文章编号:1671-4598(2023)11-0187-05 DOI:10.16526/j.cnki.11—4762/tp.2023.11.028 中图分类号:TP391 文献标识码:A

基于 Modbus/TCP 的无线通信网络安全加密控制系统设计

谢跃伟
(中国航发 四川燃气涡轮研究院,成都 610500)

摘要:为控制明文加密时长、密文响应时长之间的相对时延量,实现无线网络对于通信数据的安全性加密,设计基于 Modbus/TCP 的无线通信网络安全加密控制系统;匹配 PowerPC 嵌入式架构与复位通信控制电路之间的实时连接关系,借助微处理器子模块,确定宿主机与客户机对通信网络的贡献价值,再按照 Modbus/TCP 协议连接标准,整合交换区中已存储的通信数据文本,完成无线通信网络安全加密控制系统硬件设计;根据基本协议要素,认证待加密数据的传输身份,实现对 Modbus/TCP 可信协议的定义;利用协议文件中的可信度条件,设置密钥模板,通过移植处理通信文本的方式,确定数据信息样本的扩容总量,完成安全加密接口设计,联合相关应用元件,实现基于 Modbus/TCP 的无线通信网络安全加密控制系统设计;实验结果表明,所设计系统明文加密时长、密文响应时长之间的相对时延量始终保持为 0.1 ms,能够有效实现无线网络对于通信数据的安全性加密。

关键词:Modbus/TCP 协议;无线通信网络;安全加密控制系统;PowerPC 架构;文本移植;数据扩容;相对时延量

Design of Wireless Communication Network Security Encryption Control System Based on Modbus/TCP

XIE Yuewei
(AECC Sichuan Gas Turbine Establishment, Chengdu 610500, China)

Abstract: In order to control the relative delay between plaintext encryption duration and ciphertext response duration, and realize the security encryption of communication data in wireless networks, a security encryption control system for wireless communication networks based on Modbus/TCP is designed. The real-time connection relationship is matched between the PowerPC embedded architecture and reset communication control circuit, the contribution value of the host and client to the communication network is determined with the help of the microprocessor sub module, according to the Modbus/TCP protocol connection standard, and then the communication data text stored in the switching area is integrated to complete the hardware design in the wireless communication network security encryption control system. By the basic protocol elements, the transmission identity of the data to be encrypted is authenticated to define the Modbus/TCP trusted protocol. The credibility conditions in the protocol file is used to set the key template, determine the total capacity expansion of the data information samples by transplanting and processing the communication text, complete the design of the security encryption interface, and combine with the relevant application components to achieve the design of the security encryption control system in the wireless communication network based on Modbus/TCP. The experimental results show that the relative delay between plaintext encryption duration and ciphertext response duration of the designed system is always maintained within 0.1 ms, which can effectively realize the security encryption of communication data in wireless networks.

Keywords: Modbus/TCP protocol; wireless communication network; security encryption control system; PowerPC architecture; text migration; data expansion; relative time delay

0 引言

无线通信网络是指不需借助基础布线就可以建立通信设备互联关系的应用网络,由于网络体系的复杂程度较低,所以通信数据的传输具有较强自由性。明文、密文是无线通信网络中两种最基本的数据样本,二者响应时长之间的相对时延量决定了网络体系对于通信数据的安全加密能力。因此,对无线通信网络安全加密控制系统进行研究具有重要意义。

文献[1]设计的基于 MATLAB 与 OptiSystem 的光混沌保密通信系统具有两个时延反馈闭环,可以根据通信数据的混沌波形,确定输入信号与输出信号的差异性,再联合二进制序列条件,实现对加密模板的精准定义。文献[2]设计的多中继物理层网络编码加密系统,根据通信数据的单位吞吐率,确定信息样本的传输方案,由于 LDPC 码、中继映射码取值不可能相同,所以该系统对于不同通信数据的加密标准也有所不同。然而上述两类系统对于明文加密时长、密文响应时长之间相对时延量指标的控制能

收稿日期:2023-01-04; **修回日期**:2023-03-06。
作者简介:谢跃伟(1985-),男,大学本科,工程师。
引用格式:谢跃伟. 基于 Modbus/TCP 的无线通信网络安全加密控制系统设计[J]. 计算机测量与控制,2023,31(11):187-191,211.

