CDMA 기반 무선 LAN 에서의 보안을 보장하기 위한 새로운 다중 접속 방식

정회원 김 영 국*, 박 세 웅*

A New Multiple Access Scheme to Ensure Security in CDMA-Based Wireless LANs

Young-Kook Kim*, Sae-Woong Bahk* *Regular Members*

요 약

무선 매체는 이의 방송 특성에 의해 본질적으로 보안에 취약한 매체이다. 진행중인 통신 전송 부근에 있는 자는 누구든지 공중에 전송되는 신호를 수신할 수 있다. 더불어, 공격자는 진정한 사용자로 행세하여 무선국과 통신을 시도할 가능성도 있다. 무선 통신이 더욱 널리 사용되고 이를 통해 중요한 정보가 전송됨에 따라 보안에 관한 고려의 중요성이 대두되고 있다. 본 논문에서는 슬롯사용 CDMA에 기반한 새로운 다중 접속 방식이 보안의 강화를 위해 제안되었다. 현재까지의 대부분의 보안관련 연구는 공격자가 어떠한 비트가 전송되고 있는지는 알아낼 수 있도록 하였으나 새롭게 제안되는 방식은 spread spectrum 신호의 acquisition 자체가 어렵게 함으로서 기존의 보안 기법에 비해 부가적인 보안 계층을 제공한다. 새로운 다중 접속 방식, DSS (Double Sequence Scheme)은 하나의 LFSR(Linear Feedback Shift Register)가 아닌 두 개의 LFSR을 사용하여 보안 공격에 대해 매우 강한 특성을 지닌다. 본 논문에서는 새로운 다중 접속 방식을 공격자가 침입하기 위하여 필요한 산술량을 계산하고, 이를 통해 통신한 경우의 throughput 과 지연시간등의 통신 효율 관련 지수들을 검토하였다.

ABSTRACT

Wireless medium is inherently insecure due to its broadcast characteristics. Anyone in the vicinity of ongoing communication can receive the signals being sent over the air. Moreover, an attacker can emulate a legitimate user and try to communicate with the base station. As wireless communications become more prevalent and utilize the radio channel for transmission of critical information, the concern for security becomes an important issue. In this paper a new security enhanced multiple access scheme based on slotted CDMA is introduced. Although most of the efforts in providing security has been content with letting the attacker know which bits have been sent, the newly proposed scheme provides another layer of protection by making acquisition of the spread spectrum signals difficult for unintended receivers. The new multiple access scheme, DSS(Double Sequence Scheme), utilizes not one LFSR(Linear Feedback Shift Register) PN(pseudo-random number) generator, but two LFSR PN generators of register length R and S to create a chip sequence that is extremely resistant to attacks. The number of calculations necessary for the attacker to exhaustively guess future chip sequences is analyzed and performance characteristics of the security-enhanced slotted CDMA protocol such as throughput and delay are examined.

* 서울대학교 전기공학부(kook@netlab.snu.ac.kr)
논문번호 : 97433-1130, 접수일자 : 1997년 11월 30일
※본 연구는 과학재단의 특정기초연구과제(과제번호 96-0102-10-01-3) 연구비지원에 의한 결과임

Ⅰ. Introduction

Due to recent developments in technology, wireless communication systems have become and will continue to be of great importance. More data is being transmitted over the air as cellular wireless communications become wide-spread. In the near future, Personal Communication Systems (PCSs) will transport multimedia information such as video and still pictures as well as conventional voice. And, as communication networks are integrated in a single framework, more packet data will also be transmitted through the wireless medium.

As more data is transmitted over the air, concern for the privacy of the communications arises. The radio channel is an inherently insecure medium due to its broadcast characteristics. Anyone in the vicinity of ongoing communications can receive the signals being sent over the air. In the wireline networks, there is a physical obstacle that must be overcome by an attacker. The transmission line must be breached physically before the transmitted signals can be overheard. In the wireless environment, there exist no such obstacles.

There have been numerous efforts to deal with this problem. Under an environment where any potential attacker can receive the signals transmitted, the only way to ensure security and privacy is through cryptographic techniques. The figure below depicts the general procedure in using encryption/decryption to provide secure communication between two entities.

