채널 부호화를 통한 물리계층 무선 네트워크 보안 기술

아싸두자만*, 공형윤*, 김건석*, 김내수**
*울산대학교 전기전자정보시스템 공학과
**한국전자통신연구원
e-mail : {asad78, hkong,edaemonism}@mail.ulsan.ac.kr, nskim@etri.re.kr

Physical Layer Wireless Network Security Through Channel Coding

Asaduzzaman*, Hyung-Yun Kong*, Gun-Seok Kim*, Nae-Soo Kim**
*Department of Electrical Engineering, University of Ulsan
**Electronic and telecommunication Research Institute (ETRI)

Abstract

In this paper we introduce a new paradigm of physical layer security for wireless network. Existing security protocols like internet's transport layer security protocol has some security flaws that skilled hackers could exploit. Motivated from this point we introduce a new security protocol that works in physical layer which is much less vulnerable to hackers than any other higher layers. In our proposal, we incorporate the proposed security protocol within channel coding as channel coding is an essential part of wireless communication. We utilize the flexibility to choose a generator matrix (or generator polynomial) of a particular code that selects the code words as a core of our protocol. Each pair of wireless node will select a unique generator using their security key before they started to communicate with each other.

1. Introduction

Wireless communications technologies have undergone rapid development. Wireless technologies cover a wide range of differing capabilities oriented toward different uses and needs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Ad-hoc networks enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality also eliminates cables for printer and other peripheral device connections. Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access. Moreover, these technologies can offer dramatic cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders. In order to meet the demands of multimedia communications, next-generation wireless systems must employ advanced algorithms and techniques that not only increase the data rate, but also enable a secured and error free data communication.

However, risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new. Perhaps the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot. The loss of confidentiality and integrity and

the threat of denial of service (DoS) attacks are risks typically associated with wireless communications [3]. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance and launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks.

The conventional security mechanism is same with the wired equivalent privacy (WEP) protocol [1]. Encrypting data with WEP protects the wireless link between two wireless nodes. Wireless network administrators provide a WEP-algorithm-based key for each authorized user, thereby denying access to anyone without an assigned key. In wireless LAN wireless application protocol (WAP) specifies the WTLS (wireless transport layer security) protocol, which is similar to the Internet's transport layer security protocol [2]. WTLS provides authentication, data integrity, and privacy services within wireless technologies' limited processing power, memory capacity, and bandwidth. WTLS generally uses RSA-based cryptography. With this service, authorized devices and servers share a secret encryption key. Participating devices and servers authenticate one another by using their keys to decode a decrypted challenge message and determine whether they got the same, correct result.

Secured communications in wireless environment involves the important issue of information security, privacy, and authentication in an open space. Privacy involves ensuring that an eavesdropper cannot intercept the communication information of mobile users. Authentication involves ensuring that the services are not obtained fraudulently. In recent years, much in the literature had been written on privacy and authentication for wireless communications [1]-[4]. Good security protocol for wireless communications not only provides high security but must also have a low computational complexity. The well known CDMA technique can also provide a physical layer security. The application of CDMA is limited because of Bandwidth and other limitation like multiple access techniques. Moreover, CDMA is a very complex technique to apply only for security of wireless network.

In this paper we introduce a new dimension in physical layer wireless security protocol. In this proposed protocol we incorporate the security algorithm within conventional channel coding. Error control coding is an essential part of all type of wireless system due to the random behavior of wireless channel. We apply traditional channel coding for wireless security as well as for error correction. We don't need to increase the complexity to achieve a high level security in wireless network. For simplicity we analyzed our protocol through a linear block code. Other channel codes like convolutional code, turbo code, cyclic code, etc. also can be used for security in similar manner. The rest of the paper is organized as follows. Section 2 describes some overview of block code. Our proposed algorithm is explained in section 3. In section 4 we support our idea with some numerical simulation and finally we conclude this paper in section 5.

