Design of Remote Industrial Control System Based on STM32

Rongfu Chen, Yanlin Zhang(✉), and Jianqi Liu

School of Information Engineering, Guangdong Mechanic and Electrical College, Guangzhou 510550, China
{343656182,350054049}@qq.com, liujianqi@ieee.org

Abstract. Pushed by "Internet +" and Industry 4.0, the production mode of traditional industry will be changed by technological innovation. Since the core is intelligent manufacturing, the manufacturing industry will be intelligentized and internetized. Nowadays, however, most of the manufacturing facility cannot meet the requirement for intelligent manufacturing. Therefore, it's necessary to design a remote industrial control system, having STM32F407 be the master CPU since its operating frequency can reach 168 MHz and STM32F103 be the node CPU since its cost performance is quite impressive. The master connects to the node with RS485. The master can also be the gateway, responsible for data exchange between intranet and server, while the node can detect sensors and control actuators. This system helps to realize intelligentization and internetization, meanwhile, administrators can monitor and control the system through computer and mobile terminals APP.

Keywords: Remote monitoring · STM32 · Cloud service · MODBUS

1 Introduction

Currently, old-fashioned production control system is still widely adopted by most manufacturers. In this kind of production control system, each process node is independent, meanwhile, one worker is needed to monitor and manipulate one process node or several, which causes the waste of resource, the discrepancy between products due to the competence of each worker, and thereby inefficiency in the enterprise. With the promotion of Industry 4.0 [1], smart plant is popularized, therefore, that old-fashioned control system will become obsolete.

To solve the problem mentioned above, for better stabilization and manipulation, one remote industrial control system is designed with 3 layers: node perception, master control gateway and cloud service. Node perception layer is responsible for collecting field data, processing simple data, packing data and sending to master control gateway; the gateway will encrypt the received data and send to cloud server by package; the server can complete data analysis, obtain the optimal control parameters, feedback to the control system and manipulate the system. This remote industrial control system helps to automate the production system, optimize the allocation of resources, achieve uniform quality [2], and improve the efficiency during production process.

J. Wan et al. (Eds.): Industrial IoT 2016, LNICST 173, pp. 257–267, 2016.
DOI: 10.1007/978-3-319-44350-8_26

1.1 Diagram of System Composition

The node perception layer of this remote industrial control system is composed of various nodes and each node can complete one process in the industrial production. Also, the node perception is capable of actuator control, monitoring the parameter of a certain procedure according to the received control signal. As a transfer station of the whole system, the master control gateway is in charge of collecting the uploaded data of each node, completing encryption & protocol conversion, sending that information to the cloud server, receiving the control signal from the cloud server, conducting decryption & protocol conversion [3], and modulating the parameter of relevant nodes. User administration terminal is composed of PC or mobile terminal. The system diagram is shown in Fig. 1.

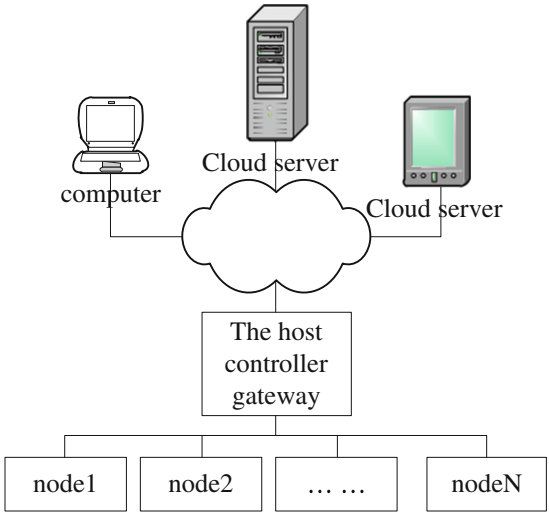

Fig. 1. System composition block diagram

1.2 Data Transmission

Data transmission is divided into two parts: LAN and WAN. LAN refers to master control gateway and each node, while WAN is the cloud server. PC and mobile terminal can choose LAN or WAN according to its network access point.

