modbus TCP安全性分析

Modbus TCP协议最初主要被用在与其他网络相隔离的工业控制网络中，除了对可靠性、实时性和效率的要求外，并未考虑到协议本身的安全问题，而且目前Modbus管理组织也没有在协议中添加任何安全特征。同时，Modbus TCP协议底层基于TCP/IP技术，因此标准以太网的底层协议缺陷也被继承下来。

当前Modbus TCP协议的安全缺陷主要有以下几类：

1）缺少认证保护

缺少认证主要表现在仅需一个合法的功能码和一个合法的地址就可以通过TCP协议的502端口建立起一个Modbus通信会话。未认证的控制指令对控制过程造成严重威胁。

2）缺少授权保护

缺少访问控制机制，任何角色都可以对目标进行访问控制。缺乏对用户的分类以及对用户权限的划分，使得任何用户都能够进行任意的操作控制，实现任何的目的。

3）缺少加密保护

缺少加密表现在整个应用层的Modbus协议使用明文传输，通信过程中双方信息被第三方获取后，可以很轻易的解析出功能码、地址、数据等协议内容，为攻击者入侵提供了便利。

Modbus协议通信方式有两种：一种最常见的是为应答机制，Modbus主机发送请求（比如控制指令）给从机（比如执行器）进行一定操作，随后从机发送应答给主机；另外一种是广播的形式，主机发送广播给所有的从机，从机执行一定的操作而不需要给主机发送应答数据包。另外Modbus协议没有任何的安全防护机制。上述特点使得Modbus通信容易受到攻击。

一般来说，应用Modbus TCP协议的工业控制系统网络主要注重命令的授权性、信息的保密性和通信的完整性。命令的授权性是指主设备发送给从设备的控制指令是合法的；信息的保密性是指主设备发送给从设备的控制指令和从设备发送给主设备的检测信息不会被攻击者获取；通信的完整性是针对Modbus TCP协议的问答机制，具体是指请求和响应数据包不会被恶意丢弃且数据包的内容不会被修改。针对Modbus TCP安全性的3个方面，产生3种针对工业控制系统的攻击：

第一种是针对协议没有认证和授权机制而发起的攻击，通过修改主设备发送的控制指令，使从设备执行清除计数器、诊断寄存器等未经授权的指令，导致工业控制系统的故障；

第二种是针对保密性的攻击，首先通过扫描的方式获取通信的主/从设备，然后获取主设备发送给从设备的控制指令或者从设备发送给主设备的测量数据；

第三种是针对Modbus TCP的问答通信机制的攻击，通过修改从设备发送给主设备的响应数据包等，实现控制端获取错误的检测数据从而执行错误的控制指令，导致控制系统异常。

1、针对协议无认证授权的攻击

针对协议本身以及通信特点的攻击，在采用Modbus TCP通信协议的工业控制系统中有四种具体的表现：

第一种攻击表现形式是模仿主设备发送强制从设备清除计数器和诊断寄存器[33]的控制指令，从而导致控制回路异常；

第二种攻击表现形式是模仿主设备发送强制从设备重启或者强制从设备处于监听状态的控制指令，从而导致对于主设备的正常控制指令无法执行。

第三种攻击表现形式是通过修改寄存器的值，来达到“欺骗”控制器，使控制器做出错误的决定，从而引发严重的后果；

第四种攻击表现形式是修改主设备发送给从设备的功能码，导致远程终端执行非法动作。

2、针对保密性的攻击

针对信息保密性的攻击，在采用Modbus TCP通信协议的工业控制系统中有两种具体的表现：

第一种攻击表现是扫描工业控制系统中可用的从设备；

第二种攻击表现是获取主设备发送给从设备的控制指令或者从设备发送给主设备的测量数据。

3、针对Modbus通信问答机制的攻击

针对Modbus通信问答机制的攻击，在采用Modbus TCP协议的工业控制系统中有两种具体的表现：

第一种攻击表现是截取从设备向主设备发送的响应数据包，发送之前截取的历史数据包；

第二种攻击表现是利用主设备只接受第一个响应数据包的特性，在正常响应数据包到达主设备之前，发送一个响应数据包给主设备。