ISSN 1004-9037,CODEN SCYCE4
Journal of Data Acquisition and Processing Vol. 34,No. 6,Nov. 2019,pp. 1110－1117
DOI:10. 16337/j. 1004-9037. 2019. 06. 018

http://sjcj. nuaa. edu. cn
E-mail:sjcj@nuaa. edu. cn
Tel/Fax:＋86-025-84892742

Modbus TCP安全协议的研究与设计

罗　旋　李永忠

(江苏科技大学计算机学院,镇江,212003)

摘　要: 针对Modbus TCP协议存在的安全问题,如缺乏认证、数据明文传输和功能码滥用等,基于原Modbus TCP协议提出一种安全的工控通信协议(Modbus-S协议):采用数字签名技术保证数据的完整性和可认证性;使用对称密钥技术保证数据的机密性;利用哈希算法的单向性原理保证数据的唯一性;最后使用“白名单”过滤机制基于角色对功能码进行管理,保证指令的可控性。实验验证和分析表明:Modbus-S协议可以全面弥补Modbus TCP协议的设计缺陷,与已有方法相比,该方法安全性更高,可以全面提高Modbus TCP协议的通信安全。

关键词: Modbus TCP协议;哈希算法;对称密钥;白名单;身份验证

中图分类号: TP393.04　　**文献标志码:** A

Research and Design of Security Protocol for Modbus TCP

Luo Xuan, Li Yongzhong

(School of Computer Science, Jiangsu University of Science and Technology, Zhenjiang,212003, China)

Abstract: Aiming at the security problems of Modbus TCP protocol, such as lack of authentication, data transmission in clear text and abuse of function codes, a secure industrial control communication protocol (Modbus-S protocol) based on the original Modbus TCP protocol is proposed. The digital signature technology is used to ensure the integrity and authentication of data. The symmetric encryption is used to ensure the confidentiality of data. The unidirectional principle of hash function is used to guarantee the uniqueness of data. Finally, the "white list" filtering mechanism is used to manage function codes based on roles to ensure the controllability of instructions. Experimental verification and analysis show that Modbus-S protocol can fully compensate for the design defects of Modbus TCP protocol. Compared with the existing methods, the method has higher security and can comprehensively improve the communication security of Modbus TCP protocol.

Key words: Modbus TCP protocol; hash algorithm; symmetric key; white list; authentication

引　　言

针对Modbus TCP协议存在的安全问题,不少学者做了相关研究,如高栋梁[1]以netfilter为框架,设计了一个Modbus TCP协议网关防火墙;Shang等[2]基于Linux平台,使用iptable工具设计了一个工业防

基金项目: 江苏省研究生实践创新计划(SJCX18_0784)资助项目。
收稿日期: 2018-09-28;**修订日期:** 2019-02-27

火墙。但是二者并未对传输数据做加密处理,不能保证数据的机密性,其次无法防止重放攻击。尚文利等[3]提出了一种基于统计分析的日志规则自学习算法,动态生成并更新规则;吕雪峰等[4]利用snort设计了基于协议缺陷和系统状态的检测规则,当测量值匹配规则时,触发告警。这二者提出的方法对规则精度的设定具有极高的要求,一旦精度设置过大或过小,都会严重影响检测效果。Fovino等[5]通过添加哈希链字段并作签名的方法实现了数据的完整性与可认证性,但仍存在功能码的滥用问题。

针对上述文献中存在的问题,本文基于功能码管理、数据传输以及可行性等问题对Modbus协议作了深入研究。以原Modbus协议为基础,设计了一种安全的工控系统通信协议——Modbus-S协议。该协议可以实现通信双方的双向认证,同时保证数据的完整性以及唯一性。该协议对关键数据字段进行加密,同时还可对功能码进行管理,从而全面提升工控通信的安全。

1　Modbus TCP协议

1.1　Modbus TCP协议介绍

Modbus TCP协议工作在TCP/IP模型的应用层,采用主从通讯模式,Modbus的主站可以与从站采用一对一或多对多方式进行通讯,其报文格式[6]如图1所示。

