The Design Of Bluetooth Voice Source Wireless Real-time Voice Encryption System

Hai Hui Huang[1, a], Jiu Ran Liu[2, b] and Yao Deng Wang[2, c]

[1]School of software engineering, Chongqing University of Posts and Telecommunications, chongqing 400065, China;

[2]School of software engineering, Chongqing University of Posts and Telecommunications, chongqing 400065, China.

[a]huanghh@cqupt.edu.cn, [b]1735088153@qq.com, [c]179923937@qq.com

Keywords: Voice Source Real-Time Encryption, Voice Encryption, Logistic mapping

Abstract. The paper proposes a new encryption method named as wireless bluetooth vioce source real-time encryption method which adopts encryption algorithm of improved Logistic mapping, in order to solve wiretapped problems, improve the security of the voice transmission and ensure the integrity of the voice signal.

1. Introduction

In today's society is the information age, information security more and more gets people's attention and becomes a more important research subject. Voice is the basis of mutual exchange of information, voice communication encryption is an important means of preventing voice signal from being tapped, falsified, intercepted and so on. For voice communication security problems, there are mainly two methods which are the security mechanism in the mobile communication and end-to-end encryption method of mobile communication. Mobile security mechanism considers the security issues from the angle of the operators. voice encryption operation and management are performed by the operators, the key lies in the operators' hands, and operators choose simple encryption algorithm to reduce cost, so its safety is lower. By comparision, the end-to-end encryption method is mainly aimed at the wireless channels encryption, the security of voice is improved to great extent. The disadvantage of the end-to-end encryption method is that only between mobile terminals and base stations is voice in the form of ciphertext, it is in the form of plaintext each two base stations, so that voice signal is easy to be wiretapped. Now a new method of mobile terminal encryption will be proposed, which guarantees voice signal in form of ciphertext between sender and recever in order to improve the integrity and ssecurity of voice signal.

2. Encryption Algorithm

2.1 Logistic mapping

Chaos is a state of motion, which is extremely sensitive to initial value and easily shows randomness and unpredictability. Chaos system is a kind of nonlinear system, obviously differ from other motion, and has some characteristics such as sensitivity to initial value and paramters, ergodicity, long-term unpredictability, boundedness.

Logistic mapping [1] is a classical mapping which is very simple and widely used. Even though thesimple and deterministic, the madel has very compex dynamic behaviors. Logistic mapping is defined as follows:

$$x_{n+1} = \mu x_n (1 - x_n) \quad (1)$$

The formula (1) shows that the sequences generated by this map are determined by x_0, μ, $x_n \in (0,1)$, $\mu \in (0,4)$. This mapping is sensitive to initial value. if x_0, μ have minorchanges, the result will completely difference. μ is a branch parameters of the mapping, as the change of value of μ, the map will appear different charaterics. there will be bifurcation cycle 1, 2, 4, …… , 2^n.

As shown in figure 1, when μ is equal to 4, the system presents completely chaotic state. However, Logistic mapping also exists security issues such as unequal sequence within the scope of (0,1), blank windows, stablity windows and so on. Logistic mapping is improved in response to these problems [2], system is defined as follows:

$$x_{n+1} = \mu k x_n (1 - x_n) \quad (2)$$

The values of x_0, μ are unchange, and $k > 1$, the change of system's chaotic state is only determined by , has nothing to do with x_0, μ. When k is equal to a certain value, the system will be always completely in the state of chaos.

