Research on Software Scheduling Technology Based on Multi-Buffered Parallel Encryption

Zeng Rong [1, a], Xia Wei [2], Wang Hongkai [2] and Gong Xiaogang [2]

[1] State Grid Smart Grid Research Institute, Nanjing, China

[2] State Grid Zhejiang Electric Power Company, Hangzhou, China

[a]zengrong@sgri.sgcc.com.cn

Keywords: Software Scheduling Technology, Multi-Buffered Parallel Encryption.

Abstract. Multiple buffers parallel-encryption technology uses multiple buffers, takes advantage of the data transfer bus and saves data transmission time. By keeping encryption chip been in working condition, can Improve the efficiency of encryption chip, and effectively improve the performance of cryptographic equipment. Using software encryption scheduling technology can achieve multiple buffers parallel encryption schedule; can increase the speed of encryption and decryption devices. Finally improve the application level password system power business.

Introduction

With the development of information networks in power, more and more electricity business applications scheduling through the information network system. In order to ensure the security of information systems business data, we used data encryption to protect data widely. Power network communication system requires encryption equipment performance increases in high speed. However, the performance of encryption chip subjects to the development of hardware technology. Growth performance is difficult to meet the demand for electricity network communication system. We need to upgrade the cryptographic device encryption capabilities through other means.

Since during operation of large-scale data transmission requires a lot of time in the bus, so the effectiveness is wasted in the presence of the encryption program scheduling in encryption chip. Therefore encryption chip is not in full working condition. We can research a high-performance encryption device scheduler to enhance the efficiency of encryption chip. This paper presents a scheduling method by multi-buffering parallel encrypted data in the interface to mention reduce the transmission loss of time, improving the efficiency of encryption chip, making the encryption device performance boost.

Principle

The DSP processor on encryption card connects to the host through PCI bus. PCI interface can theoretically provide 1Gb / s bandwidth, fully meet the encrypted card data transmission requirements. In order to maximize data transmission speed on PCI bus, encrypted communication between card and host uses DMA transmission mode. DMA transmission mode has the advantages that DMA controller controls data transmission on PCI bus and does not require the processor to do anything during the operation, and sends a set of data each clock cycle. DMA transmission mode is the most efficient data transmission mode. Begin the PCI DMA transmission start, DSP processor in encryption card needs to write source data address, destination data address and data length written to the DMA controller, then DMA controller start DMA transmission. Although the DMA transmission is the fastest known transmission method, but the data written through PCI bus still takes time, if the time can be eliminated, it will greatly improves the performance of encryption card.

Usually data encryption card is designed in single buffer mode. The host processor and DSP on data encryption card have a data buffer each other for data exchange. Example of a data packet encryption, at first the host stored the plaintext data in the host buffer, notified the processor DSP on the data encryption card. DSP notified DMA controller to copy data to the DSP memory buffer, then controlled

encryption chip to encrypt data. Encrypted data covered plaintext data. After encryption, DSP transmitted data to host data buffer covering plaintext, and notified the host that encryption was completed. The process that DSP operate encryption chip only takes up part time. Another lot of time was wasted on data transmission on PCI bus. When data are transmitted on PCI bus, encryption chip does not work. Encryption chip computing power is wasted. It is evaluated that about 30% of the encryption power, if we can take advantage of this part of the time, will makes data encryption card performance improve greatly.

System sets up several data buffers both in host memory and DSP memory. Taking advantage of the characteristics of DMA data transmission operation procession does not need DSP participate, DSP processor can operate encryption chip encryption and decryption in idle time. The analysis revealed that DSP processes on the DMA transmission only takes up very little calculation capability. It can be make most of the computing capability DSP to control the encryption chip to encrypt and decrypt. There are four groups buffer both in the host memory and DSP memory. One buffer in the host is corresponds to another in DSP. If there is a buffer is idle on DSP, DSP will read plaintext from the host buffer. Also, once the data on DSP buffer is processed by encryption chip, DSP will transmit the data to the host. So, the continuous data interaction by multi-buffer mode between the host and DSP is achieved.

Plaintext data from begin to complete the encryption process to go through some processes. First we need complete the plaintext data preparation. Transmit plaintext data to the cryptographic module via data transfer bus. Then encryption module writes the plaintext data to encryption chip through local bus. When encryption chip completes encryption, encryption module reads the cipher-text data. Encryption module then return the cipher-text data to encryption device via data transfer bus.

In the procession of data encryption conversion plaintext data into cipher-text, data consumes a lot of time in transit. During this period encryption chip is not in full working condition. Therefore, the effectiveness of encryption chip has much room for improvement. Improve efficiency in data transmission interface through the study, use software program to achieve data transmission scheduling, we can reduce waste time encryption chip and increase in performance encryption and decryption devices. This paper presents a multi buffered parallel encryption methods to achieve scheduler, able to control encryption chip has been in working condition, improve the efficiency of encryption chip.

In order to improve the efficiency of encryption chip, we need to create multiple buffers. We use multiple buffers provide a steady stream of encrypted data to encryption chip. It enables encryption chip encryption is always in full load operation state.

