ECE-3

Improved RFID Encryption Technology used in Internet of Things

Zhenhuag Wang, Dajun Zai
National University of Defense Technology, China, 1216786732@qq.com, 15995147242@163.com

Supervisor: Zhu Peidong, Professor
School of Computer Science, China, zpd136@sina.com

With the fast development of Internet of Things industry, the security of RFID cause concern more than before as a basic part. RFID system plays a vary important part in IoT , which helps people locate ,trace and analyze things .However, when RFID help us gain more useful information, it also increase the risk of privacy leak, may leading to heavy cost. So RFID system will not be widely used without a practical RFID information security technology.

In order to ensure the security of the transport and distribution of electronic tag's key and the communication between reader and RFID tag, we must use encryption technology. Current RFID systems commonly use DES(symmetric encryption),RSA(asymmetric encryption),etc. But size the chip size is limited by the tag, the electronic tag computing power is not strong, which makes the realization of the RSA encryption algorithm and the key generation slower. So DES encryption algorithm often used in the RFID systems which security requirements are not too high.

In this paper there is a RFID tag information transmission encryption method, based on variant DES encryption algorithm, which will lift the security capacity of RFID and lower the cost. In the communication between RFID tags and readers, after a triple mutual authentication system (ISO / IEC DIS9798-2), we will know whether the tags and readers are matching. And then we encrypt the message using a variant DES encryption in order to ensure the secure transmission of data. Even if the data is stolen, as the attacker does not know the rules of encryption and the key, the data is useless to the attacker. Before further study, here is the preliminary result. And further research is ongoing.

Triple mutual authentication method can guarantee RFID tags and readers which communicate with each other is credible. The process is as follows: ①When the tag enter range of the tag reader, the reader issues a query ID and password; ②The tag generate random numbers A1, and sent to the reader; ③After receiving A1,reader generates a random number B1, and uses the same key K and the same key generation algorithm Ek to generate an encrypted data token 1, which includes t random number A1, B1 and additional control data (CD), and sends it to the RFID tag: Token1 = Ek (A1, B1, CD, plaintext 1); ④After receiving token 1, RFID tag decode it and get the random number A1 *sent before, comparing it with A1 which is generated by itself. If they are consistent, the reader and the RFID tag itself are the same, belonging to the same system. Then RFID tag generates another random number A2, using the same key K and the same algorithm to generate encrypted key data token 2, and sends it to the reader: Token2 = Ek (A2, B1, plain text 2); ⑤After receives the token 2, reader uses the same methods to identify the RFID tag. If received B1 * and B1 are consistent the key K between the reader and the tag is the same. So, the RFID tag and reader are in common system, we can start further communication

After the identification between reader and the RFID tag, we can transmit data. In order to ensure the security of data even when they are stolen. It must match the strength of encryption before data transmission. In this paper, for the shortcomings of this DES symmetric encryption method, here is a variant of DES encryption method, proposing an effective rules to enhance the security of encryption, the process is as follows:

Existing: EPC data, agreed symmetric key Mkey, the receiver also saved a same key, whose security is ensured by the key management mechanisms.

The sender (RFID TAG): ①Using the random function to generate a 64-bit (8-byte) random key (Rkey), encrypt Rkey in DES encryption by Mkey and generate a ciphertext DATA1; ②Using random key Rkey, encrypt data in a self-defined encryption algorithm to generate DATA2; ③Assemble DATA1 and DATA2 to produce cipher text DATA.

The receiving end (RFID Reader): ①Split the received cipher text DATA into two parts according to the rules, DATA1 and DATA2; ②Lookup key MKey stored in the database and use MKey to decrypt DATA1 , getting the random key generated by sender which is also the key to decrypt the cipher text ,Rkey; ③Use Rkey to decrypt DATA2 in a self-defined encryption algorithm to get plaintext data.