力有限，不符合安全加密无线网络通信数据的应用需求。

Modbus 是一种串行式的通信连接协议，存在于以太网、互联网、串口组织等多个版本的网络体系之中，与其他类型的通信协议相比，该协议的主要内容都是在物理层网络中实现的[3]。由于互联网组织对于通信数据传输行为并不设置明确要求，所以应用 Modbus 协议后，网络节点更易于部署与维护，对宿主供应主机而言，本地数据字节的修改也不受到特殊限制条件的影响。TCP 是基于字节流所设置的传输层通信协议，接受 IETF 主机的直接定义。该类型协议文本的应用，要求通信网络主机必须同时关联下级通信设备，一方面控制数据文本使其能在既定时间内传输至目标通信位置，另一方面也可以保障网络信道的传输宽度与广度，使得数据信息的传输速率水平得到大幅提升[4]。若通信网络布局环境较为复杂，则可以建立 Modbus 与 TCP 共同配合的协议作用机制。为此，本文设计了基于 Modbus/TCP 的无线通信网络安全加密控制系统。

1 无线通信网络安全加密控制系统硬件设计

无线通信网络安全加密控制系统的硬件由 PowerPC 嵌入式架构、微处理器子模块、复位通信控制电路、宿主机与客户机模式、数据交换区域五部分共同组成，本章节将针对相关硬件设备结构的设计方法展开深入研究。

1.1 PowerPC 嵌入式架构

在无线通信网络安全加密控制系统中，PowerPC 嵌入式架构同时负载宿主机与客户机的接入请求，既可以接收复位通信控制电路输出的电量信号，也能够干预数据交换区组织对信息样本的存储能力，因此完善架构体系连接模型，是保障无线网络对于通信数据进行安全性加密的必要环节[5]。为适应嵌入式连接需求，Power 单元、PC 单元必须接受无线通信网络主机的统一调度，特殊情况下，前者可自动暂停串口功能模块与通信功能模块的运行，将 PCI 功能模块独立出来，使其在处理通信数据时能够准确分析 Linux 内核中信息样本的实时寄存量，从而正确干预 QEMU 虚拟机中的数据加密编码行为。PC 单元内负载了 SRAM、PCI Slot、Device、Net Card 四类应用模块，且它们之间保持数据互通关系，过渡单元向外输出通信数据时，未被完全利用的信息样本可暂时寄存于该单元组织之中，且数据样本存储量会随着应用模块的运行而不断减少[6]。PowerPC 嵌入式架构模型如图 1 所示。

过渡单元具有双向数据传输能力，但为保证无线通信网络中信息样本的单向传输特性，要求已被分配于 Power 单元与 PC 单元中的数据参量不得进行二次传输。

1.2 微处理器子模块

微处理器子模块对安全加密指令控制行为的实现需要 PWM 处理器、SHAMD 设备、CAN 设备、UART 设备的共同配合。整个子模块单元包括 EEPROM、SSI、QEI 等多条数据通路。其中，EEPROM 通路将 CRC 通信数据导流入 MODULE1 存储设备中，CRC 通信数据的传输功耗水平较低，对于微处理器子模块而言，该类型数据样本的存储

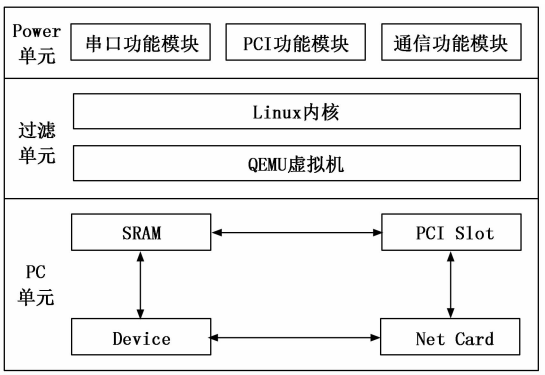

图 1 PowerPC 嵌入式架构模型

量越大，就表示子模块体系的运行稳定性越强。SSI 通路将 AES 通信数据导流入 MODULE2 存储设备中，AES 通信数据的初始输出位置为 Linux 内核、目标传输位置为 SRAM 应用模块，整个传输过程中 SSI 通路仅对信息参量进行整合处理，不干扰这些数据的实际传输行为[7-8]。QEI 通路将 GPIO 通信数据导流入 MODULE3 存储设备中，GPIO 通信数据的传输速率较快，因此 QEI 通路必须具备较强的数据承载能力。微处理器子模块的功能性布局形式如图 2 所示。

