Journal of Engineering Science and Technology Review 6 (1) (2013) 91-96

Research Article

JOURNAL OF
Engineering Science and Technology Review

www.jestr.org

Research and Implementation of Collision Detection Based on Modbus Protocol

Yinglan Fang*, Xianfeng Han and Bing Han

Department of Computer, North China University of Technology, Beijing, China

Received 25 June 2012; Accepted 15 January 2013

Abstract

In order to solve the communication errors resulted by traditional working condition multi-platform device communication using the custom protocol communication and link congestion malpractice brought by retransmission, it ensures network communication using time-sharing communication conflict detection based on mature Modbus protocol. Thereby it enhances the stability of the entire system during operation process, and provides simple, efficient, stable business specification interface for the future expansion of the system. After a comprehensive evaluation and analysis of system communication messages before and after improvement, system comprehensive evaluation target has improved. While the system is more flexible to modular design, develop transparent, structure open side and has a broad application prospects.

Keywords: Modbus Protocol, Time-sharing Communication, Conflict Detection, Protocol, Token

1. Introduction

In recent years, with the rapid popularization and development of science and technology, more and more computer technology in the industrial environment as a means of information management is applied to various fields. It spurs the construction of social information. With the continuous expansion of the system functionality and constantly renovation of the application technology in the process of the development, it makes the area more complicated. Industrial automation control process which using computer technology becomes fussier and more difficult. How to ensure normal communication and effective control between devices in different industrial equipment becomes one of solving problem in today's automation control field.

In industrial Ethernet, as the system master node the signal collector must be able to support multiple child nodes, but also it need to support concurrent things of the multiple child nodes. It allows high-speed sequential closing and re-opening connections among nodes, so it can quickly respond to the response without sent. To this concurrent inter-node access of the system, there are usually two ways to solve. The first is to use the embedded operating system. When a new connection requests, the operating system dynamically creates a task to maintain this connection. Namely each task maintains a connection, but the embedded operating system has higher hardware requirements and the kernel also consumes some CPU resources and the software's requirements are also higher. The second is the simulating multi-task system. The system pre-assigns a large data area to store the connection information and communications status for each client. Through an array or a pointer mode, it indexes and queries [1]. This method's software programming structure is more complex, data area seriously occupies hardware resources.

The paper utilizes Modbus protocol industrial network in a heterogeneous environment, abandons the traditionally communication mode which the upper computer uses polling detection methods. Using collision detection technology realizes the mutual communication between various devices. It not only avoids congestion on the network because of non-standard custom message, but also sends and receives a unified message to maximize the use of network resources. It provides a safe, simple and efficient means of communication between multiple types of platforms, many types of machine in the industrial field.

2. Traditional Heterogeneous Network Communication Status

The system consists of industrial control computer, wireless central workstation, remote data transmission radio, PLC control devices, hand-held remote control and different manufacturers of electronic scales and other a few parts; In addition to industrial control computer as upper computer places in the workshop office, other parts installs in multi-function crane to realize measurement control and data transmission in the production process. The main control unit applies Siemens programmable controller with electromagnetic compatibility.

It exist two wireless communication methods in the application environment, namely the upper computer communication by radio station and field control equipment. The communications simulates TCP/IP protocol principle and interacts using a custom message. In order to guarantee the correct reception of messages, the messages contain message header, sequence number, length, source device

* E-mail address: jlufangyl@163.com

ISSN: 1791-2377 © 2013 Kavala Institute of Technology. All rights reserved.

address, receiving device address, content, check digit and so on information. This led to on-line communication messages are generally more than 200 byte, if 1000M transmission distance is considered, Transmission and reception can not be guaranteed valid and correct transmission under interference of the strong magnetic field and strong electric field. In addition, the handheld remote control devices use Intel 8051 as the core and the scene controller Siemens PLC communication uses the free port communication [2], [3], [4].

Although the message length is relatively short, but because it has no message parity checks mechanism, so there cannot guarantee the correct message transmission. And PLC needs to maintain two sets of message protocols in order to guarantee with the communication between the upper computer and the remote control at the same time. Virtually it brings unnecessary trouble for the design and development of the PLC. If there is the addition of the new equipment involved, it will not be able to guarantee normal communication by message type expansion and can not expand device to system. It has tracked and counted the packet received from the upper computer in continuous two weeks. As in the spot environment is uncertain, so the correct messages and error messages do not occur according to a certain percentage.