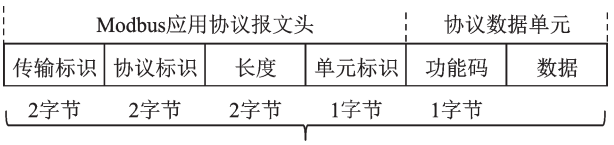

图1　Modbus TCP的报文格式

Fig. 1　Message format for Modbus TCP

1.2　Modbus TCP安全性分析

Modbus TCP协议由Modbus协议与TCP/IP融合而成,不仅未能解决原Modbus协议设计存在的安全隐患,甚至还引入了TCP/IP协议的安全缺陷[7],如:

(1)缺乏认证机制[8]。任意客户端只要与服务器端网络互通,并可对服务器端发送指令。攻击者只需接入网络中,便可对服务器发送恶意指令。

(2)无权限管理[9]。所有用户均拥有相同权限,可执行任意指令,如误操作发送了重启或关机等高危命令,服务器端仍能正常响应。

(3)数据篡改。攻击者可以通过截获数据包,并篡改相应字段,从而实现网络攻击。

(4)数据明文传输。Modbus TCP协议以明文方式传输数据,一些敏感信息很容易被攻击者获取,攻击者可以通过收集相关信息为将来攻击系统作准备[10]。

(5)重放攻击。Modbus TCP缺乏防重放机制,攻击者可以反复发送截获的数据包,从而破坏系统的稳定性。

2　Modbus-S协议设计

2.1　Modbus-S协议格式

Modbus-S协议以原Modbus TCP协议为基础,通过添加相应字段,实现工控系统的通信安全。其协议格式如图2所示。

2.2　同步机制实现原理

通过利用哈希算法的单向性原理实现数据同步,其实现原理如下所示:

(1)首先取两个随机数依次作为种子$a_{i,1}$和安全因子b_i,每一对通信对象都拥有对应的种子与安全因子,i为其编号。$V_{i,1}$为$(a_{i,1}+b_i)$进行哈希计算的值,$F(x)$的值则为x的首个字节数据,其作为同步标

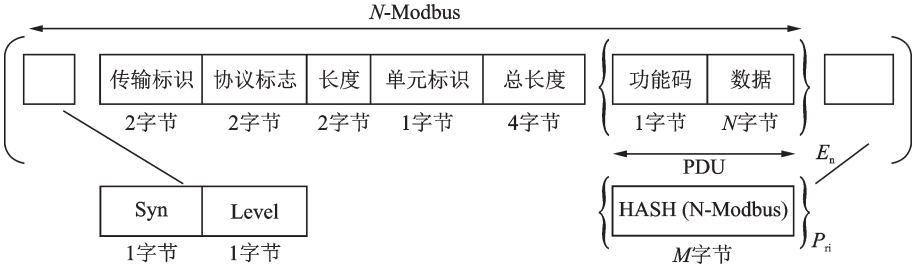

图2 Modbus-S协议格式

Fig.2 Modbus-S protocol format

识字段 $\mathrm{Syn}_{i,1}$ 的值。

$$V_{i,1}=\mathrm{Hash}(a_{i,1}+b_i)\quad i=1,2,\cdots \tag{1}$$

$$\mathrm{Syn}_{i,1}=F(V_{i,1})\quad i=1,2,\cdots \tag{2}$$

(2)若同步标识匹配成功后,则将当前哈希值与安全因子进行异或运算,然后求其哈希值,得到 $V_{i,2}$,同时取其首字节作为 $\mathrm{Syn}_{i,2}$。

$$V_{i,2}=\mathrm{Hash}(V_{i,1}+b_i)\quad i=1,2,\cdots \tag{3}$$

$$\mathrm{Syn}_{i,2}=F(V_{i,2}+b_i)\quad i=1,2,\cdots \tag{4}$$

(3)为防止攻击者发送具有相同同步标识的数据包,破坏同步性,需要重复步骤(2)操作以确保每次在网络中传输的同步标识均不相同。得到 $V_{i,3}$ 和 $\mathrm{Syn}_{i,3}$,将 $\mathrm{Syn}_{i,3}$ 作为下次发送的同步标识码。

(4)使用相同方法得到每次通信的同步标识码。

通信双方通过匹配同步标识码,确定数据的唯一性。由于哈希算法的单向性,攻击者截获数据包,无法构造下一次发送的同步标识码。同时有安全因子的加入,以及数据包中不含有完整的哈希值,这也极大地提升了同步标识的安全性。

