Computer Life (CPL) ISSN: 1819-4818
DELIVERING QUALITY SCIENCE TO THE WORLD

# Research on Network Security in Wireless Sensor Networks

Xingcheng Ran

HeXi University, Zhangye, 734000, China

*Abstract: This paper studies the introduction and characteristics of ZigBee protocol and its routing mechanism. It compares several methods of key management, analyzes the simple encryption algorithm and the encryption method of DES, and finally implements the security of wireless sensor networks. Analyzes and summarizes the possible attacks and solutions that wireless sensor networks may encounter when transferring files. Research shows that wireless sensor networks are representative of computers, and his security issues are also a key issue.*
*Keywords: Wireless sensor network; Access control technology; Key management; Security.*

## 1. INTRODUCTION

Researching wireless sensor networks can extensively understand the leading technologies of current computers, and can effectively prevent attacks and destruction when transmitting data, and achieve higher security. Therefore, this paper first introduces the trusted access control method for wireless sensor networks, then studies the ZigBee protocol, and finally obtains the code for data encryption and decryption so as to solve the attacks in data transmission.

## 2. INTRODUCTION TO ZIGBEE PROTOCOL

Wireless sensor network nodes need to have wireless network protocols for data exchange. Wireless sensor requirements are difficult to achieve for traditional wireless sensors. In this way, the ZigBee protocol has emerged. Zigbee is based on IEEE 802.15.4. However, the low-level physical layer protocol can be handled by the IEEE, so the Zigbee Alliance expands and standardizes the IEEE. Zigbee is mainly used for short-distance wireless connection. These sensors require little energy to transfer data between sensors, so it has high communication efficiency. Each ZigBee network module is a mobile network base station that can communicate with each other; and Zigbee network connection is more convenient, as long as it wants to connect the basic can be, and the connection is still very good. It is suitable for low-cost equipment; low-volume equipment; batteries are used to maintain the machine; GPS is ineffective.

Table 1. ZigBee protocol stack model

| | | |
|---|---|---|
| Application convergence layer | | ZigBee Alliance |
| Application interface | | |
| Security layer | | |
| Network layer | | |
| Data link layer | IEEE | |

| | | |
|---|---|---|
| Network physical layer | | |

## 3. ZIGBEE ROUTING MECHANISM

In fact, routing is generally difficult to find, but there are methods to discover that it is the data frame. The small frame can play a great role. As long as he moves and wants to achieve the goal, the route has already been discovered at the time of application. In fact, it is also the role of nodes, small nodes are constantly moving, according to their own tasks, the purpose of moving, from the beginning to the end of the process there are. .

a). Calculation of Routing Cost

There are many paths to the ZigBee routing algorithm, but not everyone is correct and not everyone is the most effective. At this time, you need to choose and judge. It is very important to create a perfect path.

Specifically, for example, there is a path p of length [L1, D2, ... DL] of the device [L1, D2, ... DL], where the length of a sub-section [Di, Di+1] is 2, and then the total sum of this path is The following formula:

$$C\{P\} = \sum_{i=1}^{L-1} C\{[Di, Di+1]\} \tag{1}$$

A link cost is calculated by each sub-section and the following is a function of the internal link cost:

$$C\{l\} = \begin{cases} 7 \\ \min\left(7, round\left(\frac{1}{P_e^4}\right)\right) \end{cases} \tag{2}$$

The cost of routing reflects the number of times a data packet was correctly forwarded according to the link. The protocol stack provides two options, set nwkrepoertconstantcost, and then the cost value of the connection is a constant 7, determined by calculation, otherwise. With some flexibility, we can try to send a beacon or data frame and calculate packet loss based on the sequence number of the data. This is a relatively low but accurate probability calculation method.

b). Routing table

Table 2. Routing table

| Name | Size | Description |
|---|---|---|
| Destination address | 2B | The destination device address of this path |
| Status | 3bit | Route discovery status<br>Ox0:ACTIVE<br>Ox1:DISCOVERY_UNDERWAY<br>Ox2:DISCOVERY_FAILED<br>Ox3:INACTIVE<br>Ox4-ox7:RESERVED |
| Next hop address | 2B | Next hop device address on the path to the destination device |

c). Route discovery

There are many ways to route, and when you choose a good path, it's a problem to start. When the node starts to start, we must start work. First, we must first determine the inequality A<D<A+Cskip(d-