But from Fig. 1, it sees for continuous 15 days received packets statistics, error packets occupied almost more than 40% for received packets per day. The average error packet is 38.62% for 15 days. In the 10th days, the statistic error rate is high as 84.85%. Of course, the packet error rate is very low in better environment conditions. In the 6th and 7th, statistics day correct rate is 100%. In the 13th and 14th, statistics day correct rate respectively reaches 94.59% and 92.30%. It indicates that the packet transmission error rate does not occur in the code technology implementation. It is shown in Fig. 2:

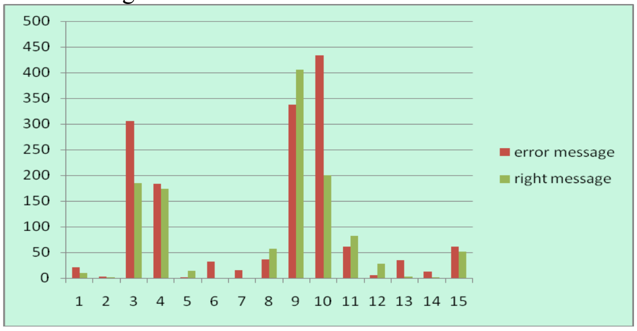

Fig. 1. Received packets correct number statistic

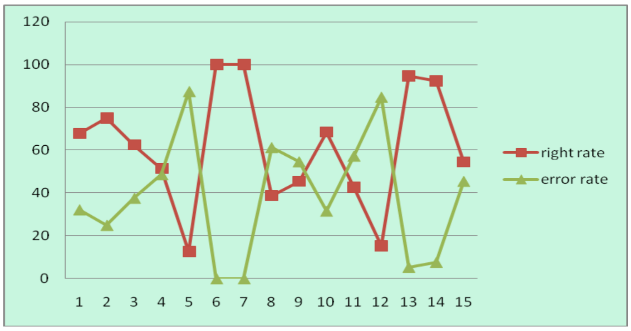

Fig. 2. Received packets correct rate statistic

It is seen for the results of the statistical analysis from the above messages for continuous 15 days. Using traditional custom packet transmission protocol, long-distance communication in packet transmission efficiency and effectiveness can not be guarantee when it faced with strong electromagnetic interference environment. How to improve the traditional packet transmission in order to meet the requirements of the scene it? In order to make the system enable to be normal and efficient operation, it must improve and optimize in the packet transmission mode.

3. Modbus Protocol Introduction

Modbus is a new type of locale bus technology, which is similar to other locale bus standard with open, intelligent, high environmental adaptability and other characteristics. It also has well installation and maintenance, high systems integration initiative weight, accurate and reliable run and other strongpoint. In addition, this agreement has strictly formulated the message structure which is able to identify in the bus network from master and slave, regardless of what network to communicate. As long as the signal frame is enveloped accordance with the data structure that set by this agreement. Different system can interconnect, that it can flexibly select the underlying transport medium in locale bus.

Modbus has a query-response cycle characteristics, the master and slave devices can communicate individually, but also it uses broadcast to communicate to all slave devices. If it communicates alone, slave device returns a message as a response. If it queries using broadcast mode, so it does not make any response. Modbus protocol establishes master device query format: device (or broadcast) address and function code and all data to be sent and error detection domain. The slave device response message is also constituted of Modbus protocol. It includes confirm action domain and any data to be returned and error detection domain. If the message occur error during reception, or the slave device does not execute its commands, the slave device will establish error message and sent it as a response.
When different devices communicate in Modbus network, each controller has a device address in accordance with the protocol requirements. The communication process device identifies is the message which sent by the address, and decide what action is produced by the specified equipment units. If it needs respond, the controller will generate feedback and use Modbus protocol unit sent to the specified device. In other networks, including Modbus protocol messages convert to frame or packet structure in this network. This conversion also extends solution according to the specific network solve node address, routing path, and error detection method. Standard MODBUS communication protocol uses two modes: ASCII (American Standard Code for Information Interchange) and RTU（Remote Terminal Unit. These two models are the same in the packet structure and functional command. Only the frame information expressed is different.