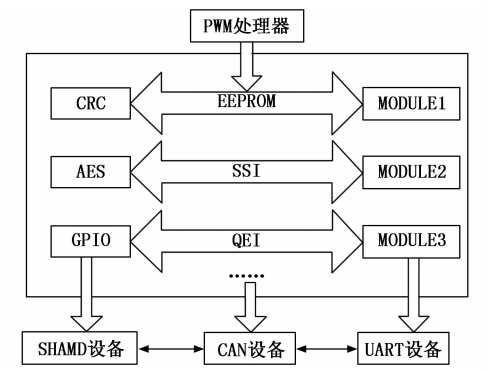

图 2 微处理器子模块的功能性框图

SHAMD 设备、CAN 设备、UART 设备分别对应通信数据、数据通路与数据存储设备，在微处理器子模块中，接受 PWM 处理器的统一调控，但为保证通信数据安全加密指令的顺利执行，在编码数据的过程中，信息参量的传输方向始终保持一致。

1.3 复位通信控制电路

复位通信控制电路将＋VCC 端电极与 GND 端电极连接在一起，可以借助 L、R、C 等多类型电子元件，对负载电流、负载电压进行分配处理，在满足频分处理器（Q）对于电量信号的消耗需求的同时，确保 Reset 变压设备不会出现跳频通信的情况，从而使得数据样本在无线通信网络中能够保持稳定且快速的传输状态，具体结构如图 3 所示。

左侧电量回路包括 3 个阻值不完全相同的感应电阻元件，通常情况下，连接于主线单元的 R1 电阻的阻值水平较高，数值上基本等于 R2、R3 电阻的阻值之和[9]。L 是对通信数据极为敏感的电量感应装置，可以根据 R 电阻两端负载电压的数值情况，调节频分处理器中通信数据样本的额

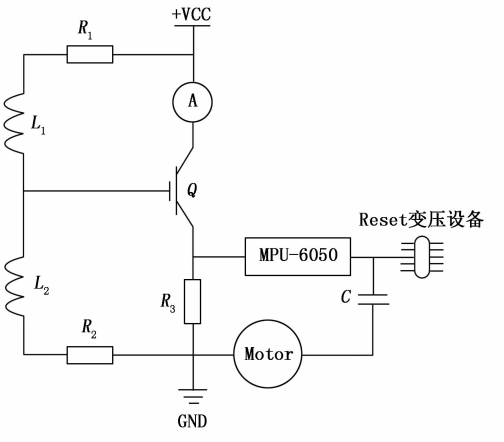

图 3　复位通信控制电路结构图

定存储数量，一方面可以维持整个电量回路中传输电流的数值稳定性，另一方面也可以避免通信数据在 MPU-6050 设备中大量累计。

Motor 集合器可对无线通信网络中的数据信息进行聚合处理，并能够在 Modbus/TCP 可信协议的作用下，将这些数据参量再次分配给下级应用设备[10]。

1.4　宿主机与客户机

宿主机与客户机模式是无线通信网络安全加密控制系统的设计基础，由宿主机设备、客户机设备两部分组成。

1.4.1　宿主机

宿主机是 Linux 内核的外接设备，在 Modbus/TCP 可信协议作用下，可以保持较长时间的自主运行状态，为适应无线通信网络对于数据信息样本的安全性加密处理需求，该结构运行所需电量信号全部来自复位通信控制电路。核心单元中，Network 宿主设备、Moudle 宿主设备保持交叉连接关系，前者负责对通信数据进行镜像加密处理，后者则负责清空通信磁盘中暂存的数据信息参量[11]。整个单元模块同时关联通信网关与无线网络 IP 地址，可以在 Windows 通信主机的作用下，设置全新的码源模板，当 DNS 密码符合码源模板定义标准时，宿主机设备会自发建立与下级客户机设备的通信连接关系。宿主机连接模板如图 4 所示。

