机械工程(4)2022,4
ISSN: 2661-3530(Print); 2661-3549(Online)

西门子变频器无线通信安全性研究

刘　亮
身份证号码：130928198208100037

摘　要：西门子变频器采用了与变频电动机相结合的方式，但也有可能被无线网路中间人入侵。为了解决西门子变频器的无线通讯中的安全问题，利用西门子SINAMICS V20 Wifi Module智能型联接装置，使移动电话或操作员工作站连接Wifi与西门子V20变频器相联接，对西门子变频器的转速、旋转方向、启停等进行了全面的监控。对西门子变频器的变频器联接模块Wifi变频器进行了仿真，发现SYNACK对其进行了入侵，从而造成其工作状态的变化，并提出了相应的预防措施。

关键词：通讯；PROFIBUS；变频器；中间人；无线通信

Research on wireless Communication security of Siemens Frequency Converter

Liang Liu
Id card Number: 130928198208100037

Abstract: Siemens inverter adopts a combination of frequency conversion motor, but it may be invaded by intermediary of wireless network. In order to solve the security problem in the wireless communication of Siemens frequency converter, the intelligent connection device of SINAMICS V20 Wifi Module of Siemens is used to connect the Wifi of mobile phone or operator workstation with Siemens V20 frequency converter. The speed, rotation direction, start and stop of Siemens inverter are monitored comprehensively. It is found that SYN ACK has invaded the transducer connecting module Wifi transducer of Siemens transducer, which causes the change of its working state, and puts forward the corresponding preventive measures.

Keywords: Communication; PROFIBUS; Frequency converter; intermediary; Wireless communication

引言：

近几年，由于出现了大量的系统缺陷，使得受到攻击的可能性大幅上升。目前的WLAN技术有MITM和DoS技术。本文着重于MITM的袭击，这类袭击可能包含很多独立的袭击，例如：干扰攻击、DoS袭击[7]，蜜罐袭击等等。当西门子变频调速电动机在无线通讯中出现Wifi MITM的情况下，会造成电机脱轨，引起控制马达的正转、反转甚至停止。在这样的情况下，入侵者与频率转换装置进行了独立的传输，而当监视器的控制面板没有出现问题的时候，整个通讯系统就会完全被黑客控制，从而造成无法预料的危险。为了解决以上问题，本文利用西门子SINAMICSV20V20型西门子变频器V20型智能型联接装置，使移动电话或操作员工作站连接Wifi与西门子V20变频器相连，从而实现西门子变频器的转速、旋转方向、启停等功能。

一、变频器控制

1.变频器控制方式比较

常规的变频调速系统有两种方法：一是采用变频调速系统内的主控面板（BOP），在BOP上设置一个按键，设置好了的参数，即可进行变频调速或变频调速，此控制方法操作简便，仅适用于变频调速器的调速；常用的是硬接线式，根据接线图，将变频器的各个控制信号和所要获取的状况信号以配线的形式存入PLC的一列信号终端，此方法还要求设置变频装置的有关参数。变频通信控制是指采用工业现场总线将变频调速系统与控制器相结合，由控制器根据通信协定实现对变频调速系统的双向通信，其中包括对变频调速系统的控制指令以及变频调速系统的工作状况等。与常规的方法相比，这种方法具有以下优势：

（1）简化了控制接线

当前，大部分工业总线都是基于RS-485的实际应用。连线采用普通的屏蔽双绞线即可达到使用的目的，与硬线相比，可节省大量的电缆成本，减少了线材的制作和配线，并可在必要的情况下改变控制系统。

（2）数字化信号传输

在通信控制系统中，变频调速系统和上一代控制器的通信硬件部分均采用数字设备，原始控制信号采用模拟式交互式转换成直数型。

与常规的数字信号开关相比，既节省了A/D/D/A变换装置，改善了控制的精确度。

（3）容易实现多台变频器的远程集控

由于频率变换技术的普及，在不同的场合下，不同的频率范围内的变频器数量不断增加，使得变频器的远程集中控制是控制系统的基础。

2.变频器通讯控制

（1）通讯控制硬件接口

变频器的通信控制模式与其他通信模式相似，还要求对通信设备的实体界面和双端机协议进行规范。所有具备通信控制的变频调速系统，均应配备一串口，一般为双线路RS-485，其通信线路电压、阻抗等由其决定，并由差分电压转换至5V。通讯链路上的控制器一般是控制主基站，其他的频率变换器作为从站，从站和主站点的相应的物理地址可以接入。

（2）通讯控制软件协议

西门子变频调速系统所使用的通信协定是一种普通的串口通信协定（USS）。由于从站没有收到主站的存取请求，因此不能将资料资料传送给主站，而从站与从站不能进行相互存取，在报文资讯中由位址字节决定。通信信息是一个固定的字段，每个数据包的开头字母STX，然后是LGE，地址字节ADR，有效数据块区，以及BCC。