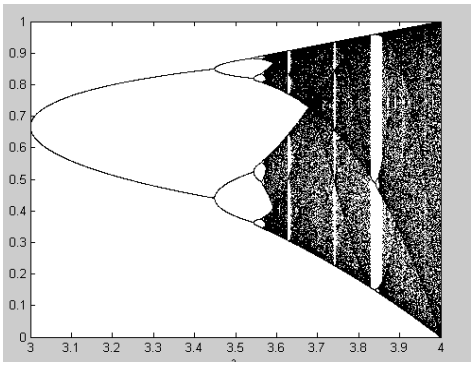

Fig. 1 bifurcation diagram

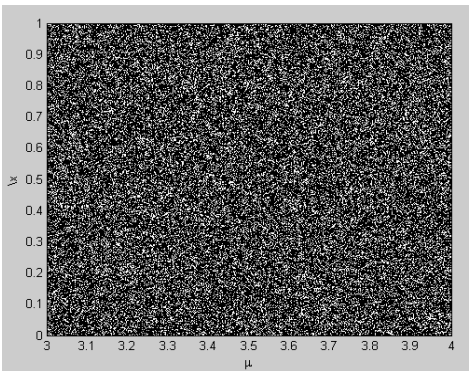

Fig. 2 bifurcation diagram of improved Logistic mapping

2.2 The choice of encryption algorithm

The volume of wireless bluetooth encryption device is smaller so that it is more convenient to carry. CPU, internal memory and cache of the device are limited, so data transmitted can't too comlex and large to be processed; during the transmission the processing time of voice is strictly limited, ITU-T phone business provides that delay time of one-way transmission of voice must be less than or equal to 150 ms, if delay times are greater than this delay time, voice quality will be seriously affected, the user will hear intermittent sound and clearly feel delay; voice transmission is real-time transmission, and low luctility. In summary, the selected encryption algorithm should be not only good safety but also low algorithm complexity. At the same time, if the complexity of algorithm is lower, its security is relatively lower. So the selected encrytion algorithm itself has certain security feature. Therefore the selected encryption algoritnm should be under the condition of guaranteeing certain strength of security relatively sampler in order to ensure voice real-time transmission, lower latency and better voice quality.

According to the above mentioned, Logistic mapping has simpler struture, lower complexity and all characteristics of chaos, especially more sensitive to the initial and long-term unpredictability, so it will be more suitable for real-time voice transmission.

3. Bluetooth voice source wireless real-time voice transmission system

Bluetooth[4] is a short-range wireless transmission technology, mainly in the 2.4GHz ISM band. Bluetooth protocol uses a layered architecture, mainly divided into the underlying hardware module, intermediate protocol and application layers. Wireless Bluetooth voice transmission system mainly uses Redio Frequency (RF), BaseBand (BB), Link Management Protocol (LMP)of the underlying hardware modules, Logic Link Control Protocol and Adaptation Protocol (L2CAP), Cable Replacement Protocol RFCOMM, Service Discovery Protocol (SDP), The Binary Phone Control Protocol (TCS) of intermediate protocol and the corresponding high-level application protocol. Bluetooth core protocol is the underlying protocol module, especially BB. BB can guarantee physical connection between the Bluetooth radio unit within the piconet and provide two different physical links that are synchronous connection-oriented link (SCO) and asynchronous connectionless link (ACL), can achieve multi-channel data transmission on the same radio frequency, be responsible for FM and Bluetooth data transmission named information frame. ACL transmits data except for voice, SCO is used for voice transmission. Different types of data will be provided dedicated channels. Bluetooth audio is achieved through transmitting directly SCO packet

on the baseband. BB can only handle digital signal, so an analog signal that must be converted into a digital signal can be transmitted by baseband. all voice packets in the process of transmission could be processed by cyclic redundancy check or forward error correction, and encryption. In the Bluetooth wireless voice transmission system, voice signal fter being sampled, quantized, encoded is converted into digital signal, and digital signal is transmitted via the SCO link of baseband.

3.1 hardware design

Bluetooth voice source wireless real-time voice transmission adds bluetooth encryption devices in front of mobile terminals on the basis of the tranditional mobile commucation system, as shown in figure 2, voice is encrypted before entering mobile terminals. The encryption device mainly contains voice processing module and bluetooth module as shown in figure 3, the two modules transmit digital audio signal through I2S.

