논문 2008-3-7

채널 부호화를 통한 물리계층 무선네트워크 보안기술

Channel Coding Based Physical Layer Security for Wireless Networks

아싸두자만*, 공형윤**

Asaduzzaman*, Hyung Yun Kong**

Abstract

This paper introduces a new paradigm of physical layer security through channel coding for wireless networks. The well known spread spectrum based physical layer security in wireless network is applicable when code division multiple access (CDMA) is used as wireless air link interface. In our proposal, we incorporate the proposed security protocol within channel coding as channel coding is an essential part of all kind of wireless communications. Channel coding has a built-in security in the sense of encoding and decoding algorithm. Decoding of a particular codeword is possible only when the encoding procedure is exactly known. This point is the key of our proposed security protocol. The common parameter that required for both encoder and decoder is generally a generator matrix. We proposed a random selection of generators according to a security key to ensure the secrecy of the networks against unauthorized access. Therefore, the conventional channel coding technique is used as a security controller of the network along with its error correcting purpose.

Key Words : Wireless security, Physical layer, Channel coding, Generator matrix, Random interleaving

I. Introduction

Wireless communication technologies have undergone rapid development. Wireless technologies cover a wide range of differing capabilities oriented toward different uses and needs. 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 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

*학생회원, 울산대학교 전기전자정보시스템공학부
**정회원, 울산대학교 전기전자정보시스템공학부
접수일자 : 2008.4.24, 수정완료일자 : 2008.6.17

denial of service (DoS) attacks are risks typically associated with wireless communications [1]. 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.

A good security protocol for wireless communications not only provides high security but must also have a low computational complexity. The well known spread spectrum technique can also provide a physical layer security. The application of spread spectrum 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. CDMA based security protocols proposed in [4] is not suitable for networks using other multiple access techniques like TDMA and FDMA. Our proposed physical layer security protocol is integrated with channel coding. Channel coding is an essential part of modern day's wireless communication due to the random behavior of wireless channel; hence, the proposed security protocol is applicable in all kind of wireless networks regardless of their modulation schemes, multiple access techniques, applications, etc.

In this paper we introduce a new dimension in physical layer wireless security protocol. We apply traditional channel coding for wireless security as well as for error correction. Therefore, we don't need to increase the complexity to achieve a high level security in wireless network. For simplicity we analyzed our protocol through linear block code and convolutional code as they are most widely used. Other channel codes like turbo code, cyclic code, LDPC, BCH code, etc. also can be used for security in similar manner.

The rest of the paper is organized as follows. Section II describes the proposed security protocol. Section III and section IV describe the security protocol for convolutional and liner block code respectively. In section V we support our idea with some simulation results and finally we conclude this paper in section VI.

II. Proposed Security Protocol

In general channel codes can be characterized by the (n, k) notation where a block of k message bits is encoded into a longer block of n codeword bits [5]. The encoding procedure assigns to each of the 2k message to one of the 2n code-words. A set of codeword that forms a particular channel code is k dimensional subspace of n dimensional binary vector space ($k<n$). This gives us the freedom of selecting 2k codeword from total 2n possibility, which enables us to incorporate a security during coding. Moreover, for a particular k-bit information sequence we can choose any one of the 2kn-bit codeword. So the possibility to select a codeword from for (n, k) code is all the possible combinations among the message blocks and codewords. So it is possible to assign different codeword set for different data block of same user and also for different users

in a multi-user scenario that will offer a high level security in physical layer.

Therefore, a 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 codewords of a particular coding technique are selected by the generator matrix. For decoding a received codeword, the exact generator matrix is required at the destination; otherwise, it is impossible to decode the codeword. Our idea is to assign different generator matrices for the different block of data transmission so that, other unauthorized nodes or any other eavesdroppers are unable to trace the exact generator to decode the coded information.

For the purposes of exposition, we consider a generalized multi-user wireless network where a group of users are transmitting and receiving signals. It may be a cellular based network, sensor network or a multi-hop ad-hoc network. We also consider there are some unauthorized wireless-nodes (intruders or eavesdroppers) are trying to access to or listen from authorized nodes. Our main purpose is to inhabit these unauthorized nodes to access to the network or receive any information from other nodes. All the mobile users are using channel coding which will offer a reliable communication by correcting error as well as a physical layer security to the system. Block diagram of a wireless node is shown in figure 1. We assume that data are transmitting as packets, where the packets are output of a channel encoder.