3.1. RTU Mode

When RTU mode establishes communication, the information transmitted as 8-bit binary, such as: 63 (hexadecimal) in RTU mode is 8-bit witch represent with binary 0ll000ll. The biggest advantage of this approach in the same transmission rate is that it can transmit more information than in ASCII mode. The model is widely used in the intelligent instrument.

3.2. ASCII Mode

When ASCII mode establishes communication, each byte of information frame is represented by two characters, such as the hexadecimal number 63 will occupy 2 bytes in ASCII mode with the character '6 'and '3' , its code is 0ll0ll0 0ll00ll. Obviously, ASCII mode communication spends twice in time and space than RTU mode. But its advantage is that it is convenient and easy to read.

4. Heterogeneous Network Communication Research Based on Modbus

Modbus protocol is a common language for the electronic controller used in industrial control field. By the protocol, various controllers, upper computer and other device can communicate. As general industry standard, control equipment from different manufacturers can be connected into industrial network and centralized monitor in a heterogeneous network. The protocol has defined the structure which a controller can recognize the message. Regardless of whether the device communicates through what network, it can achieve effective communication. And other devices realize access requirements by defining controller request. Respond to requests from other devices, as well as error detection and recording, thereby it enhances the effective and stabile communication in complex industrial environment. Meanwhile, Modbus also developed message domain pattern and content common format [5].

This system uses industrial control computer. It uses the STC89C52 microcontroller as the core unit's remote control and S7-200 series PLC to achieve Modbus protocol master-slave data communication. Upper computer is as a master device to manage the network address of the device in each sub-set, communication tokens and message transmission. To the PLC, it requires the CPU module must be CPU224 or above and it is equipped with two serial ports. PLC uses port 0 (Port0) to Modbus communicate, the master and slave communication parameter is as shown in table 1:

Table 1. Parameters of master and slave station

Parameter Type	Settings
Communication mode	Modbus
Baud rate / (bit • s_1)	9600
Parity	Even parity
Delay / ms	100
Slave address	1 ~ 118
Select literacy	read/write
PLC read/write start address	VB800
Read number (byte)	255

In the entire system network, each node monitor in specified time slice based on Modbus protocol. When it needs to send a message, it must listen on the network whether it is in idle status, it obtains the communication use right through a competitive way. Only the node which obtains the use right can send a message to the network bus, while the other nodes can only receive information frame at the same time. In the extreme case, if two or more nodes at the same time listens to the network is idle and sends messages, so it produce a conflicts phenomenon because of the same band signal, it makes message become invalid messages because of illegality falsify during transmission. The sent messages are dropped off the place which not able to recognize and respond. So each node must have the ability to detect whether the conflict occurs at any time. In a very short time if it occurs conflict, it should stop sending messages to avoid network is wasted due to send invalid messages. Then after a random delay period of time, re-contention network resources and resend the message until the message is successfully sent or it reaches a predetermined number of transmissions [6].

4.1 Communication Token Conflict Detection based on Modbus

In order to achieve the Modbus communication process caused unnecessary conflict and lead to the discarding messages, the system designs a collision detection token. It designs two communication modes on sharing same RS-485 bus:

(1) master-slave mode: It is effective communication after the possession of the channel, only the master and slave sides can communicate in network, the other nodes are in the channel monitoring status.

(2) Free communication phase: At this time there is no node occupied channel, the channel is idle. All nodes is in a peer-to-peer, when the first node successful occupies channel, it immediately switch to the master–slave polling communication status [7]. Of course, in order to ensure that communication channels are not long-term occupation or blockage, each communication must be completed within the effective time.

The system uses the time-sharing communications, each node of the system follows the communication rules and utilizes reasonable time slice. Two communication mode defined by system communicate in each time slice. The time slice that occupy by master-slave mode calls polling phase. The time slice that occupy by peer-to-peer communication mode call free communication phase. The core idea of the time slice synchronization strategy is each node in the system rest a time slice at each time intervals. The upper computer which be in management position monitors idle time slice and send data in idle time slice. Suppose the length of each time slice is T milliseconds, the polling period occupy 1T, free communication stage is 4T.