2. Over view of Linear Block Code

A. Basic Idea:

Linear block codes are parity check code that can be characterized by the (*n, k*) notation where a block of *k* massage bits is encoded into a longer block of *n* codeword bits [5]. The encoding procedure assigns to each of the 2^k massage to one of the 2^n code word. Since a set of code word that forms a linear block code is *k* dimensional subspace of *n* dimensional binary vector space ($k<n$). This freedom in selecting the 2^k codeword from total 2^n possibility enables us to incorporate a security during coding. Moreover, for a particular k-bit information sequence we can choose any one of the 2^k n-bit codeword. So the possibility to select a codeword from for (n, k) code is ${}^nC_p$. So it is possible to offer different code word set for different users in a multi-user scenario that will offer a high level security.

Physical layer security in wireless communication is possible to protect eavesdropping and unauthorized access through channel coding. This is possible because of the availability of choosing a codeword from a number of available options. The code words of a particular coding technique are selected by the generator matrix (or generator polynomial in case of convolution code). For decoding a received code word generator matrix is required at the destination; otherwise, it is impossible to decode a code word. Our idea is to assign different generators for the different pair of communicating nodes so that, other unauthorized nodes or any other eavesdroppers are unable to decode the coded information. But the main challenge is the performance of any error correcting code depends on generator i.e., we r not free to change them arbitrarily.

B. Generator Matrix:

When a number of users are communicating with each other we can allocate separate codeword for each pair of user. To do this we need to apply some codeword allocation technique. In general generator matrix is responsible to choose a set of codeword in linear block code. For a (*n, k*) linear block code a generator matrix ix a *n X k* size binary matrix that relates the k-bit input data block with n-bit output data block. Therefore, we can select different codeword for different input data block by using different generator matrix for each pair of users. A generator matrix for systematic linear block codes of (*n X k*) dimension is given as-

$$G = \left[P \middle| I_k\right] = \begin{bmatrix} p_{11} & p_{12} & \cdots\cdots\cdots & p_{1,(n-k)} & 1 & 0 & \cdots\cdots & 0 \\ p_{21} & p_{22} & \cdots\cdots\cdots & p_{2,(n-k)} & 0 & 1 & \cdots\cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ p_{k1} & p_{k2} & \cdots\cdots\cdots & p_{k,(n-k)} & 0 & 0 & 0 & 1 \end{bmatrix} \quad (1)$$

Where *P* is the parity check matrix [5] and I_k is the (*kXk*) size identity matrix. Let $[m_1, m_2, m_3, \ldots\ldots\ldots, m_k]$ be the massage words and $[u_1, u_2, u_3, \ldots\ldots\ldots\ldots u_n]$ be the code word then the relationship between them is given by-

$$[u_1 \quad u_2 \quad ..... \quad u_n] = [m_1 \quad m_2 \quad ..... \quad m_k] \times \begin{bmatrix} p_{11} & p_{12} & ..... & p_{1,(n-k)} & 1 & 0 & .... & 0 \\ p_{21} & p_{22} & ..... & p_{2,(n-k)} & 0 & 1 & .... & 0 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ p_{k1} & p_{k2} & ..... & p_{k,(n-k)} & 0 & 0 & .... & 1 \end{bmatrix} \quad (2)$$

From equation (2), we can see a particular codeword (u) is selected in accordance with a column of the generator matrix. So by changing the elements of generator matrix we can select different codeword for different communication channel. The generator matrix contains two part, parity check matrix and identity matrix. Changing the generator matrix means the changing the parity matrix.

3. Physical Layer Security Protocol

A. System model:

For the purposes of exposition, we consider a cellular based multiuser transmission where a group of users are transmitting towards a single destination shown in figure 1. We also consider there are some unauthorized wireless nodes (hackers or eavesdroppers) with in the cell under the base station. Our main purpose is to inhabit these unauthorized nodes to access to the BS or receive any information from BS.

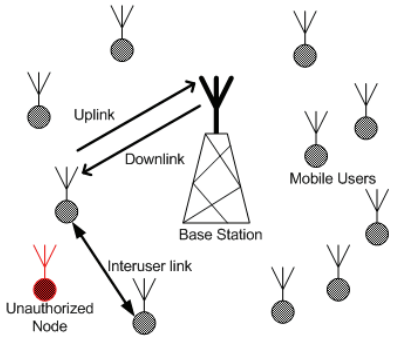

Figure1. Communication scenario.