Consider all the mobile users have their own security key. For structured network that have centralized control like a base station in cellular network, access point in Wireless LAN or a cluster head in cluster based wireless sensor network, these security keys may be assign by the centralized control unit. For structure less network like, ad-hoc network these key may be function of their address or a preset code for any particular pair of node. We will use these security key to change the generator matrix of each user as shown in figure 1. The selected generator matrix is not only dependent on the security key but also dependent on the generator matrix of the previous transmission. Therefore, even though the security key is hacked by any unauthorized node, after transmission of few blocks of data it is impossible for an unauthorized node to generate the exact polynomial; because, it has no idea about the previous state of generator matrix.

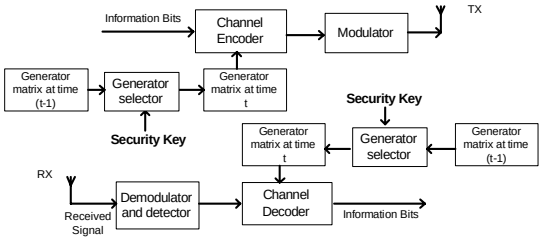


그림 1. 제한된 보안 프로토콜의 블록 다이어그램.
Fig.1 Block Diagram of proposed security protocol

Our proposed security protocol is very simple and can be describe by the following steps

Step 1:Select a suitable channel code that can fulfill the error correcting requirement of the system. (Our proposal is not only for security purpose, it will also serve the error correction along with security; so, a proper code selection

is important)

Step 2:Before starting the transmission between two nodes the generator selection algorithm will select a secret generator matrix. This selection is done based on a publicly known initial state of generator matrix and the private security key for this particular pair of nodes.

Step 3:In the first frame, the nodes use this new secret generator matrix for channel encoding. At the end of first frame transmission both source and destination select a generator for next frame by using the current generator and the security key.

Step 4:The process of step-3 repeats for entire communication.

The generator selection algorithm of step 2 and step 3 is completely dependent on the specifics of the chosen channel code. In this paper we describe this algorithm for convolutional code and linear block code in section 3 and 4 respectively.

The interesting point of our proposed protocol is we use a completely random selection of the generators for next frame. Random interleaving operation performers on the present generator using the security key as a reference of the random selection. So, different security key and current generator may select the same new generator for a particular instant but definitely it will be different in the next state because of the random nature. Therefore, our proposed protocol is able to make confusion for the hackers who are trying to hack the security key. A key update technique also may be used to reduce risk of key hacking.

The CDMA based physical layer security protocol dependents on the pseudo random scrambling because spreading code is limited to their cross correlation property. When well known Walsh code is used for spreading, a particular pair of communicating node uses a fixed spreading code which is pre-assigned. Hence, it is impossible to use same spreading code at the same time for two channels. But in our proposed physical layer security protocol we are not limited to use same generator for more than one channel at the same time. For a particular instant of time, all channels may use the same generator but at the next time it will different for each because of their different key.

We propose a security protocol where the generator matrix of a particular channel code changes with time. As we mentioned before, our security protocol will serve two purposes: security and error correcting. Therefore, we need to consider the error correcting capability of the channel code that changes its generator with time for security. The performance of any error correcting code depends on generator [7]. Performance parameter of channel codes are so called free Hamming distance property of the codewords. Minimum Hamming distance is the smallest Hamming distance between any two distinct codewords produced by the generator. Since, Generator matrices or polynomials are responsible to generate the codewords; the performance of the channel code is completely dependent on the generator. To ensure a good error correcting capability of the system we are not allowed to change the generator randomly. We need to find a suitable algorithm to change the generator with time which will ensure a good selection of generators in terms of

performance parameter.