After it synchronize system time slice, each node in the system device from the upper computer (the upper) defined Tick-Count to maintain and synchronize their respective Tick-Count to ensure Tick-Count consistent between various devices in the system, when all nodes Tick-Count consistent each node can effectively distinguish the upper polling stage and free communication stage, and a request to initiate a dialogue in the freedom of communication stage for effective communication in upper polling bus listener.

4.2 Modbus Error Detection Method

In addition to system design 1byte packet check code for packet checksum mechanism, Modbus also has its own error detection mechanisms to message. Namely standard Modbus uses two error detection methods in serial network: parity detection and message frame detection. Parity detection is available for each character. Frame detection (LRC or CRC) applies to the entire message. They are produced by the master device before the message is sent. The slave device detects each character and the entire message frames during the reception. The user need configure pre-defined time-out interval to the master device, this time interval requires long enough (e.g. 500ms), so that the slave device can do normal response. If the slave device detects a transmission error, the message will not be received, and will not respond to the master device. Such timeout event will trigger the master device to handle errors. The address that sent to the slave device not existing will produce timeout.

In this system, Modbus packet transmission itself includes the error detection fields based on CRC method. CRC field tests the entire contents of the packet. CRC field has two bytes, which is calculated by transmission equipment and added to the message. Receiving device recalculates the CRC of the received message, and compare to the received value in the CRC field. If the two values are different, it indicates an error. It starts retransmission mechanism to ensure the normal packet and valid transmission. In the CRC generation process, each of the eight bits characters are individually do Or operation to register contents. The result shifts to the low significant bit, the high significant bit is added to 0. When LSB is extracted and detected, If the LSB is 1, register individually and preset value does Or operation. If LSB is 0, then there do nothing. The whole process is repeated eight times. In the last one (the 8th bit) is completed, the next 8 bytes individually do Or operation to the current value of the register. The final value of the register is the value of the CRC value to all the bytes of the message execution [8].

This system effectively utilize the Modbus packet check code mechanism itself, it is also the system design verification mechanism to join the message itself. And thus it more effectively ensure packet transmission reliability and validity, and the use of tokens ensures network each node can be orderly and smooth communication. It provides a guarantee the system stability and efficiency.

4.3 Conflict detection application based on Modbus

In order to achieve timeshare communication mode based conflict detection, it needs to define the system cycle time T. The system determines the time of transmission of a character under the specified baud rate commonly range.
For example if the system set communication baud rate is 9600, the start is 1 bit, data is 8 bits, parity is 1 bit and stop is 1 bit, and then send a character needs 12 bits. According to the equation 1, it can calculate the transfer time T character per character is 1.25 milliseconds; in order to guarantee the system message is not timeout caused by the length, the system determines the maximum length of the protocol message is 100 bytes, according to equation 2 the maximum message transmission time T package is 125ms.

It reserves a certain margin based on the site-specific environmental conditions to consider a communication delay, so the actual time slice can select 2 to 4 times to theoretical time slice, then the actual time slice range is 250~500ms. In order to guarantee a reliable communication system chosen maximum time slice is 500ms, it can be seen the polling interval is 2500ms; the free communication phase occupy 2000ms. After spot application, communication quality and traditional mode has a significant improvement.

$$T_{\text{character}} = \frac{1000\text{ms/s}}{B_{\text{bps}}} \times C_{\text{length}} = \frac{1000}{9600} \times 12 = 1.25(ms) \qquad (1)$$

$$T_{\text{Package}} = T_{\text{character}} \times P_{\text{length}} = 1.25 \times 100 = 125(\text{ms}) \qquad (2)$$

According to the requirements of the above timesharing communications, as a management upper the upper computer of the system needs to set up and maintain Tick-Count. Under the bus is in free condition, it completed access from the slave machine. And in the freedom of communication phase, it monitors data of the bus to ensure effective communication of the whole system.

Because there are differences to the crystal of the various nodes in the system itself in order to guarantee Tick-Count used of all the nodes is consistent in the system [9]. And also in order to synchronize communicate to newly added child nodes, so the upper need to resynchronize the Tick-Count intervals. Process is shown in Fig. 3:

Only after the synchronizing signal received by the upper device transmission, the Tick-Count can respectively performed synchronization and then conduct effective communication. Each node device and upper share a set of clock mechanism, clearly judge the master computer polling stage and free communication stage.