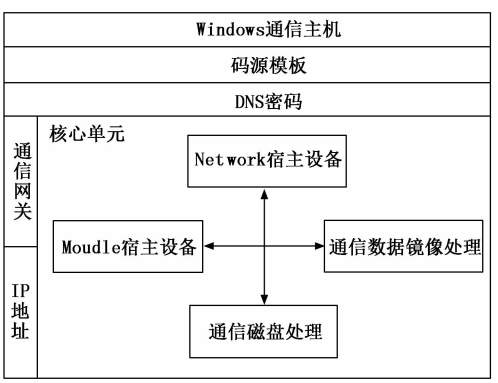

图 4　宿主机连接模板

1.4.2　客户机

客户机设备的运行模式必须与宿主机设备完全匹配，由于 Modbus/TCP 可信协议要求通信数据的传输方向必须符合一致性原则，所以实施机密处理的过程中，信息样本的传输方向只能由宿主机端指向客户机端[12]。

1.5　数据交换区

数据交换区是以宿主机与客户机模式为基础设置的独立信息处理区域，接收复位通信控制电路输出的电量信号，在无线通信网络环境中，与微处理器子模块保持同等级连接关系，随着待加密数据样本总量的增大，该区域已接入部分面积会不断增大，但由于整个区域的可用面积有限，故而当交换区域内数据样本的实际存储量达到极值条件时，无线通信网络主机对于数据信息样本的加密处理速率也会开始不断下降[13-14]。数据交换区的连接原理如图 5 所示。

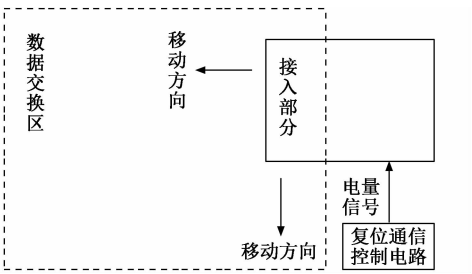

图 5　数据交换区连接原理

实施通信数据加密处理时，交换区组织的外向扩张行为遵循双向性规则，即已接入部分在横、纵两个方向上同时向着外部交换区组织进行扩展，整个处理过程中，已接入部分所存储通信数据总量不断增大，但无线网络主机对于这些信息参量的加密编码原则完全遵循 Modbus/TCP 可信协议。

2　Modbus/TCP 可信协议

加密控制系统的运行必须遵循 Modbus/TCP 可信协议，而对于协议内容的定义，则要在要素条件的基础上，对通信数据的加密身份进行认证处理。

2.1　基本协议要素

基本协议要素决定了 Modbus/TCP 可信协议对于通信数据加密模板样本的容纳能力，设置数据交换区域体系时，只有保证基本协议要素的完整性，才能激发无线网络主机对于通信数据样本的安全性加密处理能力[15]。对于基本协议要素的求解，涉及对基础构建参量的计算，具体定义如下：

$$\beta = \sqrt{\chi^2 - 1} \tag{1}$$

式中，χ 表示 Modbus/TCP 可信协议的完整性设置参数。

在公式（1）的基础上，设 q_1、q_2、…、q_n 表示 n 个不为零的通信数据编码系数，且 $q_1 \neq q_2 \neq \cdots \neq q_n$ 的不等式条件恒成立，q_{max} 表示全部通信数据编码系数的最大取值结果，δ 表示基于 Modbus/TCP 可信协议的通信数据筛选参量，α_1、α_2、…、α_n 分别表示与 n 个通信数据编码系数匹配的协议文件编码特征值，联立上述物理量，推导 Modbus/TCP 可信协议的基本协议要素表达式见公式（2）。

$$I = \frac{\beta \left\| q_{max}{}^2 - \delta(q_1 + q_2 + \cdots + q_n) \right\|}{\alpha_1 \cdot \alpha_2 \cdot \cdots \cdot \alpha_n} \tag{2}$$