The selection of generator matrix is dependent on specific channel code. But one important property of all kind of channel code is all possible generators of a particular set of channel code do not ensure the best performance. There are very few generator matrices or polynomials that have the best minimum distance property and there are some generators have very bad free distance property. The channel codes using generators that have very bad minimum distance property termed as catastrophic codes [6]. Therefore, we have to find a suitable algorithm to select generators for our proposed security algorithm that can avoid the catastrophic codes and choose the codes have best performance or very close to best performance. In this paper we will analyze the generator selection policy for convolutional code and linear block code in next two sections.

III. Security with Convolutional Code

3.1 Overview of convolutional code

Convolutional codes are trellis codes that satisfy certain additional linearity and time invariance properties. Several methods are used for presenting a convolutional code, the most popular being the connection representation, the polynomial representation, the tree diagram representation, the trellis diagram representation, etc. For the purpose of our security implementation, we will only focus on the polynomial representation of convolutional codes. A mathematical description of convolutional codes can be formulated using the notation of polynomials. These polynomials, with the coefficients in the field of the code are called generator polynomials of the convolutional code. The Generator polynomials of a convolutional code with rate R=k/n are commonly arranged into a k by n matrix of polynomials called generator matrix and denoted as,

$$G = \begin{bmatrix} g_{11} & g_{12} & g_{13} \cdots & \cdots & g_{1n} \\ g_{21} & g_{22} & g_{23} \cdots & \cdots & g_{2n} \\ \cdot & \cdot & \cdot & \cdots \cdots & \cdot \\ g_{k1} & g_{k2} & g_{k3} & \cdots \cdots & g_{kn} \end{bmatrix} \quad (1)$$

A set convolutional code with same code rate and constraint length can have many generator matrices. Generator matrices that are related by column permutation and elementary row operation are called equivalent generator matrices and they will generate the equivalent codes with same free distance property [6]. This point of convolutional code is the key factor of our security algorithm. In the next sub section we will describe our generator selection algorithm utilizing this important property of equivalent codes.

3.2 Generator Selection Algorithm

We can represent a rate k/n convolutional encoder with constraint length K as a set of k×n generator polynomials. Each polynomial is of degree K-1 or less and represents the connection of the modulo-2 adders of encoder [5]. Generator polynomials of convolutional code are usually represented in octal numbers. For example generator matrix with octal polynomial form of a convolutional code of rate $\frac{1}{4}$ with constraint length K=5 can be represented by G

= [25 27 33 37]. Our main objective is to find a suitable algorithm to allocate different generators for different pair of terminals as well as for different frame transmission of same pair of nodes. To do this we need to consider the performance of all possible generators under consideration. More specifically, we need to avoid all catastrophic codes and from the all non-catastrophic code we will select the codes have best performance.

The performance of convolutional code is also measured by free Hamming distance or simply free distance. A convolutional code is said to be a good code when it have a free distance equal or very close to upper bound on free distance of that particular group [7]. For any convolutional code there are few set of generator that offers a free distance equal of very close to upper bound. Utilizing these generators with different combination we can ensure the best performance of our security protocol. If we want to ensure a high security level through convolutional code, we need to find a larger set of generators. But it will force us to select some generators having free distance less than the upper bound; hence, sacrifice some performance. This indicates a tradeoff between security level and the performance of the convolution code. On the basis on this tradeoff we proposed 2 algorithms to incorporate security within convolutional coding. Both algorithms ensure that only the authorized user can generate the exact generator matrix to decode the information. Moreover, it also ensure that the generator matrix of proposed algorithm always maintain a good free distance property. The security level of both algorithms is a function of the number elements in generator matrix. As the number of elements in generator matrix increase, the possible combination of the generators to find an equivalent generator matrix is also increases. So, security level increases as the code rate decreases.

가. Algorithm-1

In this algorithm we proposed a security protocol which ensures the best performance. Code selection policy for this algorithm is straight forward. First select a particular convolutional code that can satisfy the system requirement. Then choose the best generator of that particular group of code which has the best free distance property i. e. , best performance. Now we well exploit the property of equivalent generator matrices by randomly interleave the elementary rows of the selected generator matrix. We will perform this random interleaving on present generator matrix to produce the generator matrix for next block of data transmission according to the security key. Following example will help us to explain our algorithm.

