無線網路上資料安全的實現

The Implementation of Data Security Base on Wireless Networks

葉生正

Sheng-Cheng Yeh

萬能技術學院電子工程系

Department of Electronic Engineering, Van Nung Institute of Technology

E-mail: peteryeh@cc.vit.edu.tw

ABSTRACT

Wireless networks provide a convenient and efficient service for the information transformation. In the meanwhile, they can access the voice and data traffic by using cordless telephones or mobile computers at any time. But with the added convenience and efficiency of wireless access come new problems, mobile terminals specially expect secure messages exchange when transmissions are broadcast over radio waves. Thereby, we propose a cryptographic protocol to achieve the goal of privacy and authentication for wireless networks in this paper. Moreover, it can be implemented with simple circuits to protect the wireless communications.

Keyword: Cryptographic, Privacy, Authentication.

I. INTRODUCTION

In the recent years, wireless PCS (Personal Communications System) has been developed very soon [1][2][3]. Additionally, wireless networks have allowed communications of voice and low speed data traffic [4]. Meanwhile, the mostly merit of wireless communications is to access the information from the network without regard to the mobility and location. However, wireless communications via radio, making them more susceptible to eavesdropping than communications carried via wires, so that the issue of data security becomes very important [5][6]. Therefore, the purpose of this paper is to propose a cryptographic protocol to resolve the privacy and authentication problems for the wireless network simultaneously.

In the follows, we will describe the cryptographic system at first, and then introduce the key exchange protocol between a base station and mobile node in Section II. In Section III, an example is given to explain how easy to implement the protocol, and discuses the feasibility and characteristics of our algorithm.

II. DESCRIPTION OF THE NEW SCHEME

The cryptographic system on a wireless network should be partitioned into two sub-systems, one is for enciphering plaintexts to ciphertexts and the other is for deciphering ciphertexts to plaintexts. In order to achieve the privacy and authentication, a mobile node generates a random number to be a private key, then using an exchange protocol to transmit the public key to a base station by the air. Additionally, the mobile node and base station will make use of some simple electronic devices (like a 4-stage shift register and Exclusive-OR gate) to authenticate each other further. As shown in Figure 1, letting RN (Random Number) denote a private key bit stream, M denote a plaintext bit stream and K denote a key bit stream, then referring to the Vernam cipher [7] we get a ciphertext bit stream C = EK(M) = M$\oplus$K. On the other hand, we can also get a plaintext with the same operation as M = DK(C) = C$\oplus$K.

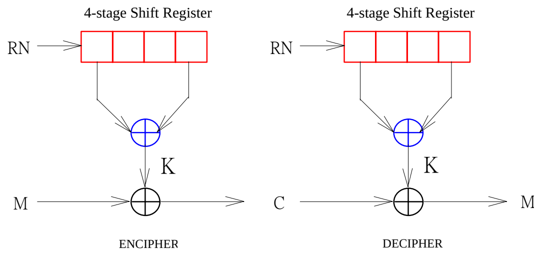

Figure 1. Encipher and Decipher system

There will be a message exchange for the key exchange. In the following, we shall propose a key assignment protocol that can be initiated by either side. If the mobile node initiates the key assignment protocol as shown in Up-link of Figure 2, it is presented as follows.

1. Mobile Node → Base Station (*ID_G*)

The *ID* number of the mobile node, the mobile identifier number assigned by operating company to a subscriber, will be encoded into Gray code at first, then Mobile node transmits the *ID* number as ID_G to Base station for the authentication.

2. Base station → Mobile node (*K_{PUB}*)

When the base station receives the ID_G, it creates the public key with an Exclusive-NOR gate as shown in formula (1) and transmits the public key to Mobile node. The K_{PRI} is the private key of Base station.

$$K_{PUB} = \overline{ID_G \oplus K_{PRI}} \quad \text{------------(1)}$$

3. Mobile node → Base station (*K_{RN}*)

The mobile node deciphers the private key with the same operation expressed in formula (2) and generates a random number (RN) to be a new private key of Mobile node. However, it also creates the new public key K_{RN} as shown in formula (3), and transmits the key to Base station eventually.

$$K_{PRI} = \overline{K_{PUB} \oplus ID_G} \quad \text{------------(2)}$$

$$K_{RN} = \overline{RN \oplus K_{PRI}} \quad \text{----------- (3)}$$

Concurrently, if the base station initiates the key assignment protocol as shown in figure 2 for Down-link, it will be described as follows.

1. Base station → Mobile node (K_{PUB})

The base station translates the *ID* of Mobile node into Gray code, then creates a public key as same as formula (1), and transmits the public key to Mobile node.

2. Mobile node → Base station (K_{RN})

The mobile node gets the private key according to the formula (2) at first, then applying the formula (3) to create a new public key and transmit it to Base station.

Finally, we present Encipher and Decipher process of the key by modular arithmetic in GF(2) as list:

1. Encipher process

Letting P=p1p2p3... denote a private-key bit stream and K=k1k2k3... denote a key bit stream, then we generate a secret public-key bit stream S=s1s2s3... by the encipher process as shown in formula (4) and (5).