The users transmit on orthogonal channels (e.g., TDMA, CDMA, or FDMA), which allows the destination to separately detect each user's data without any interference. All the mobile users are equipped with a linear block code encoder and decoder in addition with a random interleaver. Block diagram of a wireless node is shown in figure 2.

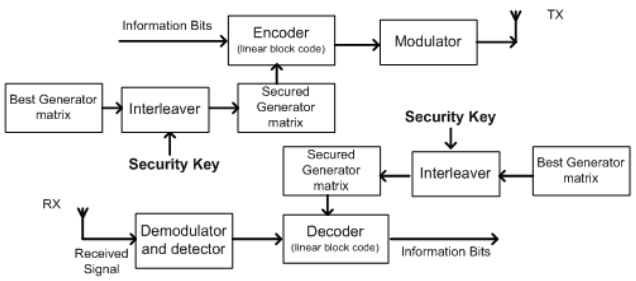

Figure 2. System Block Diagram.

However, the basic idea and operation of our proposed technique does not depend on the specifics of the channel access protocol. More over our considered scenario is very common for wireless LAN, Cellular phone, cluster based wireless sensor network etc.

B. Proposed Algorithm:

Our main objective is to find a suitable algorithm to allocate different parity check matrix i.e. generator matrix for different pair of terminals. We are not free to Change the generator matrix arbitrarily because all the generator matrixes for a specific code (n, k) does not offers maximum performance. The performance of a linear block code is a function of so called minimum free distance (d_{free}) [5]. The main problem to employ our idea is to find a group of generator matrix with good minimum free distance i.e., best error correcting capability.

Consider all the mobile users and destination has their own security code. These codes may be a function of time, location, address or simply a random number. We will use these security codes as a key to change the generator matrix of each user as shown in figure 2. To maintain a good free distance we choose the best generator matrix of a series of linear block code. We found some interesting result in our experiment that, a generator matrix found by perturbation of a good generator is also a good generator matrix. We can easily found a group of good generator matrix from the best generator of a particular linear block code group by interleaving the rows and columns of the default matrix. We assign the best generator as a default generator matrix to all the users and then each user will produce a secret generator matrix to communicate with other node (base station or any other node) on the basis of the security key. For a particular pair of communication terminal the basic generator matrix is randomly interleaved cording to their source and destination security key. First we consider all the rows of the matrix are randomly interleaved in according to source security key then the columns of the new interleaved matrix is again randomly interleaved according to destination security key therefore, only this particular pair of node can decode the data if they know the security key of each other. We assume that this security key is allocated by the base station and it is updated at a regular time interval to improve the security level of the system. The generator selection algorithm using the security key is very simple and given below:

Step 1: Select a particular block code that can satisfy the system requirement on error correcting capability.

Step 2: Choose the best generator of that particular group of block code.

Step 3: Randomly interleaved the rows of selected generator matrix according to the source security code.

Step 4: Randomly interleaved the columns of selected generator matrix according to the destination security code.

The above algorithm ensures that only the authorized user can generate the exact generator matrix to decode the

information. More over it also ensure that the generator matrix of proposed algorithm always maintain a good free distance property hence, we can provide a high level security in physical layer without any performance degradation.

4. Simulation Result:

For simulation we choose a simple (*7, 4*) linear block code with parity check matrix [1 0 1; 1 1 0; 1 1 1; 0 1 1] as a default generator. In presence of AWGN we simulate the BER performance of our proposed algorithm. AWGN noise is modeled as zero mean complex random variable with variance *1/2* per dimension. We also assume maximum likelihood (ML) detection before decoding. In our simulation we assume random numbers as a security key and the security keys of two communicating node is known to each other. For an unauthorized node we also consider a random number as security code and they try to decode the information using a new random number every block of channel information. Figure shows the BER performance of our proposed algorithm.