We select a convolutional code of rate R=¼with constraint length K=5. The best generator of this group of convolution code is G = [25 27 33 37] as given in [5]. We can find an equivalent generator matrix by randomly interleave the 4 elements of the row matrix G according to the security key. The new generator matrix is used for the transmission of the next block. Now replacing this code selection algorithm in the figure 1 we can find a complete security algorithm for convolutional

code. This algorithm is simple and always ensures the best performance. Any combination of these 4 generators has the free distance d_{free}=16 which is equal to the upper bound of this group of code. The possible combinations of these 4 generators are 4! = 24. So if an unauthorized node tries to decode the received codeword then it has the probability to find the exact generator set is 1/24, which is small enough. In general for a 1/p rate code, the probability to find the exact generator set is 1/p!, where p is the number of elements of the generator matrix.

The important thing to mention here is that, this probability of finding the generator matrix by an unauthorized node is only for one block of data transmission. In the next block, generator matrix change according to security key. So, this probability of recovering generator matrix is independent in each block of data transmission. But the information transmitted in consecutive block is not independent. In practical case, one message event is divided in several blocks or frames of data to transmit them in different time. Even though, the unauthorized node can decode one block of data correctly with a probability of 1/p!, the exact probability of decoding a message event is dependent on the size of block and message event. If we divide a message event into m blocks then the probability that an unauthorized node can decode a message event is

$$\Pr = \frac{1}{(C)^m} \tag{2}$$

where, C represents the number of generator matrix by considering all possible combination. In this case $C = p!$.

Therefore, we can improve the security level of our proposed algorithm by two ways. First, by selecting a convolutional code with larger number of elements in generator matrix; equivalently, increasing the number p. The second way is dividing a message event in larger number of blocks; equivalently, increasing the number m.

This algorithm can provide a good security level when p is large enough with fixed m. But for a high code rate p is usually small which indicates the security level is low according to equation (2). For example, a ½ rate code with m=1, the probability Pr=1/2! = 0.5 which has very high probability to find the exact generator for intruders or unauthorized nodes. To overcome this problem we propose another algorithm. In this algorithm we sacrifice some performance to provide high level security.

나. Algorithm-2

In this algorithm we use the binary representation of generators and represent them in matrix form for our purpose of exposition. If we consider the same set of code as algorithm-1 for example, the generator can be represent as

$$G = \begin{bmatrix} 23 \\ 27 \\ 33 \\ 37 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{3}$$

In algorithm-1 we did a random interleaving operation among the generator which is equivalent to interleaving the rows of the

binary matrix of equation (3). To provide a high level security we propose a column wise interleaving along with row wise interleaving of the binary matrix of equation (3). But this operation on this binary matrix gives some catastrophic codes which have very poor free distance. To avoid these catastrophic codes we proposed a new algorithm that offers a higher level security by sacrificing some performance.

In this algorithm, we will choose a generator of a particular group of code that has performance less than but very close to the upper bound. We will form a binary matrix of the selected generator like equation (3). Now divide the security key in two parts and randomly interleave the rows and columns of binary matrix according to the two parts of the security key. Select each row of the interleaved binary matrix as the generator polynomials for next frame transmission.

With out losing generality we consider same group of code as algorithm-1 with rate R=$\frac{1}{4}$ and constraint length K=5. We choose a generator of this group of convolution code which has near optimal free distance as

$$G=\begin{bmatrix}27\\33\\35\\37\end{bmatrix}=\begin{bmatrix}1&0&1&1&1\\1&1&0&1&1\\1&1&1&0&1\\1&1&1&1&1\end{bmatrix} \quad (4)$$

The selection criterion of these polynomials is simple. To avoid catastrophic code we consider all 1 polynomial (37 in octal) and the other polynomials contains only one zero. The free distance of this generator is 14, which is close to upper bound 16. Now randomly interleave the rows and columns of the binary matrix of equation (4) according to the two parts of the security key we can generate a set of generators having performance close to the upper bound. A MATLAB simulation shows that, this set of generators can avoid the catastrophic code and have free distances between 10 and 15, with an average free distance of 13. One example of the random interleaved generator of equation (4) is G=[33 37 36 27].