S = EK(P) = s1 s2 s3 ...., bit stream ------(4)

si = (pi+ki+1) mod 2, where i=1,2,3,...... ---(5)

2. Decipher process

Because (ki+1)⊕(ki+1)=0, the decipher process is performed with the same operation as shown in formula (6) and (7).

P = DK(S)=p1 p2 p3 ...., bit stream ------(6)

pi = (si+ki+1) mod 2, where i=1,2,3,...... ---(7)

From the formulae (4) to (7), they can be easily implemented in microelectronics with Exclusive-NOR gates.

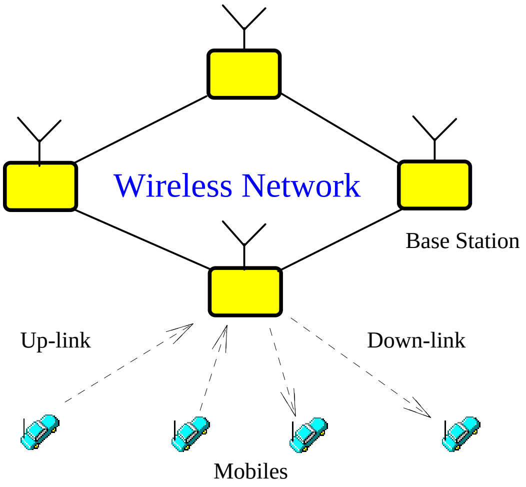

Figure 2. Wireless Network

III. EXAMPLE AND IMPLEMENTATION

We will illustrate the implementation of our protocol on Base station and Mobile node in this section.

Assume that the *ID* number of Mobile node is expressed by id1 to id4 and the private-key K_{PRI} of Base station denoted by the bit stream, then initially the *ID* number will be translated into Gray code by 3 Exclusive-OR gates as shown in figure 3. Additionally, we can create a public key from an Exclusive-NOR gate in the base station. However, the mobile node generates the new public key K_{RN} by using an Exclusive-NOR gate eventually. Figure 3 shows that the implementation of the base station and mobile node, respectively.

In this paper, we have concentrated not only on the privacy and authentication for wireless communications but also considered the feasibility of implementation. Therefore, we discuss the merits of our protocol and compare with the others as list.

(1) About the relative security and complexity, our protocol has owned all the merits of Vernam and Random Ciper [7].

(2) In order to authenticate legal registration further, we just make use of shift registers and logical gates to achieve the goal.

(3) From the above illustration, it is obvious that our algorithm is simple with low cost and low latency.

(4) The bit stream length of ciphertext is the same as the plaintext so that there is no overhead in transmission.

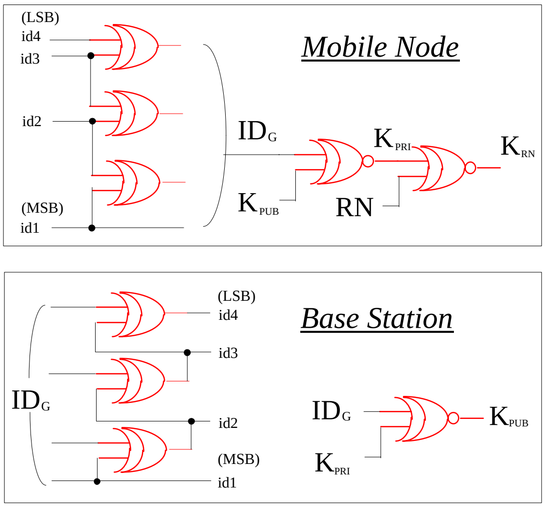

Figure 3. The Implementaion of Our Protocol

IV. CONCLUSION

Because wireless networks can provide economic and convenient services of the message (such as data and voice) transfer, they will be applied in several domains like wireless LANs and WANs, wireless PBX, Digital Cellular Ratio and Cordless Extension Phones. However, it is important that users need a safe and confident protocol to communicate with each other in the open air. In this paper, we presented a cryptography protocol that not only provides privacy and authentication for wireless network but also uses a simple circuit to implement the transmission of data security.

REFERENCE

[1] J.E. Padgett, C.G.. Gunther and T. Hattori, “Overview of wireless Personal Communications”, IEEE Personal Communications Magazine, pp. 28-41, Jan. 1995.

[2] R. Steels, j. whitehead and W.C. Wang, “System Aspects of Cellular Ratio”, IEEE Personal Communications Magazine, pp. 80-86, Jan. 1995.

[3] Richard Van Nee and Geert Awater, “ New High-Rate Wireless LAN Standards”, IEEE Communications Magazine, pp. 82-88,December 1999.

[4] Sheng-Cheng Yeh and J.-S. Wu, “Integration of Video, Voice and Data Transmission Service based on PRMA Wireless Networks”, Computer Communications, vol. 24, pp. 942-948, May 2001.

[5] Ashar Aziz and Whitefield Diffie, “Privacy and Authentication for Wireless Local Area Networks”, IEEE Personal Communications Magazine, pp. 25-31, First Quarter, 1994.

[6] M.J. Beller, L.F. Chen and Y. Yacobi, “Privacy and Authentication on a Portable Communications System”, IEEE JSAC, Vol. 11, No. 6, Aug. 1993.

[7] D.E. Denning, “Cryptography and Data Security”, Reading MA: Addison-Wesley, 1982.