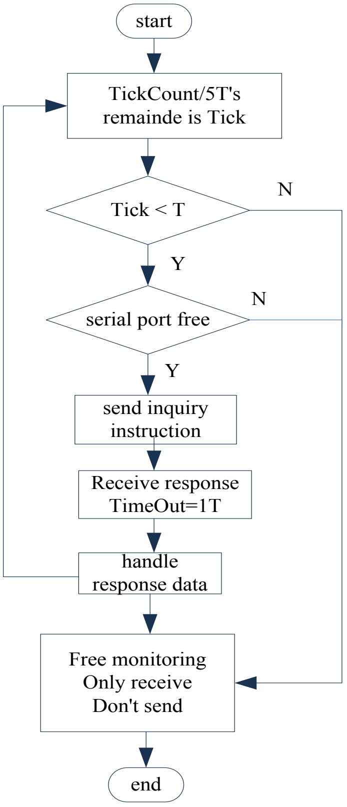
start
TickCount/5T's remainde is Tick
Tick < T
N
Y
serial port free
N
Y
send inquiry instruction
Receive response TimeOut=1T
handle response data
Free monitoring Only receive Don't send
end

Fig.3 Host computer communication processing flow chart

So each child node can send request message in free communication stages. If it needs response, the specified child nod exchange information to upper, slave device communication process flow is as Fig. 4.

4.4 Compare to Traditional Communication

Production practices indicates that the communication mode that using time-sharing communications conflict detection which replace the custom protocol based on Modbus protocol, it can effectively solve the problem of each node in the system cannot effectively communicate properly. In accordance with the size of the messages in the actual field test, under the conditions of big message (500 bytes or 200 bytes), from the 10000 message it statistically find that the effective message percentage does not exceed 95% between traditional communication mode and improved communication mode.

However, to small messages (less than 100 bytes), the improved communications mode is clearly superior to the traditional transmission mode. But it uses maximum 50 bytes messages used spot, it found than there is no bare error packages to the improved communications mode and effective message dropped 99.97%, it is as shown in table 2.

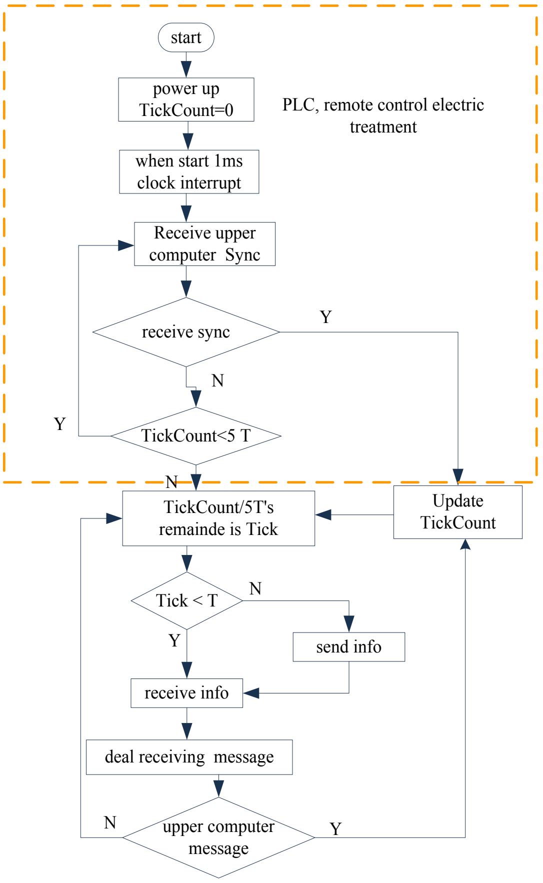

Fig.4 Slave machine communication process flow chart

Table 2. Comparison between traditional mode and improved mode

message size	transmission mode	effective message number	error message number	success percent
500 bytes	traditional mode	5253	4747	52.53
	improved mode	7876	2124	78.76
200 bytes	traditional mode	6159	3841	61.59
	improved mode	8563	1437	85.63
100 bytes	traditional mode	7757	2243	77.57
	improved mode	9943	57	99.43
50 bytes	traditional mode	8372	1628	83.72
	improved mode	9975	25	99.75
20 bytes	traditional mode	9151	849	91.51
	improved mode	9997	3	99.97

