Design of Remote Heat-Meter System Based on Trusted Technology

Changgeng Yu, Liping Lai

1School of Information and Communication Engineering, Hezhou University, Hezhou, China

*Corresponding author e-mail: yuchanggen66@163.com

Abstract. This article presents a proposal of a heat meter and remote meter reading system for the disadvantages of the hackers very easily using eavesdropping, tampering, replay attack of traditional remote meter reading system. The system selects trusted technology such as, the identity authentication, integrity verifying, and data protection. By the experiments, it is proved that the remote meter reading system of the heat meter can be used to verify the feasibility of the technology, and verify the practicability and operability of data protection technology.

1. Introduction

Hot fee levied on the basis of the construction of heat metering charge system, which is neither scientific nor reasonable. With the increasing number of meter installation, reading meters manually. The work quantity is big, the traditional meter so the problem [1]. Heating is made possible in an optimum condition by a stable running of the remote meter reading system for heat-exchange operation of the respective data are transmitted to the dispatch center, to minimize the thermal energy of the unified allocation [2].

Heat net has a broad, relatively far away from the site vary from one to another, different set of meter reading system using a different network, but the disclosure is a network of a shared transmission medium to transmit data, and transmitting data is a standard format, that is not encrypted, so that the existing system of transmission of sensitive information, such as used by the user for the charging of heat are declined, the hackers very easily using eavesdropping, tampering, replay attack and so means directly on the system of interest [3]. Therefore, By the experiments, it is proved that the remote meter reading system of the heat meter can be used to verify the feasibility of the technology, and verify the practicability and operability of data protection technology [4].

The rest of this paper is organized as follows. Section 2 related to framework for remote heat-meter system. Section 3 related to Trusted service scheme for remote heat-meter system. Finally, Section 4 concludes the paper.

2. Framework for remote heat-meter system

Framework for remote heat-meter system as shown Figure 1. It looks remote meter reading system Based on data center trusted framework requirements. This architecture is divided into the perception layer, the network layer and the application layer. Perception layer node in the on-site was installed by every household heat meter for data exchange in data center. The real-time data acquisition of the intelligent heat meter is carried out, and the data is processed and analyzed, and the results are adjusted according to the analysis results. The data collected by data acquisition gateway, on the
Internet to a data center. The data decryption data center, data reduction, and according to the overall functioning of workstation. Network layer includes LAN and WAN. It is realized communication connection between perception components, or between perception components and gateway (coordinator)[5-6].

3. **Trusted service scheme for remote heat-meter system**
Remote heat-meter system of the trusted service mainly includes identity authentication, data protection technology and system of equipment integrity verification etc.

3.1. **Authentication Methods of Remote Heat-Meter System**
The system once again verifies the integrity of the digital fingerprint, and the digital fingerprint collection device to collect the user's fingerprints when the integrity verification is successful. The client extracts the fingerprint feature template information, and the trusted authentication server interacts with authentication. Remote heat-meter system of user authentication interface as shown in Figure. 2.

3.2. **Device Integrity Verification of Remote Heat-Meter System**
The heat meter device attribute value of the IP address of an instrument, and instrument type T. As a IP address heat meter(network coding, FMU address, Company Code ) A0-A6: 48 36 03 00 00 42 41H, the type of instrument T: 20H or 28H. The attributes are fused to get the device attribute value h(IP || T). All heat meter device attributes of the data packets to form packetized data center to perform integrity verification. Figure 3 is a heat meter integrity verification result of the interface.
3.3. Data protection of Remote Heat-Meter System
Data protection of remote heat meter reading system mainly on smart meters, the transmission address of the data center and heat data was encrypted and decrypted. Figure 4 is a data protection of data center and intelligent heat meter.

Data center includes communication module, decryption module, storage module etc. Communication module is used to send the request data to the intelligent heat meter instructions and receives responses from the intelligent heat scale. The decryption module decrypts ciphertext. The storage module is used to store the decrypted random key, total quantity of heat and cumulative flow value.

The intelligent heat meter includes acquisition module, encryption module and communication module. The acquisition module is mainly used to collect the heat, flow rate and water return temperature of the field. The encryption module is used to generate the dialog key and encrypt the key data. The communication module is the command that receives the data from the data center and returns the encrypted ciphertext data to the data center.