In this algorithm a little performance sacrifice can improve the security level. For this particular example we have 3 zeros and we can place these 3 zeros in 20 possible places of the matrix of equation (4). The total possible numbers of generator matrices are

$$C=\binom{20}{3}=\frac{20!}{(20-3)!\times 3!}=1140$$

The probability of detecting the exact generator set by an unauthorized node is 1/1140 which is very low compare with this probability of algorithm 1 which is 1/24. Therefore, we provide a high level security in this algorithm. Similar Algorithms may develop for convolutional code that also has a near optimal performance in different way. But the important thing is in any case we have to sacrifices some performance for higher level security. In this case, the probability that an unauthorized node can decode a message event is also can be calculate by equation (2).

IV. Security with Linear Block Code

4.1 Overview of Linear Block code

Linear block codes are parity check code that

can be characterized by the (n, k) notation where a block of k message bits is encoded into a longer block of n codeword bits [5]. The encoding procedure assigns each of the 2k message to one of the 2n code word. 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 is a n by k 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. A generator matrix for systematic linear block codes of (n X k) dimension can be given as-

$$G=[I_k|P]=\begin{bmatrix}1 & 0 & \dots & 0 & p_{11} & p_{12} & \dots\dots & p_{1(n-k)}\\ 0 & 1 & \dots & 0 & p_{21} & p_{22} & \dots\dots & p_{2(n-k)}\\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot\\ 0 & 0 & \dots & 1 & p_{k1} & p_{k2} & \dots\dots & p_{k(n-k)}\end{bmatrix} \quad (5)$$

where P is the parity check matrix [5] and Ik is the (kXk) size identity matrix. Let [m1, m2, m3,……..., mk] be the message words and [u1, u2, u3,…….un] be the code word then the relationship between them is given by-

$$[u_1\ u_2\ \dots\ u_n]=[m_1\ m_2\ \dots\ m_k]\times G \quad (6)$$

From equation (5) and (6), 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 message block. The generator matrix contains two part, parity check matrix and identity matrix. Changing the generator matrix is indeed equivalent to the changing of parity matrix.

4.2 Generator Selection Algorithm

Our main objective is to find a suitable algorithm to allocate different parity check matrix or generator matrix for different pair of terminals. We are not free to change the generator matrix arbitrarily because all the generator matrices for a specific code (n, k) do not offer maximum performance. The performance of a linear block code is a function of minimum distance (d_{free}) that we defined for convolutional code. The main problem to employ our idea is to find a group of generator matrix with good minimum distance i.e., best error correcting capability.

To maintain a good distance we choose the best generator matrix of a series of linear block code. Similar to convolutional code, linear block codes also have the equivalent generator matrices property; hence, a generator matrix found by perturbation of a good generator matrix is also a good generator matrix [6]. 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 as the second algorithm proposed for convolutional code. We assign the best generator as a default generator matrix (publicly known) to all the users and then each user will produce a secret generator matrix to communicate with other node on the basis of the security key.

The generator selection algorithm using the security key is very simple. Select a particular block code that can satisfy the system requirement in terms of error correcting

capability. Choose the best generator of that particular group of block code. Divide the security key by two parts. First, randomly interleave the rows of selected generator matrix according to the first part of the security key. Then, randomly interleave the columns of selected generator matrix according to the second part of the security key. Now, by replacing this code selection algorithm in the figure 1 we can find a complete security algorithm for linear block code. The proposed 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 the best distance property; hence, we can provide a high level security in physical layer without any performance degradation using a linear block code. For better understanding we will give an specific example.

We consider a simple systematic (7, 4) linear block code. The best generator matrix of this group of block code is given in [5] as,

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \quad (7)$$

We can find the parity check matrix of this generator matrix by eliminating the identity matrix from equation (7) as

$$P = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \quad (8)$$

We can find an equivalent generator matrix by randomly interleave the rows and columns of parity check matrix (P) according to the security key as explained before. The new generator matrix is used for the transmission of the next block. For this particular example we have 3 zeros and we can place these 3 zeros in any one of the 12 places of the matrix of equation (8). The total possible numbers of generator matrices are