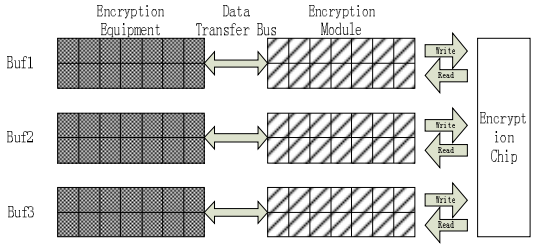

Figure 1. Multi-Buffered parallel data encryption flowchart-based encryption

Encryption module check whether the data buffer 1 is unprocessed data. If it is, then judging whether encryption chip is idle. If it is idle, encryption module sends the unprocessed data into the buffer encryption chip. When encryption chip completes encryption, encryption module reads the processed data from the encrypted chip. It stores the data into buffer 1, and identifies the data packet as complete treatment. Encryption modules then check the buffers 2, and repeat, and poll all buffers. Since the plurality of data buffers must be data to be processed, encryption chip can always be in full working condition. By tests, the efficiency of encryption chip can be close to the maximum value. Therefore, the encryption chip can work in a saturated state.

Encryption equipment needs to package in plain data before sending data to the encryption chip. Data transfer in the data transfer bus in the form of data packets.

The package in multi-buffer parallel encryption method needs to redefine buffers. The buffer adds buffer number and state identification. Encryption module identification and control data packets encryption and decryption through number and state identification.

Program model

How to make a single DSP processor to operate multi-buffer DMA transmission and control encryption chip to calculate is the most important difficulty needed to solve in the design. On the one hand DSP processors need to determine whether there is free buffer in memory, and to constantly copy data from the host, to determine whether the data in buffer has been processed, then sends the processed data to the host; On the other hand, also need to control the encryption chip encryption and decryption, constantly write unprocessed data to chip and read processed data from chip. So it needs to research a new scheduling algorithm to do both works at the same time.

The scheduling algorithm of encrypted card mainly contains to read unprocessed data from the host, to operate encryption chip encrypting and decrypting data, and to return processed data back to the host. The main program enters an infinite loop procedure after initialization. Loop procedure determines in order whether there are data need to be read to the free buffer, whether there are data need to be encrypted or decrypted, whether there are data to be written to the host. If there is data to be read to the buffer, program will enter to the appropriate process to start the DMA transmission to read data from the host buffer. After the DMA transmission starts, DSP main program will leave DMA controller to execute the DMA transmission. DSP main program comes to the next process, such as operating encryption chip subprogram. When DMA transmission is finished, DMA controller will notify DSP program by interrupt. The interrupt routine determines whether there is other free buffer .If there is, the interrupt routine start the DMA transmission, until all the four buffers are full. So in the buffers there have been enough data for encryption chip to encrypt and decrypt. When the buffers have data need to be processed, the main program comes into the data encryption and decryption routines, and DSP controls encryption chip to encrypt and decrypt operations. Then the main program determines whether there are data in buffers needed to be written to the host, and if the DMA controller is idle, comes into the DMA transmission writes subprogram. The DMA transmission writes subprogram starts DMA transmission, and writes the processed data to the host. The host will notify DSP by interrupt after get the data. When DSP receive the interrupt, it clears the buffer.

Because a DMA read data transmission routines is added into the interrupt response program, as long as the host has new data and encryption card has free buffer, DSP processor can read the data priority from host buffer to DSP buffer to ensure there is always unprocessed data for the encryption chip. Because DMA transmission does not take up the processing capability of DSP, DSP can be used to control encryption chip to encrypt and decrypt. And as the DMA transmission starts and interrupt response takes less time, so the majority of calculating capability of DSP can be used to control encryption chip calculation. So it is almost negligible that the time wasted on data transmission between the host and DSP in the encryption card.

Multi-buffer packet encryption scheduling control is realized by the software of encryption module. Establish procedures scheduling model is very important. Program scheduling more buffers control is using multiple buffers polling methods. The system will be checked each buffer state flag after operation is completed. If there is a buffer of data has not been processed, the buffer is marked. The system will read data from the buffer and write it to encryption chip buffer.

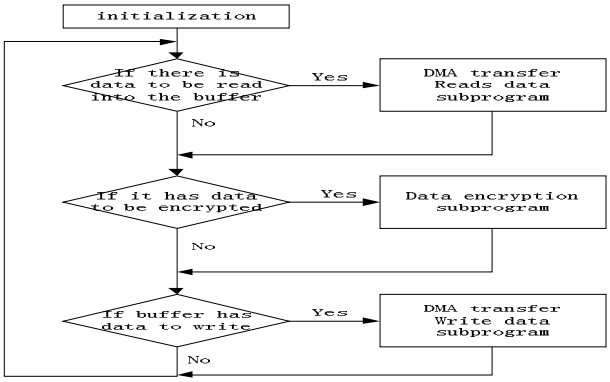

Figure 2. Multiple buffers parallel encryption scheduling process

Encryption scheduling module controls:

1. After the system completes the program initialization, it began to determine whether there is need to read data packet. If there is data to be read, DMA transfer is started. System reads the data packet from the encrypted device and saved to the buffer. The packet is marked as unprocessed state.
2. The system determines whether the buffer data needs to be encrypted. If it is, data encryption subroutine is called. The system reads the encrypted data from encryption chip.
3. Determine buffer has cipher-text data to send. Then judge whether the buffer state flag is processed. If there is data that have been processed, it starts DMA transfer. Send the data to encryption equipment. After the transfer completion flag buffer is empty. Prepare for receive the next set of data packets.