Under the MOBUS protocol, the main controller connects with the nodes through two-wire line 485. The main controller is the host mode and the nodes are slave mode. The host can read the slave by roll poling [4]. Communication format is as follows:

(1) The default format for communication is 8, N, 1 The default baud rate is 19200 bps

(2) protocol is MODBUS RTU [5], Register operation is shown in Table 1:

Table 1. The register list

SN	address	Instructions
1	0000H	read-only, model, Value A001
2	0001H	read-only, Device type B002, Representative is a node
3	0002H	Read, write, node address
4	0038H	read-only, Flow of A size
5	0039H	read-only, Flow of B size
6	003AH	read-only, Reaction zone temperature
7	003BH	Read, write, Control valve "A"
8	003CH	Read, write, Control valve "B"
9	003DH	Read, write, Heating control
10	003EH	Read, write, Motor control

The Register is 16 bit (2 bytes), HIGH in the front, and LOW at the back.

(3) Routine Data Manipulation

- Function code 03: Read multiple registers.
  The starting address: 0000H~003EH, invalid if over range
  The length of the data: 0000H~0007H, Up to a maximum reading of 7 consecutive registers.
  The host sends: address + Function code + The starting address + Data length + CRC code.
  The response: address + Function code + Returns the number of bytes + multiple data of Register + CRC code.
- Function code 10: Write multiple registers
  The starting address: 003AH~003EH, invalid if over range
  Register number: 0001~0004H, 4 registers will be the maximum for one continuous setting
  The host sends: address + Function code + The starting address + Write the register number + Number of bytes + Save the data + CRC code.
  The response: address + Function code + The starting address + the register number + CRC code.
- Function code 05: Write one way switch output
  The host sends: address + Function code + carry-out bits + Data length + CRC code.
  The response: the same as the host sends in regard of the format and content
- Handshake packet 4 bytes: 0X01 0X04 0X01 0XE3.
  Once the telecommunication line sets up, the master machine succeeds in connecting to the slave machine. After the communication status is on, no more handshake signal will be sent from the slave machine.
- Error messages: If there is an error in the set parameters, return an error code, in order to debug and repair.

Format: Address code + function code + error code + CRC code, error message is as follow:
86: Incorrect function code. The received function code is not supported by the slave machine.
87: To read or write the wrong address of data. The designated data address is over the specified address range.
88: Illegal data values. The received data value from the host is beyond the scope of the corresponding address data.

2 Design of Perception Layer

2.1 Hardware Design of Sensor Nodes

Sensor nodes are able to collect the local data, control the field parameters and communicate with the master controller. Therefore, the hardware of sensor nodes can be divided into 4 parts: CPU processor, 485 communication module, sensor module and actuator module. The block diagram is shown in Fig. 2.

Fig. 2. Node composition block diagram

The quantity of processing data handled by nodes is much less than the master controller. Then, the nodes' CPU can use medium capacity series of single-chip like STM32F103. The STM32F103xx medium-density performance line family incorporates the high performance ARM® Cortex®-M3 32-bit RISC core operating at a 72 MHz frequency, high speed embedded memories (Flash memory up to 128 Kbytes and SRAM up to 20 Kbytes), and an extensive range of enhanced I/Os and peripherals connected to two APB buses. All devices offer two 12-bit ADCs, three general purpose 16-bit timers plus one PWM timer, as well as standard and advanced communication interfaces: up to two I2Cs and SPIs, three USARTs, an USB and a CAN [6].

485 communication module uses SP3485 chip, and the RO connects to the RXD of CPU(i.e. PA10 pin). DI connects to TXD of CPU(i.e. PA9 pin), while direction control signal DE & RE connect to PB0 pin, with AB as 485 bus. The module circuit is shown in Fig. 3.

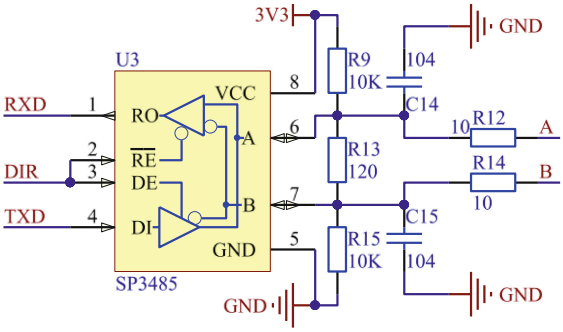

Fig. 3. Communication module circuit

Different sensor nodes have different interfaces. For better universality and installation, the nodes have several interfaces: IIC, SPI, 1-Wire, UART, AD. Each interface has a dial-up switch for checking the fitness of its setting.

Actuator module mainly consists of multiple small relay and its corresponding drive. When it's running, if the power of the small relay's drive is insufficient, that relay will impel the big relay or contactor. In order to protect CPU and its circuit, the relay control will be isolated by optocoupler. The module driver circuit is shown in Fig. 4.