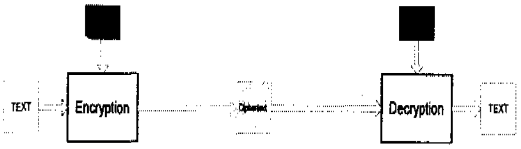


Fig. 1. Generalized Cryptographic Architecture

There are several ways to utilize the generalized cryptographic system above to provide secure communication. One of the simplest, theoretically, and surest ways of providing secure communications is to have all the end users utilize encryption and decryption software at the terminals. The information put into the communication network is itself a encrypted text and the communication network has no responsibility whatsoever for providing security. This approach is simple, yet difficult to implement as it requires every end user to implement exactly the same encryption/decryption algorithm.

Another approach is to ensure security over each link of the communication path. As has been stated, the radio link is the weakest and most susceptible to eavesdropping and intrusion. In order to defend against attacks, message encryption techniques are used. There has been studies on how to safely communicate keys between the base station and the terminal [1][2][3].

The generalized procedure for safe and private transmission of information over the radio link has been based mostly on bit scrambling where the data bits sent over the wireless medium are encrypted using a private or public (most often private) key. The eavesdropper can determine which bits have been sent, yet the communication can be considered relatively safe as the eavesdropper won't be able to make any sense of the bits that he has received without knowledge of the scrambling algorithm being used.

In Section II, the slotted CDMA-based wireless system will be discussed with emphasis on chip sequence generation and security. Security-wise problems concerning LFSR(Linear Feedback Shift Register) generated pseudo-random numbers will be looked at closely. In section III, a new medium access scheme will be introduced that utilizes the slotted CDMA framework to enhance security of the wireless system.

Ⅱ. Slotted CDMA Protocol and Random Number Generation

An important issue in implementing Personal Communication Networks is the design of the appropriate multiple access scheme for effective sharing of the limited radio channel between number of mobile users. The multiple access scheme has a great influence on user performance and overall system capacity and various methods have been proposed and implemented. The basic TDMA(Time Division Multiple Access) is used for CBR traffic in digital cellular systems such as GSM. Dynamic TDMA that supports both CBR and variable bit rate (VBR) traffic has also been proposed. Random access schemes such as ALOHA, slotted ALOHA, and CSMA (Carrier Sense Multiple Access) have been implemented in wireless and wireline environments [4]. This paper is concerned with CDMA-based multiple access techniques that combines the frame structure of TDMA with CDMA. The details of the multiple access model will be described in detail in section III.

All CDMA-based multiple access techniques have several advantages over other multiple access scheme. Due to the large user bandwidth of CDMA systems, CDMA systems provide inherent frequency diversity. Also, due to the large number of users using the same channel, there exists inherent interferer diversity. In addition, the number of transmission channels available in the system is not strictly limited as in TDMA systems. As the number of mobile users transmitting at the same time increases, the BER also increases. Moreover, the DS(Direct Sequence) CDMA already has some security protection built into the system.

In DS CDMA systems, the data bit is multiplied by chip sequences before being transmitted over the air. The signal received at the receiver, $x(t)$, is a combination of these multiplied signals from several transmitters. The receiver can determine which bits have been sent by the transmitter by multiplying the received signal, $x(t)$, with its chip sequence $c_n(t)$ and integrating. In order for this operation to result in correct determination of the transmitted data bit, the receiver's chip timing must be perfectly synchronized to that of the transmitted signal, as received with appropriate propagation delay. Note the similarity between the generalized cryptographic architecture of figure 1 and CDMA system in figure 2. The chip sequence can be viewed as a key and the multiplication of the chip sequence to the data bit acts as a encryption function.

$$x(t) = s_1(t)c_1(t) + s_2(t)c_2(t) + \cdots$$

$$\begin{aligned} &x(t)\text{: received signal} \\ &s_n(t)\text{: data bit being transmitted} \\ &c_n(t)\text{: chip sequence for terminal } n \end{aligned} \quad (1)$$

Receiver 1 will reconstruct signal $s_1(t)$ from $x(t)$ using,

$$\begin{aligned} \int_T x(t)c_1(t) &= \int_T (s_1(t)c_1(t) + s_2(t)c_2(t)\cdots)c_1(t) \\ &= \int_T s_1(t)c_1(t)c_1(t) = s_1(t). \end{aligned} \quad (2)$$

The acquisition of the chip timing is of critical importance for spread spectrum modulation systems. Various different ways to perform DS/SS acquisition have been proposed in recent years and it is currently one of the hottest topics in research. Quick acquisition in fading environment is critical for DS/SS communications. Here we are concerned not with acquisition by the intended receiver but by an eavesdropper. We are not concerned with making acquisition easy for the intended receiver but making acquisition difficult for the eavesdropper.