1). If D satisfies the formula, the result is obtained and the next goal is displayed. Going to the next step, the formula is:

$$N = A+1+\left|\frac{D-(A+1)}{Cskip(d)}\right|\times Cskip(d) \tag{3}$$

If this is not the case, it is necessary to return to the previous level and the node's information data continues to be routed upwards.

## 4. DATA ENCRYPTION

### 4.1 Simple encryption algorithm

C language is widely popular in the world and is a promising computer high-level language. It is rich in functions and flexible. It can be used to write software. C language can be used to encrypt data easily. The specific procedure is as follows:

```
#include “stdio.h”
#include <string.h>
void main ( )
{
char name1[16];
char name2[]={“love”};
printf(“Please enter your password \n”);
scanf(“%s,name1);
if (strcmp (name1 ,name2)==0)
{
printf(“111222”);
}
else
{
printf(“The password is correct!”);
}
}
```

From this we can see that first define name1 and name2. When the code is debugged without error, the word “please enter the password” appears. In this way, we can input the password set in advance, such as “111222”. After entering the correct password, the password will be displayed. This will read LOVE data.

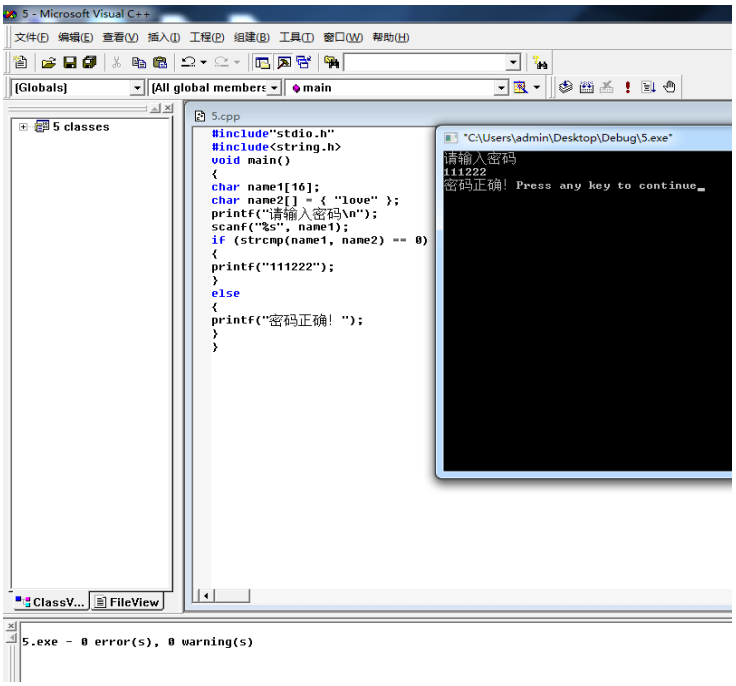


Figure 1. Simple data encryption operation diagram

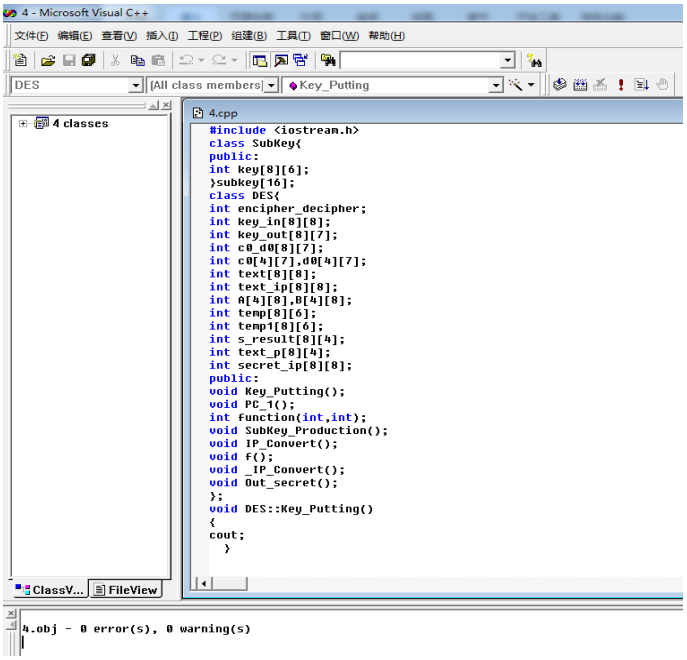


Figure 2. DES encryption algorithm C language implementation

### 4.2 DES encryption

DES, the data encryption standard, is an algorithm that uses key encryption. DES encryption In each round of encoding, a 56-bit full key yields a 48-bit "per round" key value. The DES software takes a long time to decode and the hardware decoding speed is very fast. Fortunately, such devices were not manufactured by most hackers at the time. In the last century, if you wanted to create such a computer, it would take a huge amount of money and it would cost tens of millions of dollars. It takes 12 hours for encryption and decryption to get results. So DES is considered a very powerful encryption method. With the development of the times, computer technology is also advancing. Modern computers must have been reduced to 100,000 US dollars, and 100,000 US dollars have been used to protect 100

million yuan of funds. The difference is huge and the safety factor is relatively low. Therefore, using DES should be used to protect ordinary servers. Use C language programs to write encrypted programs.

The following is a detailed algorithm:

```
#include <iostream.h>
class SubKey{
public:
int key[8][6];
}subkey[16];
class DES{