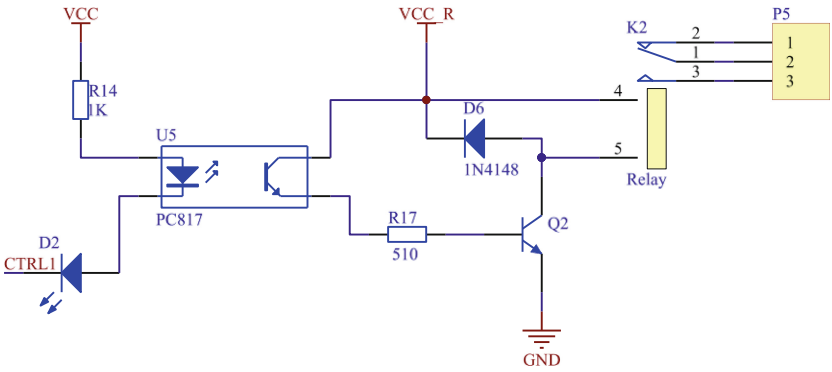

Fig. 4. Actuator module drive circuit

2.2 Software Design of Sensor Nodes

Sensor nodes take charge of three functions: reading sensor signal, controlling the relays due to the received signal and communicating with master controller. Before reading the signal from sensors, CPU will firstly scan the dial switch, read the sensor nodes and detect the sensor connected to the exact node so as to determine which algorithm should be adopted. Program flow chart is shown in Fig. 5.

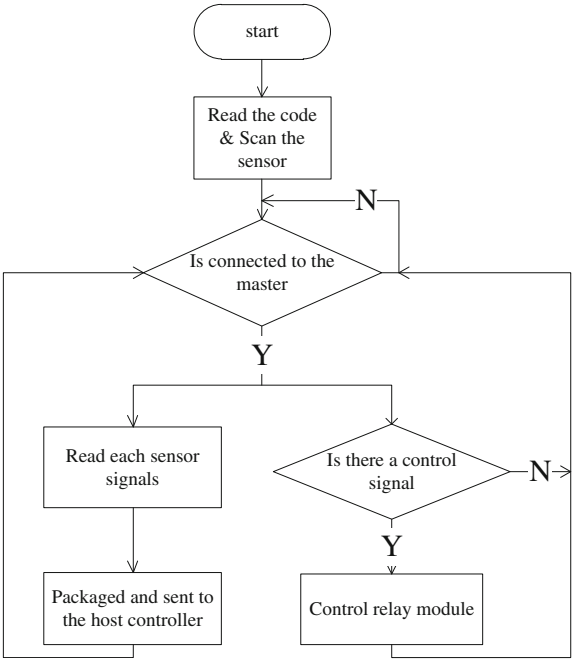

Fig. 5. The node program flow chart

3 Design of Master Control Gateway

3.1 Hardware Design of Master Control Gateway

The master control gateway is able to collect data from sensor nodes, send commands to the actuator control and communicate with the cloud server [7]. Therefore, the hardware of master controller can be divided into 3 parts: CPU, 485 communication module and internet network module. The block diagram is shown in Fig. 6.

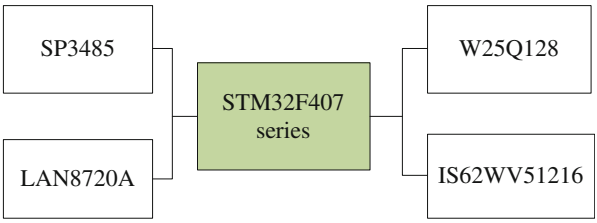

Fig. 6. The host controller composition block diagram

The master control gateway can handle complex task and require a speedy CPU, which is met by STM32F407. The STM32F407xx family is based on the high-performance ARM® Cortex™-M4 32-bit RISC core operating at a frequency of up to 168 MHz. The Cortex-M4 core features a Floating point unit (FPU) single precision which supports all ARM single precision data-processing instructions and data types. It also implements a full set of DSP instructions and a memory protection unit (MPU) which enhances application security [8].

To ensure the system can run smoothly, this system will use IS62WV51216 of 512 K × 16 LOW VOLTAGE, ULTRA LOW POWER CMOS STATIC RAM with RAM expanded and the flash expanded by W25Q128.