$$C = \binom{12}{3} = \frac{12!}{(12-3)! \times 3!} = 220$$

The probability of detecting the exact generator set by an unauthorized node is 1/220. Similar to the security protocol with convolutional code the security level of this block code based protocol also increases with the size of the generator matrix. This example illustrates that, a simple (7, 4) linear block code with rate less than $\frac{1}{2}$ has 220 different generators with best performance which is much higher than a convolutional code of rate $\frac{1}{4}$. The general equation of the probability that an unauthorized node can decode a message event developed in equation (2) for convolutional code based security protocol is also valid for linear block code based protocol. For this case the block size is related with the selected linear block code. For example a (7, 4) code divide the message event into a group of block with length 4 bits and a (19, 11) code divide the message event into a group of block with length 11 bits. So, for a particular (n, k) linear block code and a fixed message size the number of block in a message event is fixed. Therefore, we are not free to change the values of m of equation (2) but, it ensures a large

number of blocks as the size of data block in linear block code are small.

V. Simulation Result

Our intension is to show the security of data transmission; therefore, we consider our simulation environment as simple as possible. We perform a baseband equivalent simulation. A simple BPSK modulation is considered for simplicity. In presence of additive white Gaussian noise (AWGN) we simulate the BER performance of our proposed algorithms. 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. We consider a 16 byte security key for a particular pair of communicating nodes. The security keys are generated randomly for our simulation and we avoid the key update technique. For an unauthorized node we also consider a random security key of 16 byte and they try to decode the information using a new random number in every block of channel information. If the unauthorized node can decode one block successfully it will use the same security key for next block, other wise it will change the security key randomly.

First we will verify our proposed security algorithm for convolutional code. For simulation we choose the same codes as mentioned in the examples of section 3. The publicly known Generator for algorithm-1 is G=[25 27 33 37] and for algorithm-2 is G=[27 33 35 37]. For convolutional code based protocol we consider a message event of size 1 K-bits (1024 bits) and a data block of 256 bits. Therefore number of block per message event (m) is 4.

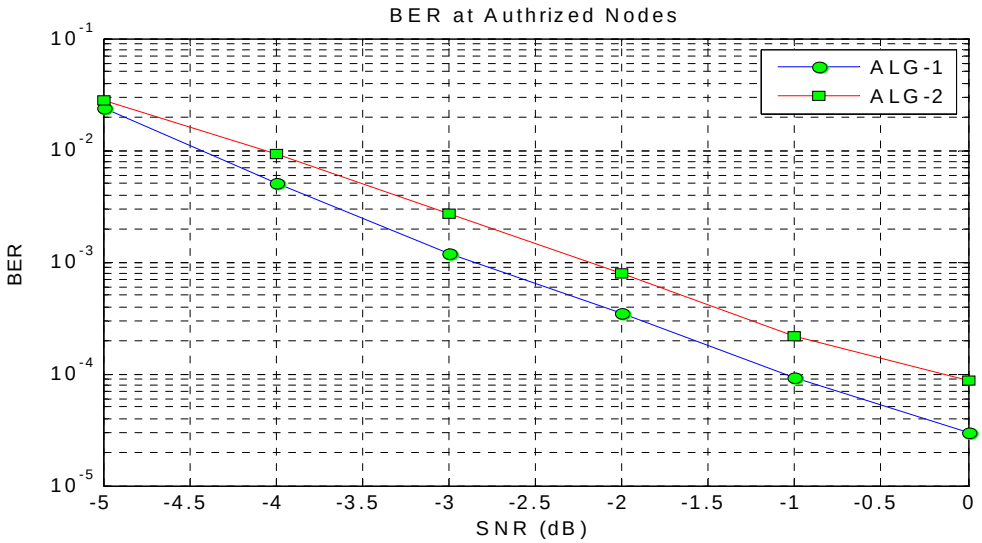


그림 2. 콘벌루션 코드 기반의 보안 프로토콜에서 권한이 있는 노드의 BER 성능
Fig. 2. BER performance at authorized node for Convolutional code based security protocol

Fig.2 shows the BER performance comparison of our 2 proposed algorithms at authorized node. Performance of algorithm 1 is the best performance (equal to the upper bound) for this chosen group of code. Figure 1 depicts that the performance penalty for high security in algorithm 2 of section 3 is about 1 dB at BER level 10-4, which is very small. Therefore we do not need to sacrifice any performance for algorithm 1 and the performance sacrifice for higher order security in algorithm 2 is also very small.

