In Thing Networking RFID System Node Communications Security Research

He Weigang, Zhang Fan, Li Zhenglin, ZhangYin, Wu Qiqi

College Of Electric And Information
Guangxi University Of Science And Technology
Guangxi Liuzhou 545001 China

Keywords: Internet of Things ;RFID； Communications security ;data encryption

Abstract

The thing networking unceasing development and the application, while take to us to live convenient, also gave the informationsecurity to bring the challenge.Communications security question faces which in view of the networking architecture and the RFID system; Has studied in with emphasis the networking sensation level the RFID system communications security, has introduced one kind of 2 RFID architecture, and has given the corresponding status authentication and the data encryption solution based on this structure.Has the promotion application value.

1 Foreword

The ITU clearly pointed out in its annual report, the goal of the development of Information Communication Technology has changed, from being able to connect anyone, to being able to connect anything, at anytime in anywhere. All things connected forms the Internet of Things (IOT). In China, the report on the work of government of 2010 explained IOT as: such a network, via information sensing equipment, in accordance with the contract agreed, connecting anything to the Internet to make the exchange and communication of information, in order to realize the intelligent recognition, tracking and monitoring.[1,2,3]

The Prime Minister Wen put forward the construction of "Sensing China" in his inspection visit to Wuxi. Currently, IOT has been listed formally as one of five national emerging industry of strategy. The plan of The Twelfth Five-Year Guideline clearly named IOT technology as an important project with strong support, turning it into a national emerging industry of strategy, and a prominent growth point of economy. Since the IOT broaden the range of the Internet, the problem of its safety and privacy has been more severe. Faced with the circumstances of the application of the IOT on a large scale, the task of speeding up the technology of security has been imminent[4,5,6]

2 The system structure of the IOT and the security of the RFID communication.

2.1 System construction

The IOT combines the technology of sensor, of the computer network, of the intelligent control together, not only realizing the communication between one and another, but also between one thing and another, even persons and things. Nowadays, we generally define the system construction of the IOT into three layers, sensing layer, network layer and application layer, as widely recognized[7,8,9].

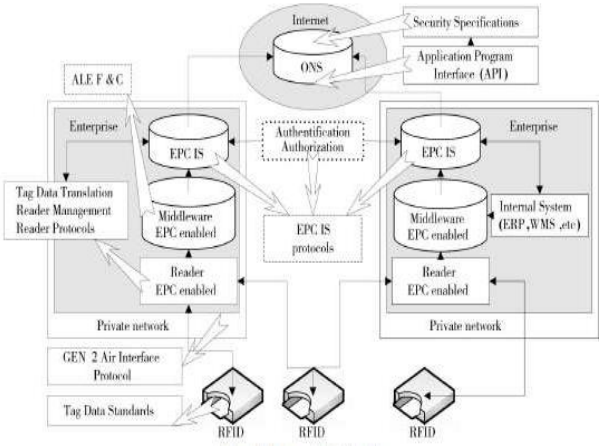

fig1 architecture of the Internet of things

As picture 1, lies in the bottom is the sensing layer, in charge of collecting different kinds of information, consisted mainly of radio frequency identification tab, different kinds of sensors, sensor network gateway, M2M terminals. In the middle is the network layer, in charge of the transformation and distribution of information. The IOT application, connected to the network by wireless or wired means, provides service of transmit and share of information to the outside world, with the support of network. The application layer, on the top, provides the support and management of execution, responsible for the transfer control, storage, correlation and analysis of information sensed, for supporting the flattening of distributed information processing framework, making use of the advantages of network

computing, distributed computing, cloud computing to the fullest.

2.2 The security of the RFID communication

In the three-layer construction of the IOT, the application of the network layer relies on all the network existed, so the safety of it, considering the rearrangement and design unavailable. Application layer is a variety of upper services, platform independent implementation, the safety of it largely relies on the lower layer. In the bottom, the sensing layer, at the end of the IOT, in charge of the collection of different kinds of information, is the base of all applications of the IOT. Usually, the processing capacity of sensing layer is week, unable to use strong encryption algorithm. Thus, how to ensure the integrity, confidentiality and credibility of information acquired by the RFID node equipment, poses a challenge to the safe application of the IOT.