Fig. 2 Bluetooth voice source wireless real-time voice transmission process

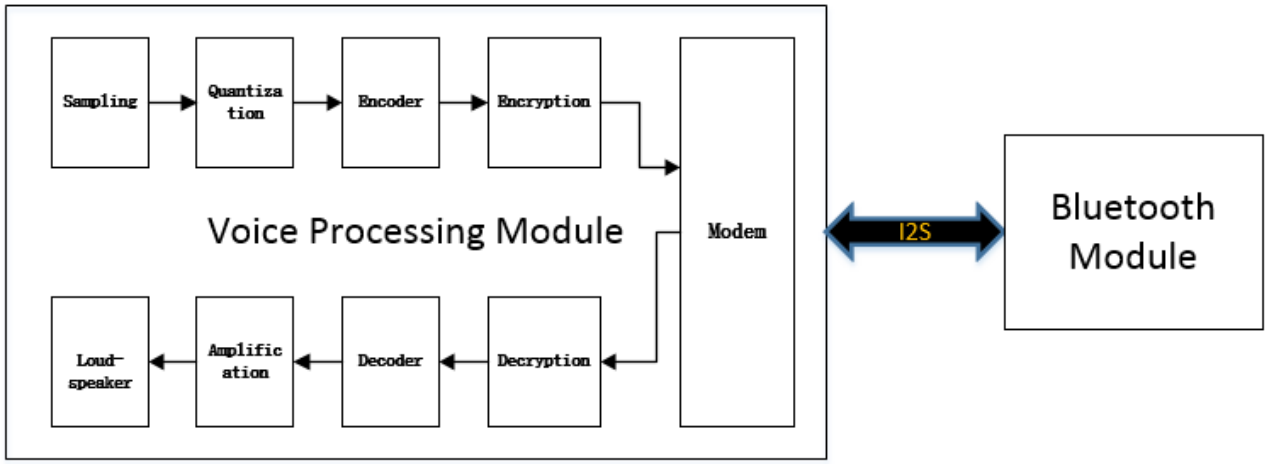

Fig. 3 bluetooth encryption device logic module

The voice processing module has mainly sampling, quantization, codec and encryption of voice. the encrypted digital signal with pseudo-randomness can't be identified by mobile terminals[5,6,7], so the voice processing module must modulate the encrypted digital signal into class vioce signal with voice feature before entering mobile terminals in sending end and demodulate class voice signal into encrypted digital signal with pseudo-randomness before enterring bluetooth encryption device in receiving end.

The voice processing module adopts STM32F4DISCOVERY[8,9,10]. STM32F4DISCOVERY bases on STM32F407VGT6 chip, STM32F407VGT6 microcontroller has 1M FLASH memory, 192 k RAM, LQFP100 encapsulation, kernel ARM architecture(M4 32-bit MCU with floating-point processing unit (FPU)), 3 ADCs, 15 communication interfaces. LIS302DL used as three axis digital output accelerator can improve the speed of data processing. Audio MP45DT02 used as digital microphone, signal coming from the microphone is digital directly,which is more convenient and saves the time converting analog into digital signal. CS43L22 used as audio DAC can convert digital signal into analog signal. embedded debuggging tool interface ST/V2 complies and debugs program, and which the running time of program can be seen directly is easy to judge whether the selected algorithm meets the limited time. According to the characteristics of the STM32F4DISCOVERY, it meets the required speed and storage capacity of bluetooth encryption device.

Bluetooth module adopts CC2564[11], the module has some basic functions, mainly sends the encrypted vioce to mobile terminals in sending end and receives the encrypted vioce from mobile terminals in receiving end by radio frequency.

3.2 systematic design

Bluetooth voice source wireless real-time voice encryption and decryption process as shown in figure 4. In sending end voice entering wireless bluetooth encryption device through a microphone is sampled, quantized, and coded, which makes analog signal converted into digital signal. Then the digital signal is encrypted by Logistic map, and encrypted voice is also modulated into class voice with voice feature. in turn, the voice signal is sended to mobile terminals by RF, further transmited to the mobile communication network.

In receiving end mobile terminals receives the voice signal from the mobile communication network, and transmits voice signal to bluetooth encryption device by RF. voice signal is demodulated into digital signal with pseudo-randomness, and then decrypted in accordance with the inverse Logistic map. In turn, the digital signal is converted into analog signal by D/A. voice signal is amplified and restored to original voice. the original speech is spread out through the speaker.