（3）过程控制与状态读取

在变频器通讯控制中，变频调速系统的运行模式，例如：正反转向、启停控制、运行频率等，都要重新编写PZD区域的控制字段，并根据PZD区域的读数来监控变频器的工作状况。尽管PZD区域的定义是0至4个字长，但是一般都是2个字长，而且根据传输的方向不同，其形式也不同。如果有必要对频率转换装置进行控制，则PZD区域由第一个字母作为STW，第二个字母是以设定频率速率（HSW）为次序构成。STW字符16个比特，分别规定了不同的操作模式，如上升或下降、正反转向、本地和远程操纵等。HSW是变频调速器的一个频率，它可以分为十进制和十六进制数法，由P2009的参数来决定。PZD区域包括在要求监测频率转换的情况下，其开头是一个状况（ZSW），而另一个是一个真实操作参数（HIW）。每个ZSW字每个人都定义了变频调速器准备、运行、故障、过载、报警等，HIW字符可以是用P2016的设定数值来决定的实际工作的频率或电流。

二、问题描述

1.存在的安全风险

另一方面，无线通信系统本身就具备持续发送SSID的特性，使得其易于被恶意用户察觉和使用。而在另一种情况下，频率转换器通讯的代理人会对网络套件进行干扰。接着，本文对IEEE 802标准中的无线通讯系统的安全性进行了研究。802.11协定群集是由IEEE（IEEE）制订的用于WLAN的标准。在IEEE 802中，显示了WLAN的架构。

根据IEEE 802. 11协议，MAC层帧可以分为管理帧、控制帧和数据帧3种类型。只有数据帧的有效负载部分受诸如WEP和WPA/WPA2之类的安全机制保护，管理帧则容易被破坏、复制或伪造。因此，在收到伪造的取消身份验证帧后，客户端会错误地认为这些帧来自合法AP，然后与合法AP断开连接[7]。如果攻击者不断发送伪造的取消身份验证帧，则客户端将永远无法连接到合法的AP，很难区分攻击。

三、西门子变频器攻击实验

1.MITM攻击过程

MITM是一种在通讯双方都没有察觉的前提下，对整个通讯进程进行监控和窃取和修改。变频器接入V20智能连接模块。西门子式1LA70704AB10Z与西门子SIMAMICSV20变频设备成功地接通后，该系统的无线通讯模组指示灯为绿灯，表明通讯正常。将WIFI接入计算机，通过kali的词典，强行破译，获得频率转换键。把虚拟机与实体主机连接起来，把变频机、攻击机、虚拟机与一个局域网连接起来，可以很方便地侦测到目标网路的资讯，并降低网路的路径，使得攻击更易于实施。

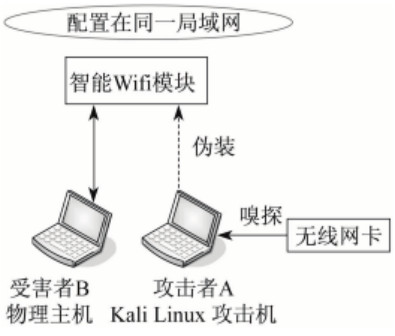

图1　网络拓扑结构

即，黑客在与变频器的Wifi智能模组及目的主计算机之间进行沟通时，已经取得了一定的效果。

2.无线钓鱼攻击过程

同时，由于系统的SSID信号一直在向外界发送，因此在无线通讯时，西门变频设备也很易遭受网络钓鱼的侵害。因为Aircrack具有网络侦测、数据包嗅测、WEP、WPA/WPA2 PSK等多种能力，所以它可以通过Aircrack（kali）来探测周围的SSID和MAC，构建DHCP系统，并设置好了实验条件。

建立一个无线网络钓鱼网的详细方法是：设置一个无线网络诱饵的热点，设置一个自动诱饵的端口，设置一个IP地址进行发送，然后对一个目标的主机发起一个无线的ddos，连接到一个新的网络。接着进行试验，选取网页和网页，对试验的结果进行攻击。通过测试，发现这个钓鱼网页和真实的登录网页一模一样，但却不是自己要登录的，一旦登录到了一个网络钓鱼网站，就会面临很多危险，这对西门子的网络系统来说，将是一个巨大的隐患。

四、结束语

因为这个袭击是建立在无线Wifi基础上的，所以首先要从发送无线讯息开始。厂商可以将其改装成一个无线模组，只要有一个人与该模组相连，就会自动切断SSID讯息的发送，从而在某种意义上，防止被骗。

不会轻易地连上WIFI。尽管受害人会因无线DDOS的袭击而被迫掉线，但普通的Wi-Fi伪热点验证与真正的WIFi验证程序还是有区别的。要知道，大部分的无线网络都会选择先联网，然后才会进行身份验证。一旦这个问题被澄清，那么，这个“诱饵”就会不攻自破。

参考文献：

[1]王勇，冯秀楠，顾龙，等.西门子变频器无线通信安全性研究[J].上海电力大学学报，2021，37（5）：5.

[2]周志敏，纪爱华.西门子变频器工程应用与故障检修实例[M].中国电力出版社，2016.

[3]王勇，冯秀楠，顾龙，等.西门子变频器无线通信安全性研究[J].上海电力大学学报，2021，37（5）：5.