Explicitly speaking, the threat of the safety of the RFID mainly focuses on the intercept of the RFID tab information and crack of the RFID information. When the RFID tab information is fetched illegally, the attacker could use the RFID system without authorization, such as faking, especially the unsafe FRID tab, which will release some sensitive information, having the hidden troubles of cheating, replay, interference, hacking, cloning and virus, furthermore, having a bad influence on the safety of the whole RFID system. It is an important step, in designing the RFID system, to ensure the safety of RFID communication, which is also fundamental for the utility of sensing information of the IOT

3 The study on safety of the RFID system

31 The Security of the RFID communication

The RFID technology, as one of the core technologies of the IOT, is a non-contact, automatic identification technology, which can work under all kinds of bad circumstances. By sending radio frequency signal to identify target object automatically and get the data related, the RFID technology can identify the object with high speed and multiple tabs at the same time with operation fast and convenient.

A typical RFID system usually consists of three parts: electronic tag, reader-writer, middleware and database. In the application of the IOT, large amounts of RFID tabs and reader-writer are needed.Between nodes, much communication is taking place. In order to reduce the burden of the reader-writer and make it more manageable, we could use the two-layer GRID construction, shown as picture 2. The secondary RFID reader-writer is faced with the terminal nodes of the RFID tabs directly, in conduction of the collection of identification and management of information in the bottom. In the layer, the RFID device, though week in processing capacity, huge in quantity, is generally in charge of 10-30 RFID tabs of each secondary RFID. Senior grade RFID reader-writer, in control of secondary reader-writer by connecting its information, can also face the RFID tab terminal nodes with higher qualification of security of data directly. The device, in this layer, is powerful in processing capacity, small in numbers. Each senior grade RFID reader-writer can take charge of 5-20 secondary reader-writer nodes or terminal nodes of RFID tabs.

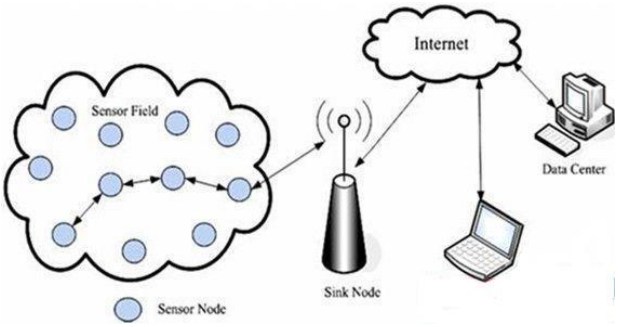

fig 2 rfio system structure

Different methods of identify authentication and data encryption can be used in the RFID system shown as picture 2 to reach the balance of the safety of data and the performance of communication. As to the secondary RFID reader-writer and nodes of the RFID terminal device, for week in processing capacity and lower demand for security in itself, we could use group identity authentication and symmetric encryption algorithm with low processing capacity, better performance. As to the senior RFID reader-writer and the outside world, for powerful in processing capacity and higher demand for security in itself, we could use end-to-end authentication and asymmetric encryption algorithm, more complicated.

3.2 The communication between secondary nodes and the outside world

The same management key is preset in the secondary reader-writer and the terminal nodes of its management. The so-called group identity authentication is to carry out the identity authentication of multiple terminal nodes in a time; the reader is set up to manage the terminal node identity information, and the identity authentication is only required to check the table. When communication is needed between devices, the secondary RFID reader-writer broadcasts the authentication message around, using preset management key to encrypt their identity, and then send the authentication replay message to the nodes of secondary RFID reader-writer, which makes the decryption of the information received, if correct, make data encryption using management key, sends Start messages, starting the exchange of information with the terminal nodes.

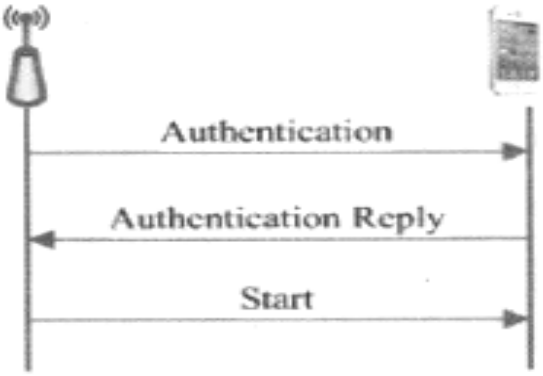

fig 3 level 2 RFIO read-write device node authentication flow chart

The process of reading and writing server-side key enabling codes are as follows RFID terminal parts are relatively simple no longer give the:

```
int startConnect(int to) //to
{
  boardAuth(); //
  int st = getClock();
  while(1)
  {
    int end = getClock();
    if(end □ st > to)
      break;
    if(end □ st > 10)

boardAuth();
    recvMsg();
  }
}
void recvMsg( )
{
  char *msg = getMsg();
  unencypto(msg, getPSK());
  if(TYPE(msg) == AUTH_REPLY)
REPLY
  {
    if (authList (msg))
START
      sendMsg(AUTH_START);
  }
  else if((TYPE(msg) == DATA_TEMP)
  .....
}
```

3.3 The communication between the first class nodes and the outside world

In order to guarantee the security of the first class nodes reader and the mutual authentication between the two sides, we design the authentication mechanism that does not involve the third party to achieve the identity authentication and key agreement. In this authentication mechanism, the first class reader and the outside nodes should have a common authentication key K before the mutual authentication, assuming that it is safe and not known to the third party. Its mechanism is shown in figure 4.