2.3 功能码管理机制

通过设定“白名单”过滤规则实现对功能码的有效管理,其规则模型[11]如图3所示。

Level	IP地址	设备ID	功能码

图3 “白名单”规则模型

Fig. 3 Rule model of "white list"

“白名单”过滤规则以Level, IP地址、设备ID以及功能码作为过滤对象。Level字段的值用于进行角色划分,如root, admin和monitor。root权限最高,可执行任意指令;admin的权限次于root,只拥有线圈与寄存器值的读写权限;monitor的权限最低,只可监视线圈或寄存器状态。多个用户也可以设置相同的权限等级,另外通过绑定MAC地址可以防止ARP攻击,提升网络的安全性。采用结构体数组方式存储“白名单”列表。每一条“白名单”规则对应结构体数组中的一个结构体,其参数由用户事先设定。

3 Modbus-S协议系统的设计与实现

3.1 Modbus-S协议系统实现原理

Modbus-S协议系统通过自己开发的一对通信软件Modbus-S client/server实现数据的安全通信,以负责Modbus TCP与Modbus-S之间的协议转换,其实现原理如图4所示。

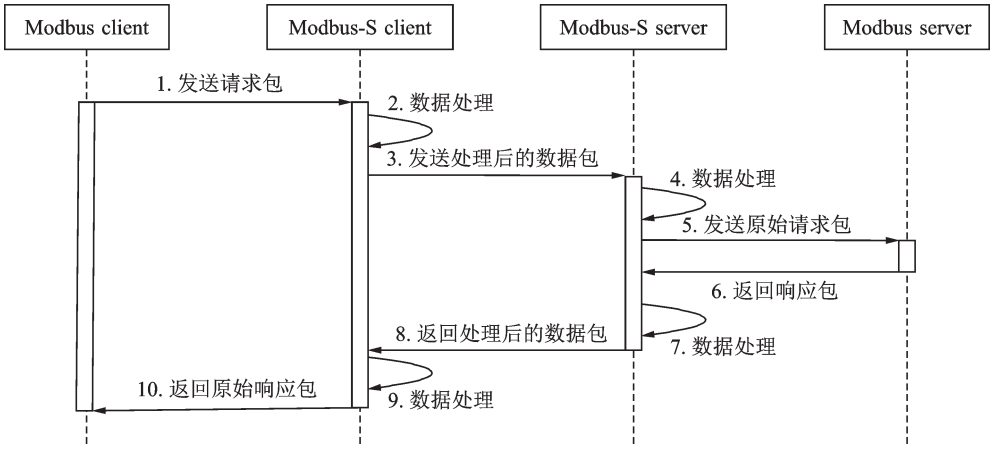

图4　Modbus-S协议系统实现原理

Fig. 4　Implementation principle of Modbus-S protocol system

3.2　Modbus-S协议数据处理过程

Modbus-S协议的数据处理由Modbus-S client与Modbus-S server实现,其处理过程为:

(1)Modbus client发送Modbus请求包(M_{req});

(2)Modbus-S client接收到M_{req},按照式(5,6)构造Modbus-S请求包C,并发送给Modbus-S server端,其中各字段含义如下所示。

Syn:同步标识;Level:权限等级;T_{ID}:传输标识;P_{ID}:协议标识;L:长度;U_{ID}:单元标识;L_t:加密后的PDU总长度;E_n:对称密钥;P_{ri}:私钥。

$$N-\mathrm{Modbus}=\mathrm{Syn}\,|\,\mathrm{Level}\,|\,T_{ID}\,|\,P_{ID}\,|\,L\,|\,U_{ID}\,|\,L_t|\{PDU\}\,E_n \tag{5}$$

$$C=[\,N-\mathrm{Modbus}\,]\{\mathrm{Hash}(N-\mathrm{Modbus})\}\,P_{ri} \tag{6}$$

(3)Modbus-S server接收到请求包C后,首先计算本地的同步标识码,将其与请求包中的同步标识码进行匹配,若匹配成功则进行签名认证,其次再进行"白名单"粗过滤,即匹配Level,IP与设备ID字段的值。然后再对PDU进行解密,最后进行"白名单"细过滤,即匹配Level, IP, 设备ID与功能码的值。返回其结果True或False。

$$R=\mathrm{Check}\left(\mathrm{Syn}_{sc},\mathrm{Syn}_{ss}\right)\&\mathrm{Auth}(C)\&\mathrm{WhiteListCheck}(C) \tag{7}$$