Now we will perform the similar simulation for block code. For simulation we choose a simple (7, 4) linear block code with parity check matrix [1 0 1; 11 0; 1 1 1; 0 1 1] as a default publicly known generator. Figure-4 shows the BER performance of our proposed algorithm. First we compare our proposal with the fixed generator matrix (i.e. all the node have same generator over all the communication period). In this case we chose the best generator matrix of (7, 4) linear block code. In our proposed algorithm we choose best generator matrix as a reference and produces a new generator by random interleaving the best generator using the security key. Figure-4 shows that our proposed algorithm offers same performance with the fixed best generator matrix. Therefore we do not need to sacrifice any performance for security. We consider an unauthorized user who does not know the source security key and tries to decode the received signal using a random security key as explained for convolutional 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.

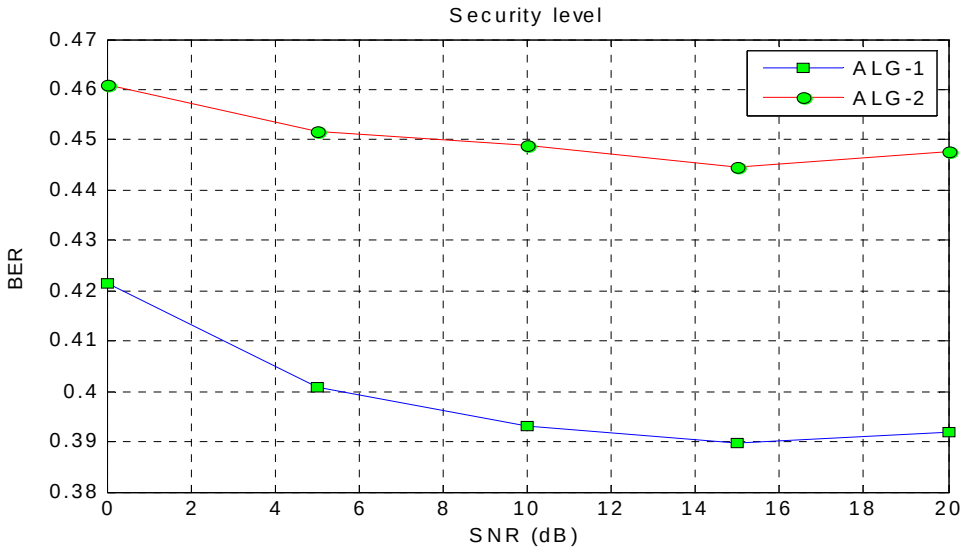


그림 3. 콘벌루션 코드 기반의 보안 프로토콜에서 권한이 없는 노드의 BER 성능
Fig. 3. BER performance at unauthorized node for convolutional code based security protocol