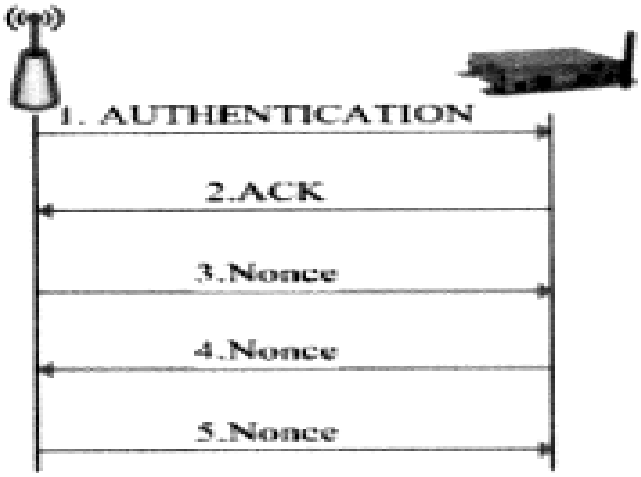

fig 4 status authentication agreement work flow chart

Mutual authentication of the implementation process is as follows

1) Authentication message is sent from secondary nodes to first level nodes.

2) First level nodes reply with ACK message.

3) The secondary node receives a ACK, generates a random number A and uses public key K encryption, then uses the ID number of a node to generate the NONCE to send to the first class node.

4) The first level node receives the NONCE and compares it with its own ID number,if the same as the K, the decryption of the random number A and the random number B, which uses the public key to encrypt the formation of NONCE and then sends to the secondary node;if not, stops.

5) The secondary node will receive the NONCE once again sent to the first level node, and then use public key to decrypt, extract the random number A 'and A contrast with their own, the same, then the two level nodes believe that authentication is successful; otherwise, the authentication fails.

6) After the first level node receives the NONCE, the public key K is used to decrypt the NONCE, extract the random number B' and compare it with the B, and compare it with the B.If the same, the first class nodes see the certification as a success; otherwise, the authentication fails.

The mutual authentication is generated by random number to identify each other and examine the authenticity of purpose. In the fifth step, the secondary node sends NONCE again to

make the first level node be able to verify the random number B. After the identity authentication, the two sides can use their stomach to generate the key data encryption, mutual exchange of information.

4 Summary

This paper introduces the system construction of IOT and the security of RFID communication, and the structure of RFID system in the environment of IOT, giving the corresponding identity authentication and data encryption scheme. With the increasing development of IOT, in the near future, we will see the application of it in our life on a large scale, correspondingly, the safety of sensing information more mature.

Fund project: supported by the National Natural Science Foundation Project (61464001)

References

[1] Luo Hengfeng, Zhu Jianhong, Li Jinhua, Yang Xiaoming, Li is attractive. RFID system safety assessment target system and appraisal model(J). Electronic products reliability and environmental testing, 2009,05:56-59.
[2] Liu Chenghua, He Shengyu. Studies J based on the RFID technology agricultural product physical distribution(system). Rural economy, 2012,10:91-94.
[3] Qian Ping Wu Meng. It summarized research and method of Internet privacy protection [J]. Computer application research, 2013,01:13-20.
[4] xie lei, Chen, lu SangLu, Chen tao. Storage RFID data management: algorithms, protocols, and performance evaluation [J]. Journal of computers, 2013 01:457-470.
[5] Wang Suping. Iot perception layer security research review [J]. Journal of sensors and micro system, 2015，06: 6-9.
[6] Jiang Fa group, xiao-qin wang, Chen green ping. RFID system safety and evaluation method research [J]. Computer security, 2011,01:39-43.
[7] He Ming joshaoska, xiao-hu Chen, mark chan. Internet of things technology and its safety study [J]. Computer security, 2011, 04:49-52.
[8] Jiang Gongqi Ren Jingru. Food traceability system based on qr code and RFID application in aviation food safety supervision and explore [J]. Port health control, 2014 01:1-3.
[9] the army. The RFID security authentication based on Internet of things technology research [J]. Journal of network security technology and applications, 2014, 07: 187-188.