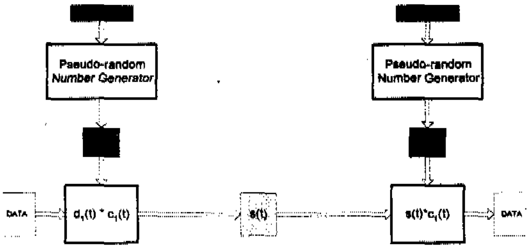

Pseudo-random Number Generator
Pseudo-random Number Generator
DATA
$d_1(t) * c_1(t)$
s(t)
$s(t)*c_1(t)$
DATA

Fig. 2. Direct-sequence spread-spectrum system

Figure 2 depicts a typical DS CDMA system architecture. Note that the chip sequences are generated using pseudo-random number generator. Pseudo-random number generators are deterministic functions that emulate random number generators. The numbers generated are not random but deterministic values of functions of the seeds. The transmitter and the receiver have identical PN generators and agree upon a common seed before the start of data transmission.

LFSRs(Linear Feedback Shift Registers) are used to generate pseudo-random numbers. LFSRs are easy to implement and very fast. Figure 3 is a simple example of LFSR. Each clock time the register shifts all contents to the right. The new value at the first register is calculated as a linear function of the register values in other registers

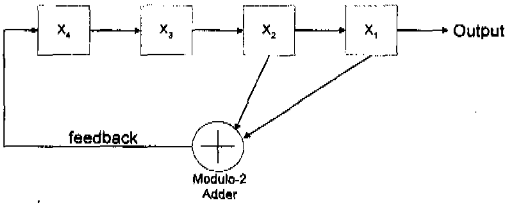


Fig. 3. Linear Feedback Shift Register

Under certain conditions the LFSR generated sequence has period $P=2^R-1$ where R is the number of registers in the LFSR. Such LFSRs are called maximum length shift registers. All the LFSR discussed in this paper are assumed to be of this type. Although the LFSR PN generators are easy to implement and produce long sequences from relatively short seeds, the LFSR generated chip sequences are extremely insecure. The knowledge of any 2R consecutive chips suffice to allow the seed to be determined, hence the entire sequence can be reconstructed by an attacker[5]. As a consequence, CDMA chip sequence multiplications as a security measure are also very insecure.

As has been stated, data bits act as plaintext and the chip sequences, as encryption keys. Due to the simplicity of the encryption function, most often multiplication, data bits are easily guessed. If the data bit value is '1' (or '0') for two consecutive bits, the signal emitted for that duration is exactly (or the inverse of) the 2R chips used as keys for those bits. Each bit is assumed to be multiplied by R chips for simplicity of analysis. The same argument is also valid for other cases.

The LFSR's initial values and the feedback connections can be determined from the signals received. The attacker can rebuild the LFSR completely from these 2R chip sequence and ascertain the correctness of the rebuilt LFSR by comparing consequently received chips with the sequence generated from the reconstructed LFSR.

Ⅲ. DSS(Double Sequence Scheme)

One can see from the discussion in section II how prone the LFSR generated chip sequences are to security breaches. Of course, the attacker has to have a-priori knowledge of the number of stages used for the LFSR and the feedback function (most often modular addition). But, such information must be assumed public and known to the attacker, since all the manufacturers must have the knowledge of such information in order to build appropriate base station and terminal hardware. Only the information that can be altered dynamically should be assumed to be secure, such as seeds for the LFSR and maybe the feedback connections.

Here we propose a new multiple access protocol based on slotted CDMA that provides security by making unintended acquisition of the signal by eavesdroppers extremely difficult. Up to this point most of the efforts in providing security has been content with letting the attacker know which bits have been sent. The privacy was provided by scrambling the bits so that the eavesdroppers are unable to make sense of the bits they have listened on. We propose adding a another layer of security to the system by making the acquisition and thereby the determination of the transmitted bits itself impossible.