If we need to do decryption operation, the encryption mode of operation is similar.

The scheduler can perform the above operation for each buffer. So it can poll all buffers sequentially. Ensuring each buffer packet can be processed.

Interrupt program

In order to achieve efficient on the data bus to transfer data, encryption module uses encrypted data transmission between the DMA and encryption devices. Interrupt response procedure is used to implementing data transfer via DMA channel processing. Encryption module starts packet transfer by setting the transfer order. After the end of DMA transfer, the system will start interrupt response procedures. Encryption module can operate subsequent transmission in the interrupt response program.

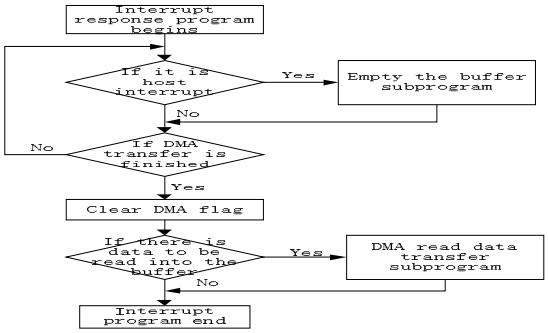

Figure 3. Interrupt response process

Encryption module interrupt response program:

1. At first, system judges whether the interrupt is host interrupted. If it is, clear the buffer data currently pointing. Ready to accept the next set of data.
2. Analyzing whether DMA transfer is completed. If it is, ready to start the next set of data transmission.
3. Determine whether there is data to be read. If it is, start DMA transfer. Reads the data from the corresponding buffer packet encryption device to the corresponding buffer in encryption module.
4. After the above flow process is completed, finish the interrupt program.

Interrupt response program implements the transmission scheduling of packet data transmission on the bus. So the program can cycle data to the buffer for transmission processing. Whenever there is data to be processed in buffers, as long as the data transfer bus is idle, encryption module will start the DMA transfer. The system can use the bus for data transmission efficiently.

Test results

The original encryption card applied single-buffer mode that runs by three-step in order, including DSP read data from the host and controlled encryption chip calculation, and written to the host. The accelerated encryption card use multi-buffer mode, which has four buffers. The performance contract between the original encryption card and the accelerated encryption card were list in Tab. 1.

Table 1. The comparison between original encryption card and accelerated encryption card

	Performance of original encryption card	**Performance of accelerated encryption card**	**Percent of speed improved**
Single encryption card	44 Mbps	61 Mbps	38.6%
double encryption cards	86 Mbps	119 Mbps	38.4%

The comparison test shown that when single card is used, performance of encryption card increased 38.6%, and when double cards is used, performance increased 38.4%. It is shown that the performance of the accelerated encryption card is faster than the original encryption card more than 38%. It is proved that the multi-buffer mode effective to improve the performance of encryption card, and multi-buffer scheduling algorithm can increase the encryption speed of the card dramatically.

Summary

Encryption software based on multi-buffer scheduling, it enables parallel encryption on the Encryption Module. Encryption module can save large data transmission time on the bus if we use the scheduling technology. It makes encryption chip has been in working condition always. Thus enhance the performance of encryption module. The experimental results show, the encryption device uses encryption technology based on multi-buffer is faster than the encryption device than not using the technology in the speed of encryption.

References

[1] Li Zhitang,Sun Chen, Performance analysis of multi-card parallel encrypted VPN, Journal of Huazhong University of Science and Technology[J], 33, 5 (2005)

[2] Yuan Liang, Gu Tianxiang, Xu Sanlin, Hardware and driver design of a data-encryption card based on PCI, Journal of electronic measurement and instrument[J], 19, 6,(2005)

[3] Huang Xingli, Cai Guoqiang ,Yu Hongyi, Research and Implementation of IPSec Encryption Card on Linux2. 4 Kernel, Computer technology and development[J], 21, 7,(2011)

[4] Tan Xiao Gang, Xie Jian Feng. Design of Data Encryption card PCIJMC2000 Based on DSP. Computer Information[J]，2007，23(10)：154-155

[5] Chen Jin, Zhang Xi Cai, Zhang Jin Guo, et al. The design of the PCl encryption card driver based on DM642. Manufacturing Automation [J]，2011，33(2)：129-131

[6] Huang Jian, Chang Chao Wen, Ma Shi You, et al. Design and Implementation 0f Encryption Card Base on PCMCIA. Network Security Technology and Application[J], 2008, : 94-95

[7] Jiang Lin, Zhu Yi Wei.: Hardware Design and Implementation 0f High Performance Data Encrypted Card. Computer Engineering[J], 2008,34: 105-107