无线通信网络主机在加密处理数据信息参量时，要求相关数据样本的选取必须满足同向性原则，对于 Modbus/TCP 可信协议文件而言，数据样本同向性避免了差异化信息取值结果的出现，可以在保持密钥模板编码稳定性的同时，对待处理信息参量进行按需定义，从而最大化缩短明文加密、密文响应的表现时长[16]。

2.2 加密身份认证

加密身份认证就是按照基本协议要素条件，求解网络主机对于通信数据的安全性加密处理原则，设计加密控制系统时，如果通信数据的身份信息不符合认证标准，不但会导致交换区组织失去对数据信息进行妥善处理的能力，还有可能造成宿主机、客户机模式出现混乱运行的情况[17-18]。假设 e 表示可信度参数，则关于参数 e 的可信作用条件为 $W(e)$，若以 Modbus/TCP 协议作为加密编码标准，则有：

$$\begin{cases} -1 < W(e) \leqslant 1 \\ W(e) \neq 0 \end{cases} \tag{3}$$

式中，$W(e) \in (-1,0)$ 表示利用 Modbus/TCP 协议加密通信数据时，数据交换区运动方向与加密主机认证的正方向相反；$W(e) \in (0,1]$ 表示利用 Modbus/TCP 协议加密通信数据时，数据交换区运动方向与加密主机认证的正方向相同。设 γ 表示 Modbus/TCP 协议中数据信息样本编码参数，$\varphi_{\max}$ 表示加密码源占比系数的最大取值，$\varphi_{\min}$ 表示加密码源占比系数的最小取值。在上述物理量的支持下，联立公式（2）、公式（3），可将基于 Modbus/TCP 可信协议的通信数据加密身份认证表达式定义为：

$$R_{\varepsilon} = \frac{(\gamma-1)^2}{\sqrt{|\varphi_{\max}|^2 - |\varphi_{\min}|^2}} \times \left| \frac{1}{W(e)} I \right|_{I \geqslant 1} \tag{4}$$

由于无线通信网络在单位时间内所能容纳的数据样本总量有限，所以安全性加密控制系统的设计，还要求认证表达式的计算取值应属于 $(1,+\infty)$ 的数值区间。

3 安全加密接口设计

安全加密接口按照 Modbus/TCP 可信协议，对通信数据参量进行深度编码处理，具体接口设计流程如下。

3.1 密钥模板

密钥模板是无线通信网络安全加密控制系统处理数据样本时所遵循的加密原则，对于系统接口组织而言，模板体系的开放程度固定，随着通信数据样本的不断累积，码源节点所处位置不会发生变化，系统在对其进行编码处理时，不需额外消耗时间完成对密钥指令的定义，故而明文加密时长、密文响应时长都能得到较好控制，二者之间的相对时延量也就不会超过预期长度数值[19-20]。模板体系的定义要求所选取的源向量必须处于同一数据交换区组织内，但又不能完全相等。如 s、a 是既定数据交换区内两个不相等也不等于零的源向量，关于源向量的密钥参数分别为 d_s、d_a，φ 表示明文样本、密文样本之间的相互转码系数，联立公式（4），推导无线通信网络安全加密控制系统的密钥模板表达式为：

$$\hat{u} = \sum_{\varepsilon=1}^{+\infty} R_{\varepsilon} \prod_{\substack{s\neq 0 \\ a\neq 0}} f\left(\frac{1}{d_s \pm d_a}\right)^{1/\varphi^2} \tag{5}$$

其中：f 表示密钥模板对于通信数据的编码权限，ε 表示数据文本编码参量的初始取值。对于无线通信网络安全加密控制系统而言，只有保证密钥模板的完整性，主机元件才能实现对数据样本的准确编码。