485 communication module uses SP3485 chip, and the RO connects to the RXD of CPU(i.e. PA3 pin). DI connects to TXD of CPU(i.e. PA2 pin), while the direction control signal DE & RE connect to PG8 pin, with AB as 485 bus and nodes connected by 485 bus. The module circuit is shown in Fig. 3.

Network communication module will use LAN8720A. The LAN8720A is a low-power 10BASE-T/100BASE-TX physical layer (PHY) transceiver with variable I/O voltage that is compliant with the IEEE 802.3-2005 standards [8]. The circuit chart is shown in Fig. 7.

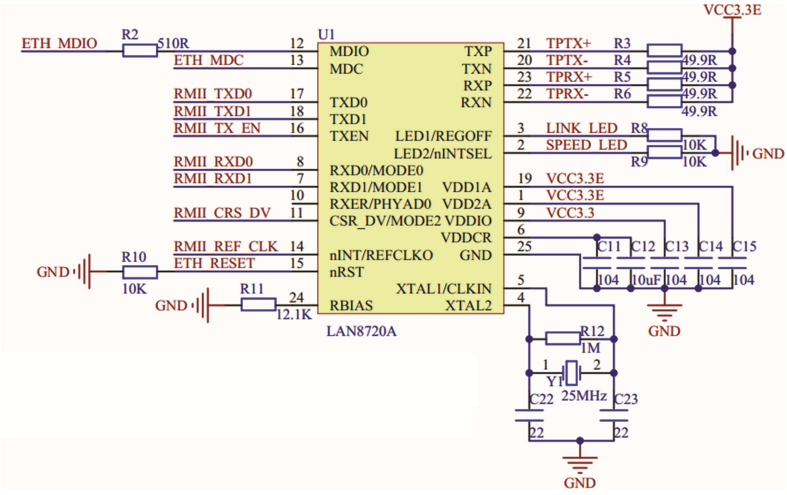

Fig. 7. The principle diagram of the network module

3.2 Software Design of Master Control Gateway

The master control gateway takes over three functions: collecting data from sensor nodes, sending commands to the actuator controller and communicate with cloud server. It can read the information from sensor nodes by roll poling [9], online update the list of sensor nodes regularly, collect the information from online sensor nodes regularly, encrypt the data and transmit it to the cloud server. When the command signal from

cloud server is received, it will send out the command and make the nodes control actuators. Program flow chart is shown in Fig. 8.

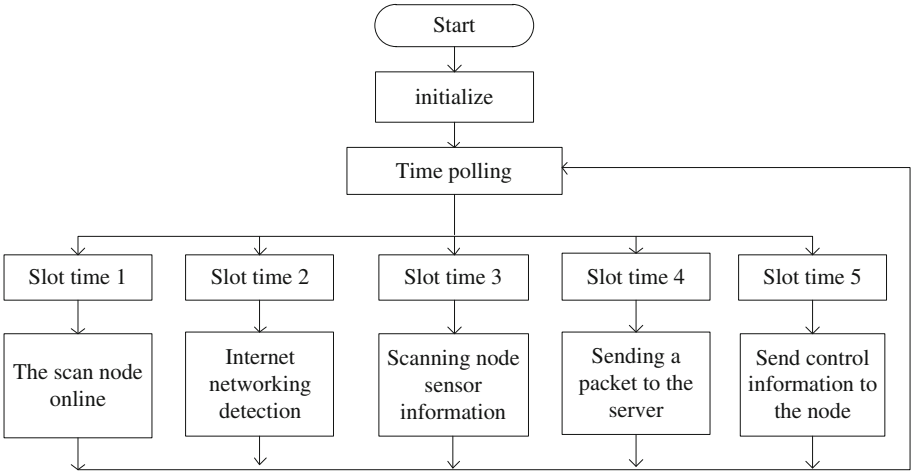

Fig. 8. The host controller gateway program flow chart

4 Design of Cloud Server

4.1 Cloud Computing Platform

With the help of flexible server, Linux operating system and Hadoop components (HBase, Zookeeper, Sqoop, Hive, Pig, MapReduce, Mahout), in view of two features of intelligent industrial control system: Small quantity of data for one single device and longer online time, this cloud computing platform is built through Infrastructure deployment technology of Virtualization and flexibility, under the dynamic allocation strategy to design computing resource, storage and internet. Please refer to the Fig. 9.