(4)只有当匹配结果为True时,才会构造原始请求包M_{req}并转发,否则丢弃并告警。

(5)服务器端的响应包采用相同方法进行处理。

4　实验与分析

4.1　实验环境

实验以4台虚拟机与本地主机为环境,虚拟机与本地主机均为windows 7系统,使用Modbus poll/slave分别模拟Modbus TCP客户端与服务器端,使用自己开发的Modbus-S client/server分别模拟Modbus-S客户端与服务器端。虚拟机模拟Client端,本地主机模拟服务器端。其中3台虚拟机安装有Modbus poll与Modbus-S client。本地主机安装有Modbus slave与Modbus-S server。其中PC_1, PC_2, PC_3均加入"白名单"列表,权限等级依次为100, 50, 10。其实验环境如图5所示。

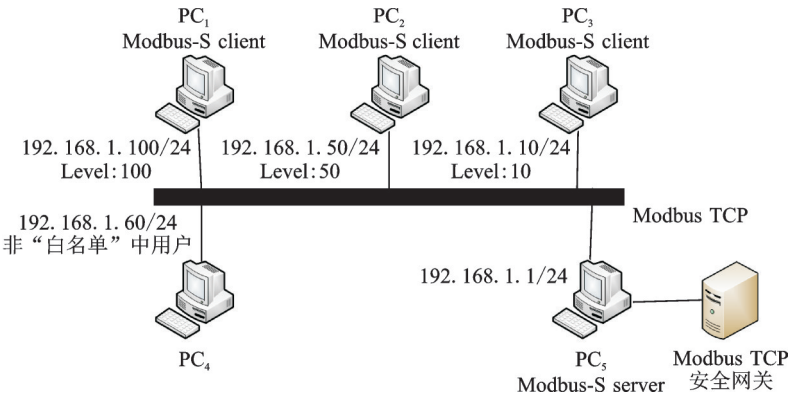

图5 实验环境图

Fig. 5 Experimental environment diagram

4.2 Modbus-S窃听攻击测试

实验使用Wireshark抓取Modbus-S协议正常通信时的数据包进行分析。图6为Modbus-S请求包的ADU数据,图7为Modbus-S响应数据包ADU数据,由图可知数据的关键字段已被加密,测试结果符合预期。