A. Equal Period Sampling of the PN

In order to make acquisition by attackers difficult, the inherent weakness of the LFSR must be dealt with. Any 2R consecutive chips provide enough information for reverse reconstruction of the LFSR. The attacker knows from that point on the chip sequence being used for multiplication with the data bits. Then, the attacker can synchronize signals just as easily as the intended receiver.

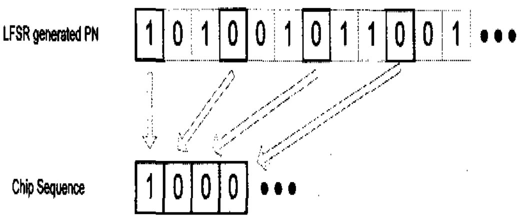


Fig. 4. Periodic sampling of the LFSR generated PN sequence.

One simple change that is possible is sampling of the LFSR generated sequence at equal intervals to produce a new sequence that can be used as the chip sequence. The chips are not consecutive outputs from the LFSR PN generator. The figure above depicts an example of the periodic sampling method.

Unfortunately the equal period sampling method described above is not very effective. The attacker can reconstruct the LFSR just as easily if he knows the period being used. The number of calculations increases as multiple of the period, yet, the number of chips that the attacker must correctly receive is exactly the same as before, 2R.

The reasoning is as follows. Let's assume that the period of sampling is M. The attacker is assumed to have knowledge of this value. The attacker knows not all LFSR outputs but those that have been sampled to be used as chips. These occur every M chips. If the outputs from the LFSR are named a_n, The eavesdropper can ascertain $a_1, a_{1+M}, a_{1+2M}\ldots$ by listening to the chips sent over the air.

$$\begin{aligned} \mathit{InitialValues} &= a_1, a_2, \cdots a_R \\ \mathit{Connections} &= c_1, c_2, \cdots c_R \end{aligned} \tag{3}$$

$$\mathit{ReceivedValues} = a_1, a_{1+M}, a_{1+2M}, \cdots \tag{4}$$

$$a_{R+n} = \sum_{k=n}^{R+(n-1)} c_{(k-n+1)} a_k \quad , k=1,2,\cdots \tag{5}$$

The attacker needs to know the initial values in the LFSRs and the feedback connections ($a_1, a_2, \ldots a_R, c_1, c_2, \ldots, c_R$). The set of equations can be solved if the number of unknown variables equals the number of equations. For $a_{R+1} = \sum_{k=1}^{R} c_k a_k \ (k=1,2,\ldots)$, there exist 2R unknown variables. If the equations for $a_{R+2}, a_{R+3}, \ldots$ are introduced to the set of equations one by one, the number of equations increases by one and another unknown variable is introduced unless n = mM+1 (m=1, 2...). When n ≠ mM + 1 (m = 1 ,2....) another unknown variable a_{R+n} is introduced to the set of equations along with another equation. When n = mM + 1 (m=1,2...), no unknown variable is introduced whereas another equation is added to the set of equations. The value of a_{R+n} is known when n = mM+1. This value is exactly the chip received over the air. Thus the difference between the number of unknown variables and the number of equations decreases by one whenever n = mM + 1, i. e the moment when the chip is sent. Therefore the attacker need only receive 2R chips that are sent over air to reconstruct the LFSR. Remember that the difference between the number of unknown variables and the number of equations was 2R-1 for the first equation introduced and that this difference is changed only when n = mM + 1.

The number of equations that must be solved, and thus the number of calculations increases M times over the conventional LFSR generated chip sequences. Yet, the number of chips that must be received is exactly the same. The main cause of the weakness of the periodic sampling scheme is that the period is a constant value that does not change. In the analysis above, we assumed that the attacker had a-priori knowledge of this constant value. Even if this value is unknown to the attacker, he can exhaustively search $2^R - 1$ possible periods which is not incomprehensible. The number of calculations necessary when the attacker does not know the period is as follows. The attacker tries all possible periods. We assume that the attacker uses Gaussian elimination to solve the system of linear equations.

$$\begin{aligned} &\mathit{Number\ of\ Calculations} = \sum_{k=1}^{2^R-1} \left(\frac{2}{3}\right)(2R\times k)^3 \\ &= \left(\frac{2}{3}\right)(2R)^3 \left(\frac{(2^R-1)(2^R)}{2}\right)^2 \\ &\cong \left(\frac{1}{3}\right)R^3\times 2^{4R} \end{aligned} \tag{6}$$

For R = 16, the number of calculations necessary is about 2^{78}. Such computing power is not unfeasible in the near future, especially considering the fact that the attacker can record the signals received over air and keep trying different combinations off-line.