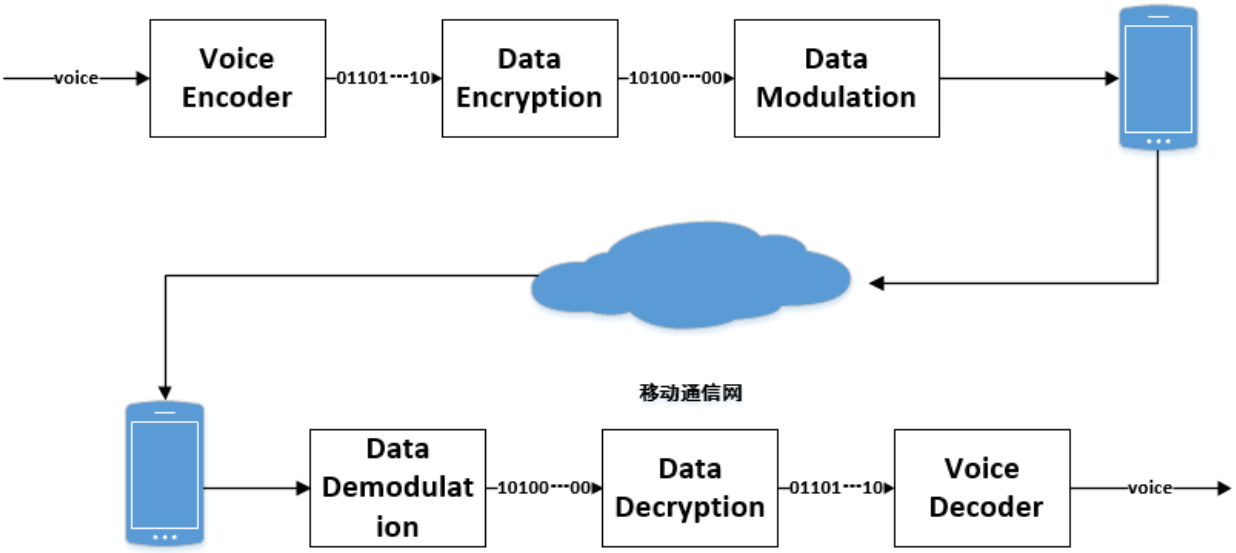

Fig. 4 bluetooth voice encryption transmission process

4. Summary

Bluetooth voice source wireless real-time encryption method will resolve problems that the traditional mobile communications end-end encryption method exists such as easily wiretapping, improve the security and ensure the integrity of speech data transmitted, but its real-time requirements is relatively high, the complexity of the selected encryption algorithm is not very high since the processing ability of the encryption module is very limited. On the premise that the voice quality dosen't affect during the call, further real-time will be enhance and delay time will be reduced.

Reference

[1] Shaojang Deng, Di Xiao, Fenghua Tu: submitted to Journal of Chongqing University(2004).

[2] Dong Wu, et al. Chaotic Encryption Algorithm: Two-Dimensional Arnold Mapping and Logistic Mapping improved. J. Information & Communications. 1(2014):41-42.

[3] Khare, Ankur A., P. B. Shukla, and S. C. Silakari. Secure and Fast Chaos based Encryption System using Digital Logic Circuit. J. International Journal of Computer Network & Information Security6.6(2014).

[4] Xinyu Wang. Technology of Voice Chaotic Encryption and Decryption via Bluetooth Real-time Wireless Transmission. D. Guangdong University of Technology (2015).

[5] Chumchu, P., A. Phayak, and P. Dokpikul. A simple and cheap end-to-end voice encryption framework over GSM-based networks. Computing, Communications and Applications Conference(ComComAp), 2012 IEEE, 2012:210-214.

[6] Biancucci, G., A. Claudi, and A. F. Dragoni. Secure Data and Voice Transmission Over GSM Voice Channel: Applications for Secure Communications. 2013 Fourth International Conference on Intelligent Systems, Modelling and Simulation (ISMS 2013) IEEE Computer Society, 2013:230-233.

[7] Yucun Yang, et al: submitted to Journal of Chongqing University of Posts & Telecommunications (2009).

[8] Yaru Li. Wireless Voice Transmission System Based on STM32. D. BeijingUniversity of Posts and Telecommunications(2013).

[9] STM32F4xx on http://www.st.com.

[10] STM32F407 on http://www.st.com.

[11] CC256X on http://www.ti.com.