This design adopts the technology of Dynamic Feedback Load Balance [10], DFLB. Hadoop conducts cluster collection of the loading condition for current nodes and feedback to the scheduling system, which works as the weight of job scheduling algorithm. Through this way, a dynamic feedback closed-loop system is formed, which makes the cluster load gradually balance. Once all the nodes are of insufficient supply, this platform can apply to the system for more hardware resources (computing capacity, network bandwidth and storage space) in order to meet the application requirements.

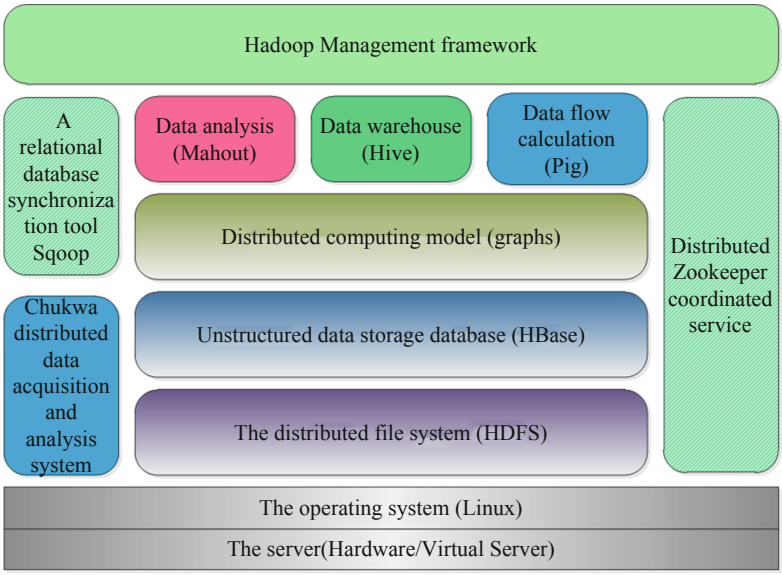

Fig. 9. Cloud computing platform architecture

4.2 Cloud Data Center for Designing Internal and External Network, Hybrid Encryption

According to the available data, if big data is not duly handled, user's privacy will be infringed badly, which is a big obstacle to promote smart industrial system. That's why the moment big data was raised its security issue attracted much attention. However, this system is designed within improved security policy, including configurable data acquisition platform for users and cloud data center storage.

For the user configurable data acquisition platform security strategy, according to the importance of the configurable data, three levels has been formulated: Level 1: running status of acquisition equipment and user log; Level 2: running status of acquisition equipment and user log (do not contain user address information); Level 3: only acquisition equipment running status data (do not contain user address information, time, etc.). The higher the level, the better user's privacy is protected. Users can configure freely in the intelligent master controller the gateway configuration page.

Cloud data center storage security [11] policy: firstly, to store data by independent internal and external network so as to realize logical isolation between the inside and the outside (basic data storing in the internal network, while the business data storing in the external network), which reduces network circuitry and equipment, make full use of the information available. By using advanced security means like firewall, user's information can be prevented from illegal invasion. Secondly, by using the password techniques, we can make sure the confidentiality and integrity of intelligent household data in cloud data center, as shown in Fig. 10.