int encipher_decipher;
int key_in[8][8];
int key_out[8][7];
int c0_d0[8][7];
int c0[4][7],d0[4][7];
int text[8][8];
int text_ip[8][8];
int A[4][8],B[4][8];
int temp[8][6];
int temp1[8][6];
int s_result[8][4];
int text_p[8][4];
int secret_ip[8][8];
public:
void Key_Putting();
void PC_1();
int function(int,int);
void SubKey_Production();
void IP_Convert();
void f();
void _IP_Convert();
void Out_secret();
};
void DES::Key_Putting()
{
cout;
  }
```

Figure 2 shows that there is no error in code verification using C language. First, the subkey is defined as a class, and the number of object groups of subkeys is defined, and it is judged whether to encrypt or decrypt.

## 5. NETWORK LAYER ATTACKS AND DEFENSES

Wireless sensor networks are very dynamic and do not have a fixed center. They are generally placed on the enemy to monitor the enemy and also on the enemy who cannot be reached or survive, so that no one can understand it. However, such an approach is also dangerous and challenging. If the power is low, there is no way to change the battery. Moreover, the computing power and efficiency of the general sensor processor are very limited. According to the characteristics, it can also be known that the communication distance is short, the function is low, the communication bandwidth and range are very limited, the sensor node is a micro-component, and the storage space is very high. With these characteristics, the security of the wireless sensor network must be challenged. There are also many common wireless sensor network attack methods and their defense techniques.

There are numerous nodes in the sensor network. Each node represents a different meaning. Nodes continue to jump to complete the communication between them, to achieve the purpose of transmission, in this process the enemy will take the opportunity to disrupt their transmission, to destroy and steal data. If you want to attack the network layer, the enemy must pay attention to the link layer and network layer of the network. The following are the possible attacks and corresponding solutions during data transmission.

a). Sinkhole and Wormholes attack: Under this attack, absorb the data circulating in one area, and then attack and destroy its data. Since the data transmission destinations in the sensor network can mutually know each other, that is, as long as there are high-quality routes, the nodes can be destroyed illegally, which will directly affect the communication functions of the sensor nodes. Therefore, the Sinkhole attack is very sensitive to the sensor network.