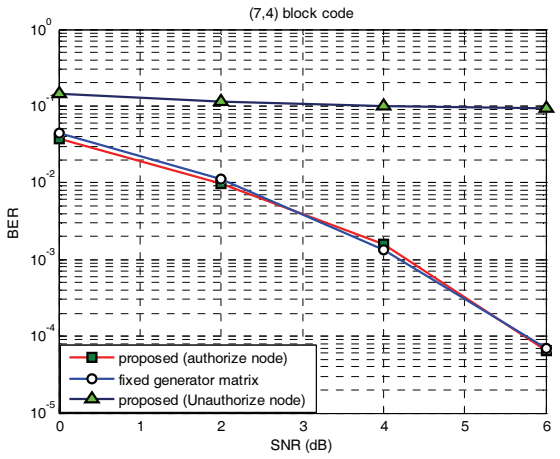

Figure 3. BER performance

First we compare our proposal with the fixed generator matrix (i.e. all the node have same generator). In this case we chose the best generator matrix of (7, 4) linear block code. In our proposed algorithm we chose best generator matrix as a reference and produces a new generator by random interleaving the best generator using the security key. Figure-2 shows that our proposed algorithm offers same performance with the best generator polynomial. Therefore we do not need to sacrifice any performance for security. We consider an unauthorized user who does not know the source security code and tries to decode the received signal using a random security code. We found that BER performance is almost constant with received SNR. So, our proposal is offering a high level security with out sacrificing any performance. Moreover, our proposed algorithm increases a negligible amount of system complexity as we use interleaving operations to generate the generator matrix for each user.

To find the security level of our proposal we make some simulation for two different code (7, 4) and (23, 11). We try to detect the information in an unauthorized node using arbitrary random number as a security code. Our simulation results show that probability of detecting a transmitted block at an unauthorized node is dependent on the size of the parity matrix. As the size of parity matrix increases security level of our proposed algorithm also increases. For example (23, 11) block code perform better then (7, 4) code because the first code has a larger parity check matrix. The main reason behind this is the size of parity check matrix i.e. size of generator matrix. For small size of parity check matrix the total possible cases of interleaved parity check matrix is also small. As the size of the parity check matrix this probability is also decrease which offers a high security level.

5. Conclusion:

Physical layer security is in wireless network is supposed to be the strongest security then other upper protocol layer because physical layer is much less vulnerable against hackers. Although the proposed system does not sacrifices any performance but it increases the system complexity. Instead of using a fixed generator polynomial it requires to perform two random interleaving operations to generate the generator polynomial. This added complexity is very less in comparison with other higher layer security system like network encryption. In this work we analyze the physical layer security using linear block code but other channel coding like convolutional code, turbo code, cyclic code etc. also can be used for physical layer security by changing their generator using a proper algorithm. The most important feature of our proposed security protocol is we apply this in any kind of wireless network regardless of the network protocol and topology as coding is an essential part of wireless communication.

Acknowledgement

"본 논문은 정보통신부(MIC)와 국방부에서 출연한 민군겸용기술개발사업 일환으로 한국전자통신연구원(ETRI) 지원에 의해 수행된 연구결과입니다"

Reference

[1] N. Borisov, I. Goldberg and D. Wagner, ”Intercepting Mobile Communications: The Insecurity of 802.11”, In Proc. of the Seventh Annual International Conference on Mobile Computing and Networking, July 2001.

[2] Facing the challenge of wireless security Miller, S.K.; Computer Volume 34, Issue 7, July 2001 Page(s):16 - 18 Digital Object Identifier 10.1109/2.933495

[3] S.Wong, ”The Evolution ofWireless Security in 802.11 Networks: WEP, WPA and 802.11 Standards”, SANS Institute, March 2003.

[4] N. Borisov, I. Goldberg and D. Wagner, ”Intercepting Mobile Communications: The Insecurity of 802.11”, In Proc. of the Seventh Annual Internatioinal Conference on Mobile Computing and Networking, July 2001.

[5] J.G. Proakis, *Digital Communications*, 4th Edition. New Yor k: McGraw-Hill, 2001.