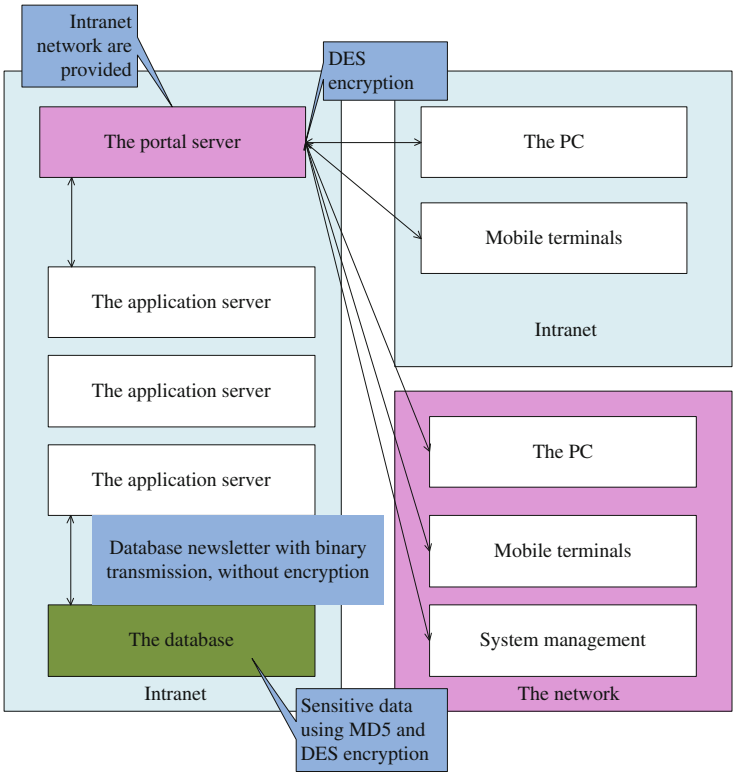

Fig. 10. Cloud data center storage security policy

Symmetric encryption algorithm (DES) can do the encryption speedily, but its shortcoming lies in using the same key to encrypt & decrypt, which cannot guarantee the security or manage the key well; compared with asymmetric key system (RSA), although it's not necessary to undertake negotiation about key, a plan for public key management is needed. Moreover, asymmetric encryption algorithm is inefficient and slow, only suitable for encrypting a small amount of data. Intelligent industrial system has a large number of data source and the data quantity is big. It requires good timing, speedy encryption and efficient encryption algorithm. Thus, the symmetrical encryption algorithm is suitable for data encryption, however, the asymmetric encryption algorithm is suitable for the encryption of metadata or secret key.

5 Conclusion

With STM32F4 as the host CPU and STM32F1 as the nodes, this remote industrial control system also has its corresponding cloud service platform and data center framework, enable to achieve remote monitoring & controlling. Since its stability and data security are quite impressive, this system can realize automation of production system and optimal allocation of resources. This remote control system is suitable for

manufacturing enterprises who intend to implement automation, to improve the quality of end product, to optimize the use of resources and to improve production efficiency.

Acknowledgments. The authors would like to thank Guangdong Province Special Project of Industry-University-Institute Cooperation (No. 2014B090904080), 2013 Guangdong Province University High-level Personnel Project (Project Name: Energy-saving building intelligent management system key technologies research and development) and the Project of Guangdong Mechanical & Electrical College (No. YJKJ2015-2) for their support in this research.

References

1. Lee, J., Kao, H.A., Yang, S.: Service innovation and smart analytics for industry 4.0 and big data environment. Procedia CIRP **16**, 3–8 (2014)
2. Liu, J., Wang, Q., Wan, J., Xiong, J., Zeng, B.: Towards key issues of disaster aid based on wireless body area networks. KSII Trans. Internet Inform. Syst. **7**(5), 1014–1035 (2013)
3. Want, R.: An introduction to RFID technology. IEEE Pervasive Comput. **5**(1), 25–33 (2006)
4. Liu, J., Wan, J., Wang, Q., Li, D., Qiao, Y., Cai, H.: A novel energy-saving one-sided synchronous two-way ranging algorithm for vehicular positioning. Mobile Netw. Appl. **20**(5), 661–672 (2015). ACM/Springer
5. Peng D, Zhang H, Yang L, et al.: Design and realization of modbus protocol based on embedded Linux system. In: International Conference on Embedded Software and Systems Symposia, pp. 275–280. IEEE press (2008)
6. Liu, M., Yu, J., Liang, H.: Wireless geotechnical engineering acquisition system based on STM32. Instrum. Techn. Sens. **5**, 95–97 (2010)
7. Liu, J., Wan, J., Wang, Q., Zeng, B., Fang, S.: A time-recordable cross-layer communication protocol for the positioning of vehicular cyber-physical systems. Future Gener. Comput. Syst. **56**, 438–448 (2016)
8. Gill, K., Yang, S.H., Yao, F., et al.: A zigbee-based home automation system. IEEE Trans. Consum. Electron. **55**(2), 422–430 (2009)
9. Liu, J., Wan, J., Wang, Q., Deng, P., Zhou, K., Qiao, Y.: A survey on position-based routing for vehicular ad hoc networks, telecommunication systems (2015). doi:10.1007/s11235-015-9979-7
10. Shu, Z., Wan, J., Zhang, D., Li, D.: Cloud-integrated cyber-physical systems for complex industrial applications. Mobile Netw. Appl. (2015). ACM/Springer. doi:10.1007/s11036-015-0664-6
11. Zhang, X., Du, H., Chen, J., et al.: Ensure data security in cloud storage. In: 2011 International Conference on Network Computing and Information Security (NCIS), vol. 1, pp. 284–287. IEEE press (2011)