Figure 5 is a safety communication flow chart of data center and intelligent heat meter. Data center every 60 seconds to the smart meter sends a request address instruction, after intelligent heat meter to receive instruction, random encryption of smart meter address and session key and after form ciphertext C1 response. Data center receives the ciphertext C1 is decrypted to obtain the address, heat and intelligent heat meter sends a request to the address instruction, calorimeter capable of receiving the instruction, the data encryption key randomly, form cipher C2 and reply. The details of the request address and the key data of the request are further illustrated in figure 6.

Figure 6 is a block diagram of request address and the decryption algorithm. After receiving instruction of intelligent heat meter, the random number generator is used to generate the random key key_{i+1} and save it. Use the first i session random key key_{i}, encrypted processing of its own address, d,
and key_{i+1} at the random key, to get a cipher C_{1} response. Data center after receiving the ciphertext C_{1} intelligent heat meter. With random key key, the decryption get clear data, get the smart heat meter address d and the random key key_{i+1}. Heat request with a request of an encryption and decryption algorithm and decryption algorithm is the same as the address, the heat related data p is decrypted.

**Figure 6.** Block diagram of request address and the decryption algorithm

Figure 7 is a i+1 random session key verification flow. After data center decrypts the random key_{i} and heat p content. Judging whether key_{i+1} value is equal to the random key key_{i} value. If equal, then, we store the heat p and the random key key_{i+1}, discard the random key key_{i} and waiting for the next session. If not equal, discard the heat p and the random key key_{i+1}, end the session and determine the exception.

**Figure 7.** Block of i+1 random session key

4. Conclusion

Every advances in industrial technology are all aimed at reducing costs and creating efficiencies of the meter reading through technical innovation reduce the wastage of the energy transmission, at the same time reduce the cost of management. In the urban heat supply industry, the use of computer technology to monitor the operation of the heat network can make full use of energy and reduce environmental pollution. With high reliability of network transmission data, it has great advantages in construction cost and maintenance cost, and it can improve work efficiency and production management level for heating enterprises.

It is of great practical significance and extensive application value to ensure the safe and stable operation of heat supply and heat network. With the improvement of network and the further reduction of cost, the network based remote monitoring system will be more widely used.

**Acknowledgement**

This work was financially supported by the National Natural Science Foundation of China (Grant No. 6154055), the Doctor's Scientific Research Foundation of Hezhou University (No.HZUBS201506), the Dean Project of Guangxi Key Laboratory of Wireless Wideband Communication and Signal Processing, China, the Science Research and Technology Development Program of Hezhou (No. 1707041), and Hezhou University of scientific research project in 2017(2017ZZZK03).

**References**

[1] Krejcar, O., Frischer, R., Real Time Voltage and Current Phase Shift Analyzer for Power Saving Applications, SENSORS, 2012, Volume: 12, Issue: 8, Pages: 11391-11405, ISSN: 1424-8220

[2] MOCZAR G, CSUBAK T and VARADY P, Distributed measurement system for heat metering and controlling, IEEE Transactions on Instrumentation and Measurement, Vol 51(4), pp.691-694, (2002).
[3] Liu Yansong, Probing into some Questions about heating measuring and charging of resident building, China Construction Heating&Refrigration, pp.21-23, Jan. (2005).

[4] Chen Yinkang, Li Xiangyang, Xiao Jing, The hardware design of concentrator for wireless intelligent meter reading system, Components and IC, pp.37-40, Jan. (2005).

[5] Robert F B, Quartz capillary flow meter for gases, Review of Scientific Instruments, Vol 75(3), pp.772-779, (2004).

[6] Faruk Mendi and Kuriulus Boran, Fuzzy controlled central heating system, International Journal of Energy Research, pp.1313-1322, Jan. (2002).

[7] Horalek, J., Matyska, J., Sobeslav, V. (2013). Communication protocols in substation automation and IEC 61850 based proposal. CINTI 2013-14th IEEE International Symposium on Computational Intelligence and Informatics, Proceedings, art. no. 6705214, 2013, pp. 321-326.