Solution: In this protocol, although the location of each node is not fixed, it is still unique, so that a topology can be established between them. If there is a hacker attack, it will inevitably go through the topology. As long as the local node is destroyed, the attacker will be seen. At the same time, you can also design routes to defend. The method of resisting Wormhole attack by non-GPS nodes and GPS nodes collaborated by Kwok.

b). The Sybil attack: Douceur gave a concept for the first time and is still circulating today. It is the Sybil attack concept. Under such attacks, identities are the most important. An attacker can apply a certain method to have many identities. Then he can enter the network with fake signals. Then he combines with the nodes in the network to transmit data. These fake nodes can then attack these. data. The harm caused by the Sybil attack to the sensor network was analyzed by Newsome.

Solution: To solve this problem, there is a way to transfer data between nodes. A unique key must be established between them to verify the identity of the other party through the protocol. Authenticated neighboring nodes or encrypted links can be implemented by negotiating keys. However, attackers also have methods. They also have their own keys so that they can attack, but we can also limit them.

c). HELLO Flood Attack: Many protocols require that a node broadcast a HELLO packet to find its neighboring node and receive the packet's node, which will ensure that it is sent on the sending side. Therefore, in the network node, trying to use the route to communicate with the base station, but due to a subset of the attacker, the distance is far, so that the sandwiched file is easily lost, so more and more losses will be unthinkable.

Solution: Trust the base station. If you want to attack, you need to authenticate each other's identity with neighbors before they can cross the border. The base station plays a very important role. It can limit the number. If the attacker wants to act this time, it must have a large number of with node authentication, the more authentication, the more obvious the goal is and it will attract attention.

Table 3. Cyber attacks and defenses

<table>
<tr><td>Network level</td><td>Attack method</td><td colspan="2">Defense means</td></tr>
<tr><td rowspan="2">Physical layer</td><td>Physical destruction</td><td colspan="2">Node camouflage and covert</td></tr>
<tr><td>Congestion attack</td><td colspan="2">Low duty cycle, frequency modulation</td></tr>
<tr><td rowspan="3">Link layer</td><td>Unfair competition</td><td colspan="2">Use non-priority and short-frame strategies</td></tr>
<tr><td>Exhaustion attack</td><td colspan="2">Set the competition threshold</td></tr>
<tr><td>Collision attack</td><td colspan="2">Listening channel, retransmission mechanism</td></tr>
<tr><td rowspan="6">Physical layer</td><td>Select forward attack</td><td rowspan="6">Link Layer Encryption and Authentication Mechanism</td><td rowspan="6">For internal attacks, link layer encryption, key management, multi-path routing, self-location, ID number and other methods</td></tr>
<tr><td>Sinkhole attack</td></tr>
<tr><td>Sybil attack</td></tr>
<tr><td>Wormholes attack</td></tr>
<tr><td>HELLO Flood attack</td></tr>
<tr><td>Confirming the spoofing attack</td></tr>
</table>

## 6. SUMMARY

This article introduced the ZigBee protocol and researched and improved the ZigBee protocol. Combined with key management, data encryption and decryption are studied, and data encryption and decryption procedures are made. Finally, the security issues of wireless sensor networks are studied, and the possible attacks in the network data transmission are proposed, and solutions to these attacks are proposed.

## REFERENCES

[1] Akyildiz I F, Su W, Sankarasubramanian Y, et al.A Survey on Sensor Networks [J], IEEE Communications Magazine, 2012, 40(8): 102-114

[2] Chan H, Perring A. Security and Privacy in Sensor Networks [J], IEEE Computer, 2013, 36(10):103-105

[3]Perrig A Szewczyk R, Wen V, et al. SPINS : security protocols for sensor networks[J], Journal of Wireless Networks, 2012, 8(5):521-534

[4]Perrig A, Stgner D. Security in Wireless Sensor Networks [J], Communications of the ACM, 2014, 47(6):53-57

[5] R. Brooks, P. Ramanathan, A. Sayeed. "Distributed target classification and tracking in sensor networks", Proc. IEEE 91(8): 1163-1171, (2013).

[6] A. Wood, J. Stan kovic, "Denial of service in sensor networks", IEEE Comput. Mag. 35 (10): 54-62, (2012).