3.2 通信文本移植

所谓文本转移就是将通信数据文本由一个存储位置转移到另一个存储位置。Modbus/TCP 协议要求，文本信息转移过程中通信路径传输宽度必须完全相等，且信息参量的每一次对接都需符合密钥模板的编码原则[21]。移植处理的目的就是为了扩大通信文本所能达到的传输区域，在密钥模板内码源样本类型不发生变化的情况下，数据参量在无线通信网络中所能到达的交换区组织越多，就表示系统主机对于安全性加密指令的控制能力越强[22]。设 λ 表示无线通信网络中的数据传输路径配置系数，$\bar{h}$ 表示待编码通信数据样本的单位累积量，ΔT 表示加密指令的单位执行时长，k' 表示安全性加密系数，联立上述物理量，推导通信文本移植表达式如公式（6）。

$$G = \lambda \hat{u} - (\bar{h}^2 + k' \mid \Delta T \mid) \tag{6}$$

为保证系统主机对于通信数据样本的处理能力，文本移植表达式的定义还需参考密钥模板的实际求解结果。

3.3 数据扩容

数据扩容就是提升网络主机对通信数据的存储能力，实施加密处理时，大容量的数据存储空间表示系统主机在单位时间内所能编码的信息总量更多[23-24]。$\bar{j}$ 表示基于 Modbus/TCP 协议所选取的通信数据扩容系数，其计算式如下：

$$\bar{j} = \frac{G}{\kappa - 1} \tag{7}$$

式中，κ 表示标准数据存储系数。在公式（7）的基础上，设 μ 表示目标加密参数，l 表示安全性判别条件，$\vec{x}$ 表示通信数据在无线网络环境中的传输映射向量，联立上述物理量，可将数据扩容表达式定义为：

$$Z = \frac{l^2 \sqrt{\mu \bar{j}}}{x} \tag{8}$$

如果数据扩容条件达不到控制系统的实际应用标准，无线通信网络在加密数据样本时可能会出现非安全性处理的情况。

4 实验分析

为验证设计的基于 Modbus/TCP 的无线通信网络安全加密控制系统的有效性，本次实验判断无线网络主机对于通信数据的安全性加密能力，在不考虑其他干扰条件的情况下，加密能力的考量可以参考明文加密时长、密文响应时长之间的相对时延量，具体实施环节选择所设计系统、文献［1］系统和文献［2］系统 3 种方法。

4.1 网络布局

以 Windows 主机作为核心数据处理器，将无线通信网络布局作为实验环境，无线通信网络布局形式如图 6 所示。

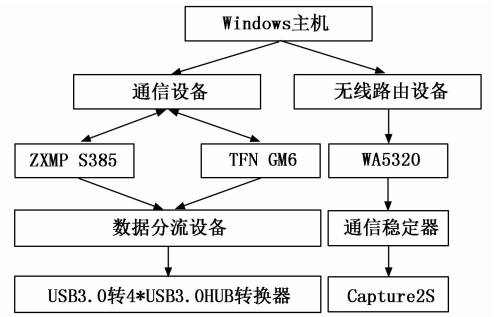

图 6　无线通信网络布局形式

借助 USB3.0 转 4 * USB3.0HUB 转换器完成对通信数据的分流处理，再以此为基础，将 ZXMP S385 通信设备、TFN GM6 通信设备连接起来，从而为通信数据提供一个相对稳定的传输空间。将 WA5320 型无线路由设备与 Capture2S 型通信稳定器串联起来，利用 Windows 主机搭载的控制系统对已输出的通信数据进行加密处理，并记录明文加密时长、密文响应时长的具体数值结果。

完成网络环境布局后，首先利用实验组系统（所设计系统）对 Windows 主机输出的通信数据进行加密处理，所得加密时长、密文响应时长作为实验组变量；然后利用对照组（a）系统（文献［1］系统）对 Windows 主机输出的通信数据进行加密处理，所得加密时长、密文响应时长作为对照组（a）的实验变量；其次利用对照组（b）系统（文献［2］系统）再次重复上述实验步骤，所得时长数据作为对照组（b）的实验变量；分析所得实验数据，总结实验规律。

4.2　实验结果与讨论

明文加密时长、密文响应时长之间的相对时延量可以反映出无线网络对于通信数据的安全性加密能力，在图 6 所示无线通信网络环境中，相对时延量的计算数值越小，就表示无线网络对于通信数据的安全性加密能力越强。