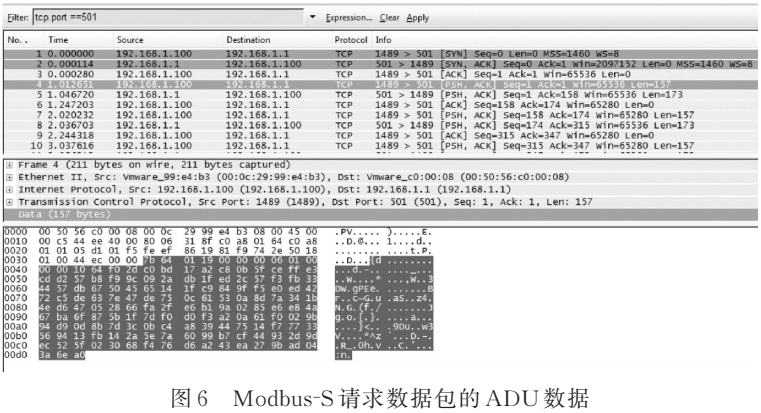

图6 Modbus-S请求数据包的ADU数据

Fig. 6 ADU data of Modbus-S request packet

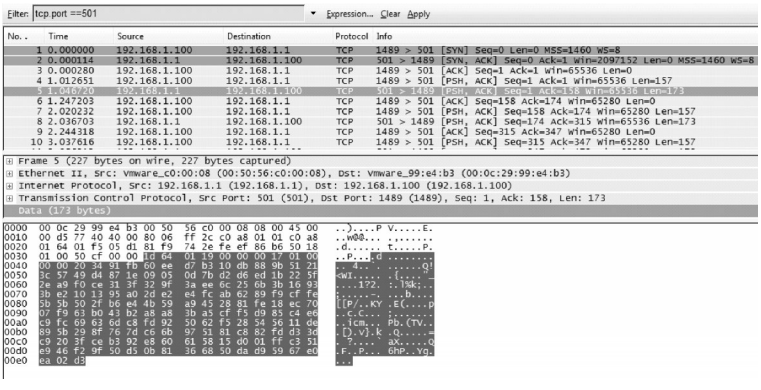

图7 Modbus-S响应数据包的ADU数据

Fig. 7 ADU data of Modbus-S response packet

4.3　“白名单”过滤测试

表1为实验测试的“白名单”列表,表2为测试结果,数据通信数据包如图8所示,图9显示了告警日志。由实验结果可知“白名单”过滤方法可以有效地实现非法指令的过滤。

表1　实验测试“白名单”列表

Tab. 1　"White list" of experimental test

Level	IP	Function	UnitID
100	192.168.1.100	All	All
50	192.168.1.50	1-6,F,10H	All
10	192.168.1.10	1-4	All

表2　“白名单”实验测试结果

Tab. 2　Results of "white list" test

PC	IP	FunctioID	UnitID	Result
PC_1	192.168.1.100	3	9	Receive
PC_1	192.168.1.100	6	9	Receive
PC_4	192.168.1.60	3	6	Discard and alert
PC_4	192.168.1.60	6	6	Discard and alert
PC_2	192.168.1.50	3	5	Receive
PC_2	192.168.1.50	6	5	Receive
PC_3	192.168.1.10	3	1	Receive
PC_3	192.168.1.10	6	1	Discard and alert

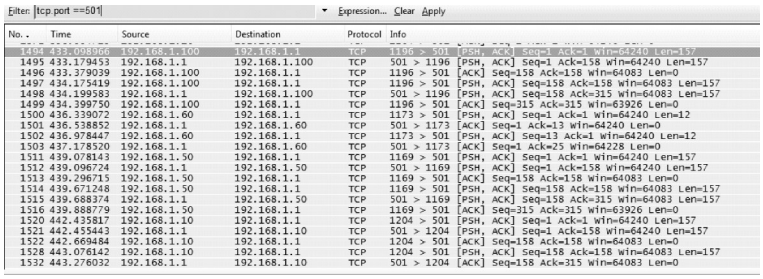

图8　数据通信数据包

Fig. 8　Data communication packet

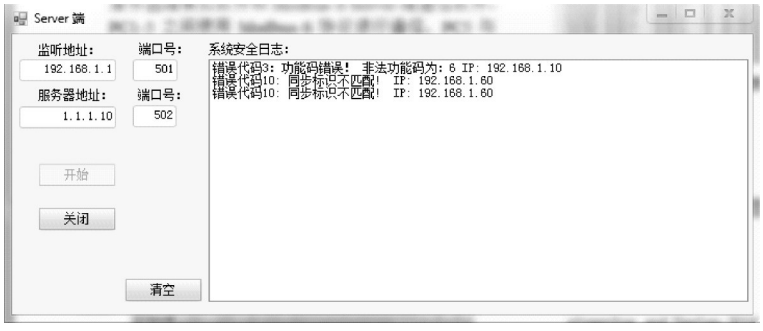

图9　Modbus-S server端告警记录

Fig. 9　Alarm record of Modbus-S server

4.4 Modbus-S时间性能分析

实验以使用最广泛的信息摘要算法5(Message digest algorithm 5,MD5)、高级加密标准(Advanced encryption standard,AES)算法以及非对称加密(Rivest-Shamir-Adleman,RSA)数字签名算法进行分析。通过wireshark抓取通信链路的数据包,通过计算响应包与请求包的数据差值得到如图10所示的时间对比图。该图反映了Modbus-S协议进行一次通信所消耗的时间。通过对比图可知Modbus-S的数据包传输时间比Modbus TCP协议增加8 ms左右,比文献[5]增加2 ms左右。与提高安全性相比,这种差异可以忽略不计。