B. DSS(Double Sequence Scheme)

In order to enhance the security of the radio channel, we introduce DSS multiple access scheme. The basic frame of the protocol follows that of slotted CDMA introduced in section II. We concentrate on the use of CDMA chip sequences as security measures to dramatically reduce the ability of the eavesdroppers to correctly synchronize the signals sent, thereby making correct determination of the transmitted bits impossible.

Unlike conventional CDMA systems, DSS utilizes two LFSRs to generate chip sequences. Each LFSR generates a distinct PN sequence and the two sequences are used jointly to produce a single chip sequence to be multiplied to the data bit for spread spectrum communication. We name each of these two sequences Slot Sequence and Terminal Sequence. The slot sequence is valid only for the slot it has been designated for and is shared by all the terminals transmitting over the slot. The seed and the feedback connections for this sequence is to be sent to all the terminals in the previous frame as data. We assume that this information is protected by some error control scheme and that each terminal receives it correctly. The terminal sequence, on the other hand, is different for all the active terminals and is used throughout the duration of communication. The figure 5 depicts how the slot sequence and the terminal sequence varies between the terminals and over time.

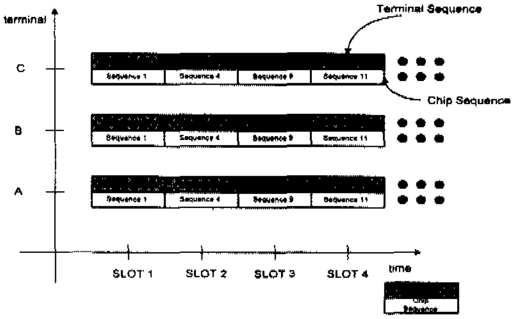


Fig. 5. Slot Sequences and Terminal Sequences.

The chip sequence is produced from the slot and terminal sequence as follows. When slot sequence is $a_1, a_2, \ldots$ and terminal sequence is $b_1, b_2, \ldots$ the chip sequence is determined as $Z_i = a_{i_k}$ where i_k is the position of the k-th '1' in the sequence $b_1, b_2, \ldots$ This method of pseudo-random chip generation is very fast and is resistant to various known attacks[6].

The attacker must guess the terminal sequence and the slot sequence from the actual chips sent. In order to determine the terminal sequence, the attacker must known at what intervals the terminal sequence is being sampled. The intervals are not constant as in the periodic sampling scheme. They themselves are pseudo-random numbers extracted from the slot sequences that change over time. Figure 6 depicts the difficulty of the attacker when trying to guess the terminal and slot sequence.

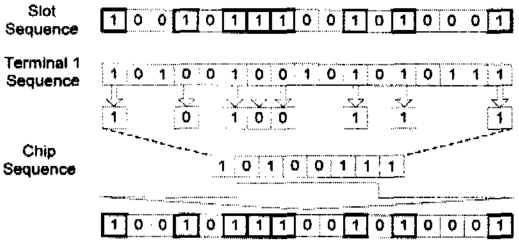


Fig. 6. Reconstruction of the LFSRs from the chip sequence

The attacker knows that there is an '1' in the slot sequence whenever a chip is sent. Although he knows which terminal sequence output has been sent, he does not know how many terminal sequence output has been skipped as he has no knowledge of the slot sequence that changes every slot. There are approximately R possibilities for the interval: approximation is due to the fact that the run length of a LFSR sequence is less than or equal to R and there can be only one run of length R-1 or R. The attacker must know how many '0's were in the slot sequence between the '1's in order to reconstruct the LFSR as it did in the periodic sampling case.