实验组、对照组明文加密时长与密文响应时长的具体实验数值分别如图 7 和图 8 所示。

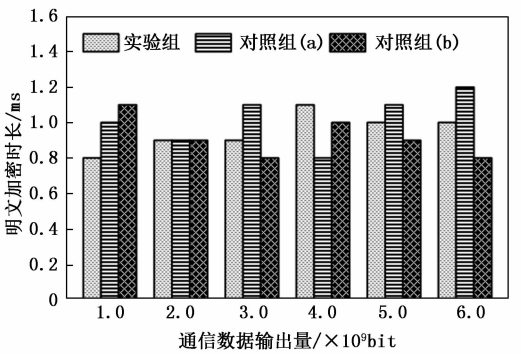

图 7　明文加密时长

对照图 7、图 8 对明文加密时长、密文响应时长之间的相对时延量进行计算，具体数值如表 1 所示。

根据表 1 可知，整个实验过程中，实验组明文加密时长、密文响应时长之间的相对时延量始终保持为 0.1 ms；

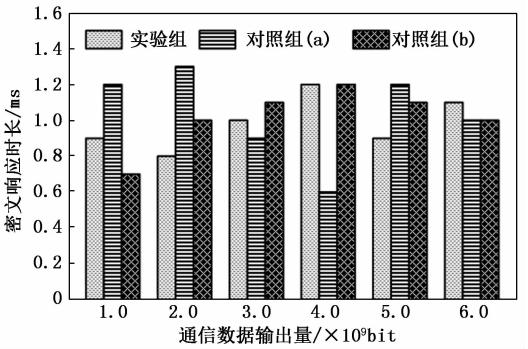

图 8　密文响应时长

对照组（a）相对时延量的最大取值为 0.4 ms、最小取值为 0.1 ms，平均相对时延量为 0.2 ms，高于实验组数值；对照组（b）相对时延量的最大取值为 0.4 ms、最小取值为 0.1 ms，平均相对时延量为 0.2 ms，也高于实验组数值。

表 1　明文加密时长与密文响应时长的相对时延量

通信数据输出量/×10⁹ bit	实验组/ms		对照组(a)		对照组(b)	
	实际数值	相对时延量	实际数值	相对时延量	实际数值	相对时延量
1.0	−0.1	0.1	−0.2	0.2	0.4	0.4
2.0	0.1	0.1	−0.4	0.4	−0.1	0.1
3.0	−0.1	0.1	0.2	0.2	−0.3	0.3
4.0	−0.1	0.1	0.2	0.2	−0.2	0.2
5.0	0.1	0.1	−0.1	0.1	−0.2	0.2
6.0	−0.1	0.1	0.2	0.2	−0.2	0.2

综合上述分析可知，文献［1］系统和文献［2］系统对于明文加密时长、密文响应时长之间相对时延量的控制能力有限，因此这两类系统在安全加密通信数据方面的应用能力也就不能完全满足实际应用需求；而所设计系统可以有效控制明文加密时长、密文响应时长之间的相对时延量，对于安全加密通信数据可以起到一定的促进性影响作用，可实现无线网络对于通信数据的安全性加密。

5　结束语

本文设计的无线通信网络安全加密控制系统在 Modbus/TCP 可信协议的基础上，针对控制明文加密时长、密文响应时长之间相对时延量过大的问题进行改进，联合 PowerPC 嵌入式架构、微处理器子模块、复位通信控制电路等多个硬件结构，定义完整的密钥模板，从而实现对通信文本的移植与扩容处理。所设计系统具有宿主机与客户机连接模式，能够在加密通信数据的同时，对其身份信息进行对应性认证，有效控制明文加密时长、密文响应时长之间的相对时延量，实现无线网络对于通信数据的安全性加密。

参考文献：

[1] 刘劲杨，周雪芳，毕美华，等. 光混沌保密通信系统在 MATLAB 与 OptiSystem 中的协同实现［J］. 光电工程，2021，48(9)：43－51.

（下转第 211 页）