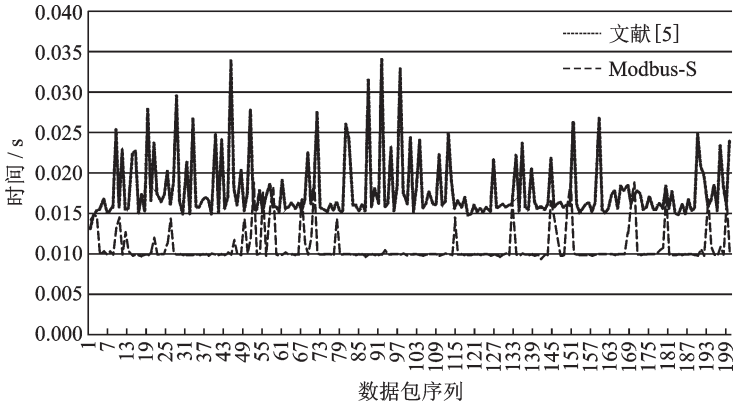

图10 Modbus-S数据包构造与解析时间对比图

Fig. 10 Time comparison chart of Modbus-S data packet construction and parsing

5 结束语

针对Modbus TCP协议存在的安全问题,本文通过开发一对通信软件并设计安全的通信协议Modbus-S,实现了Modbus TPC协议的安全加固。由于原客户端通常为计算机,可直接部署相应软件处理数据,而服务器端通常为安全网关,需要借助其他终端部署对应软件。为降低实施成本,还需研究相应的硬件模块,这将是下一步需要研究的方向。

参考文献:

[1] 高栋梁.MODBUS TCP/IP协议防火墙的研究与实现[D].北京:北京邮电大学,2015.
Gao Dongliang. Research and implementation of MODBUS TCP/IP protocol firewall[D]. Beijing: Beijing University of Posts and Telecommunications, 2015.

[2] Shang Wenli, Qiao Quansheng, Wan Ming, et al. Design and implementation of industrial firewall for modbus/TCP[J].Journal of Computers,2016, 11(5): 432-438.

[3] 尚文利,雷艳晴,万明,等.基于哈希算法的工业防火墙规则自学习方法[J].计算机工程与设计,2016, 37(12): 613-617.
Shang Wenli, Lei Yanqing, Wan Ming, et al. Self-learning method for industrial firewall rules based on hash algorithm[J].Computer Engineering and Design, 2016,37(12): 613-617.

[4] 吕雪峰,蒋烈辉,孟奂.基于MODBUS的SCADA系统网络威胁与入侵检测[J].计算机工程与应用,2017,53(24): 122-128.
Lv Xuefeng, Jiang Liehui, Meng Huan. Cyber threats and intrusion detection for MODBUS-based SCADA system[J]. Computer Engineering and Applications, 2017, 53(24): 122-128.

[5] Fovino I N, Carcano A, Masera M, et al. Design and implementation of a secure modbus protocol[C]//International Conference on Critical Infrastructure Protection. Berlin, Heidelberg: Springer, 2009: 83-96.

[6] Goldenberg N, Wool A. Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems[J]. International Journal of Critical Infrastructure Protection,2013,6(2): 63-75.

[7] 蔡宇晴.SCADA系统中Modbus TCP/IP协议的异常检测研究[D].北京:北京交通大学,2017.
Cai Yuqing. Research on anomaly detection of Modbus TCP/IP protocol in SCADA systems[D]. Beijing:Beijing Jiaotong University,2017.

[8] 程超.工业控制网络Modbus TCP协议深度包检测技术研究与实现[D].成都:电子科技大学,2016.
Cheng Chao.Research and implementation of deep packet inspection of Modbus TCP on industrial control network[D]. Chengdu: University of Electronic Science and Technology of China,2016.

[9] 万明,尚文利,曾鹏,等.基于功能码深度检测的Modbus/TCP通信访问控制方法[J].信息与控制,2016,45(2): 248-256.
Wan Ming,Shang Wenli,Zeng Peng, et al. Modbus/TCP communication control method based on deep function code inspection[J].Information and Control,2016, 45(2): 248-256.

[10] 胡爱群,李古月.无线通信物理层安全方法综述[J].数据采集与处理,2014,29(3): 341-350.
Hu Aiqun,Li Guyue.Physical layer security in wireless communication:Survey[J].Journal of Data Acquisition and Processing, 2014,29(3): 341-350.

[11] 张仁斌,李思娴,刘飞,等.基于Modbus功能码细粒度过滤算法的研究[J].计算机应用研究,2018,35(1): 277-281.
Zhang Renbin, Li Sixian, Liu Fei, et al. Research on fine grained filtering algorithm based on Modbus function code[J].Application Research of Computers,2018,35(1): 277-281.

作者简介:

罗旋(1993-),男,硕士研究生,研究方向:工控网络安全,E-mail: 851033149@qq.com。

李永忠(1961-),男,教授,硕士生导师,研究方向:计算机网络通信与安全、信息安全和嵌入式系统应用等。

(编辑:王静)