5. Conclusions

This paper has discussed in detail RS-485 bus communication design principle and method based on Modbus protocol. It has tested twenty nodes in network environment using the Modbus protocol. Each node sends data request every 50 ms, all the requests of the node can get correctly respond. It has implemented the remote Ethernet no error communication between the collector and the client. At the same time this paper does not increase system cost using scheme. But also it allows the master computer liberate from the busy communication work. It better accomplishes the human-computer interaction and data processing and other task. Thereby it improves the system independence and speed up system speed of recovery from a failure and effectively improves system reliability and security. The system meets the design requirements and functional requirements design in operational phase. It provides reliable raw production data for all levels of production and research management people. Carry out related technology research, it provides a reliable way in order to further deepen the aluminum production process variations in understanding. Practice has proved that the system is stable and low failure rate and easy to operate and safe and reliable.

Using conflict detection techniques according to time-sharing communication, it uniformly manages to different application platform system. It does polling communication and free communication in accordance with the time slice. It not only ensures the master machine effectively manages to a variety of the slave machine, but also it provides a technology platform for the information interaction between each slave machine. So it ensures to coordinate control and information exchange among the system equipment. It is a good solution to the traditional production process that can not be normal operation under the conditions of strong electromagnetic interference. It provides technology means for the enterprise precision management. Take advantage of the enterprise in the device's automation control improve enterprise comprehensive competitive ability, it has the broad application prospect.

Acknowledgment

The work in this paper has been supported by Beijing Natural Science Foundation (No.4131001). It is also supported by National Science and Technology Support program (No.2012BAH04F00) and Beijing Natural Science Foundation (No. 4132026) and Beijing Education Science and Technology Development plan (No.KM201210009006) and Beijing Image Information Processing and Intelligent Recognition Scientific Research Platform Construction (No.PXM2012-014212-000024).

References

1. HAN Jiang-hong, WEI Zhen, CAI Zhi-wen, HAN Dong, WEI Zhen-chun, "Collision and information error of topologies in clustering protocol, Journal on Communications", Vol.32(5), pp.97-103, 2011
2. LIU Guichen,YANG Xianhui,"Cable wireless hybrid transmission of Modbus messages", Journal of Tsinghua University (Science and Technology), Vol.48(S2), pp.1844-1847, 2008,
3. ZHI Yan, JIANG Cun-bo, XU Jian, "Application of the Modbus communication protocol in CNC system", Journal of Lanzhou University (Natural Sciences), Vol.46 Supp, pp.205-208, 2010
4. ZHU Xiao-chao, XU Xue-chun, "Implementation and Simulation of Communication between Host Computer and MCU Based on Modbus Protocol", Instrument Technique and Sensor, Vol.6(6), pp.65-68, 2011
5. CHEN Shan-lin, YANG Cheng-zhi, YANG Xiao-hong, WU YU-cheng, LIU-Wei, "Wireless Long - range Data Acquisition System Based on Modbus Protocol", Journal of Kunming University of Science and Technology(Science and Technology), Vol.29(2), pp.53-56, 2004
6. Weng Jiannian, Zhang Hao, Peng Daogang, Li Hui, "On embedded ARM based Modbus TCP Protocol and its Implementation", Computer Applications and Software, V01.26(10), pp.36-38, 2009

7. CHI Xinze, ZHOU Hao, ZHAO Baohua, "Multicast Error Control Protocol in Wireless Mesh Networks Based on Forward Error Correction", Journal of XI'AN JIAOTONG UNIVERSITY, Vol.45(8), pp.30-36, 2011
8. LIU Wen-jun, LI Xiang-yang, "Design a Class Modbus Protocol Based on Automatic Addressing", Science Technology and Engineering, Vol.12(6), pp.1412-1415, 2011
9. LI Bao-ren,ZHOU Lei,ZHOU Hong, "The Realization of Communication Node Based on Modbus /TCP Protocol", Machine Tool & Hydraulics, No.l2, pp.153-155,2004