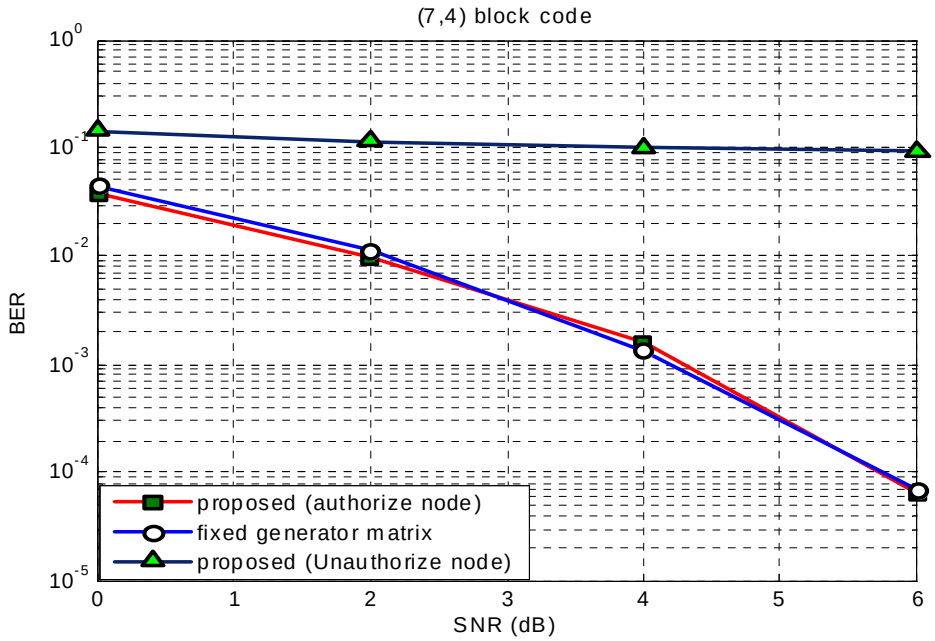


그림 4. 블록 코드 기반의 보안 프로토콜에서 권한이 있는 노드와 권한이 없는 노드의 BER성능

Fig. 4. BER performance at both Authorized and unauthorized node for block code based security protocol

The BER performance of the linear block code based protocol at unauthorized node is about 0.1; whereas, this value for convolutional code based protocol is about 0.391 and 0.448 for algorithm-1 and algorithm-2. This lower bit error rate for block code based security protocol is due to its systematic behavior. In systematic block code the codewords contain the exact copy of the message block along with the parity bits. We consider a nonsystematic convolutional code which means that there is no exact copy of message block. This nonsystematic behavior will definitely increase the BER of wrong decoding at unauthorized nodes then the systematic codes. This point suggests that, nonsystematic codes will provide a better security than systematic codes.

VI. Conclusion

Physical layer security is in wireless network is supposed to be the strongest security then other upper protocol layers because physical layer is much less vulnerable against hackers. In this paper we introduce a new paradigm of physical layer security in wireless network through channel coding. We proposed a wireless security protocol with a minimum increased complexity. This added complexity is very less in comparison with other higher layer security system like network encryption. More importantly, we don't need to add any extra hardware for security except a specially designed error correction encoder and decoder. In this work we analyze the physical layer

security using linear block code and convolutional code but other channel coding like turbo code, LDPC, 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 can apply this in any kind of wireless network regardless of the network protocol and topology because coding is an essential part of wireless communication.

Reference

[1] S.Wong, "The Evolution of Wireless Security in IEEE 802.11 Networks: WEP, WPA and 802.11 Standards", SANS Institute, March 2003.

[2] Miller, S.K.; "Facing the challenge of wireless security", Computer Volume 34,7, July 2001, Pages:16 - 18.

[3] 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.

[4] Tontong Li; Jian Ren; Qi Ling; Anil Jain; "Physical layer built-in security analysis and enhancement of CDMA systems", Military Communications Conference, 2005. MILCOM 2005, 17-20 Oct. Vol. 2, Pages:956 - 962 .

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

[6] Richard E. Blahut, "Algebric Codes for Data Transmission" Cambridge University press 2003.

[7] Andrew J. Viterbi, J. K. Omura, "Principle of Digital communication and coding", McGraw-Hill, 1979.

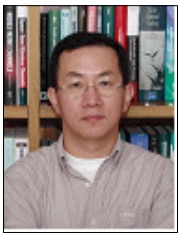
이 논문은 2007년도 정부(과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임 (No. R01-2007-000-20400-0)

저 자 소 개

아싸두자만(학생회원)

- 2001년 1월 : University of Chittagong(방글라데시) 전기전자공학과 학사
- 2006년 3월 : 울산대학교 전기전자정보시스템 공학과 박사과정

<주관심분야 : 변복조 기술, 부호화 기술, 무선센서네트워크, 협력통신, MIMO>



공형윤(정회원)

- 1989년 2월 : New York Institute of Technology(미국) 전자 공학과 학사
- 1991년 2월 : Polytechnic University(미국) 전자공학과 석사
- 1996년 2월 : Polytechnic University(미국) 전자공학과 박사
- 1996년~1996년 : LG전자 PCS 팀장
- 1996년~1998년 : LG전자 회장실 전략 사업단
- 1998년~현재 : 울산대학교 전기전자정보시스템공학부 교수

<주관심분야> 모듈레이션, 채널 부호화, 검파 및 추정 기술, 협력통신, 센서 네트워크