If the terminal sequence generating LFSR has R stages and the slot sequence generating LFSR S stages, there are $(2^S-1)^{2R}$ combinations of intervals between the $2R$ chips. The number of calculations necessary for exhaustive search of correct LFSR setting is as follows. If the number of skipped TS chips are $(k_{i_1}, k_{i_2}, \cdots k_{i_{2R}})$ then the number of calculations necessary is $\frac{2}{3} \times (k_{i_1}+k_{i_2}+\cdots+k_{i_{2R}})^3$. Therefore,

Number of Calculations

$$= \sum_{i=all} \frac{2}{3} (k_{i_1}+k_{i_2}+\cdots+k_{i_{2R}})^3 \tag{7}$$

$$\cong 2^{2SR} \times \frac{2}{3} (2R)^3 \frac{1}{2^S} \left(\frac{2^S \times (2^S-1)}{2}\right)^2$$

For $R=16$ and $S=16$, the number of calculations is about 10^{170} for exhaustive search. One can easily increase the difficulty of guessing by using greater number of stages in the slot sequence generating LFSR. Therefore the wireless communication system can be altered to provide any necessary amount of security by increasing the number of stages in the slot sequence generating LFSR.

C. Performance of The DSS

In order to determine DSS system's performance measures like transmit delay and throughput, a model of the scheme has been developed along with a model of the basic slotted CDMA protocol. The DSS model is based on the basic slotted CDMA protocol, but has several features added such as information slots for delivery of the masks and seeds for the generation of next frame's slot sequences. The figure below depicts the operation of the DSS model.

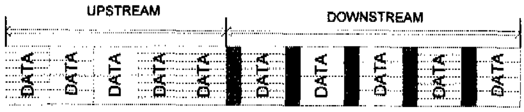


Fig. 7. DSS simulation model frame

The frame can be divided into upstream and downstream transmission phases. The upstream and downstream transmission is time-duplexed and share the same frequency bandwidth. In the upstream slots, each mobile terminals begin transmitting at the beginning of the slot. The slot sizes are same in upstream and downstream slots. 53*8= 424 bits are delivered in each slot. The number of bits delivered in a slot, 424, was chosen to reflect the fact that in the future ATM cells might be directly transmitted in the wireless environment. In the simulation, 5 upstream and downstream slots were assumed for each frame. If any error is detected within a slot, a NACK cell is sent by the base station and the upstream data is resent in subsequent frames until there is no NACK.

In the downstream phase, two kinds of slots are transmitted. The information slots precede each data slots and deliver information necessary for the implementation of the DSS scheme to the mobile terminals. Here the mask and the seed for the slot sequence generating LFSR is included. If S stage LFSR's are used for generation of slot sequences in the DSS scheme, 2S bits are needed. If 16 stage LFSR's are assumed, 32 bits of information must be sent in the information slot in order for the next frame's upstream communication to be possible in that slot. Therefore, the length of the information slot depends on the slot sequence generating LFSR's length.

To alleviate the decrease in throughput due to allocation of slots to each packets, the base station also includes in the information slot the number of mobiles that transmitted to the base station in the last frame. As the number of mobiles is less than or equal to 64, this should take 6 bits. When the mobiles receive this information, it decides whether to switch to another slot to transmit the rest of the packet. The slot it switches to is selected randomly. Thus a total of 32 + 6 = 38 bits must be sent in the information slot duration.

A detailed simulation model was built to analyze the performance of the operation mentioned above. Total system bandwidth was assumed to be 1.6 MHz and with QPSK/DPSK/MSK - type modulation, the spectral efficiency was assumed to be 1.6 bits/Hz (corresponding to a nominal 2 bits/Hz and a 25 percent excess bandwidth factor) [4]. With spreading gain of 64, the terminal data rate is 1M/64 = 15.625kbps and the data slot duration is 424 / 15.625k = 27.136 ms. With 38 bits to be sent, the information slot duration is 2.432 ms. Accounting for the guard time, the information slot duration was assumed to be 2.7136 ms. Therefore, with 10 data slots in a frame - 5 upstream and 5 downstream - and 5 information slots, a frame transmission time is about 280ms.

The mobile terminals were assumed to be in close proximity with the base station. As such, large scale and small scale fading effects were ignored. Also the Gaussian noise was assumed to be irrelevant compared to signal levels. In all, the wireless system assumed is a pico or nano-cell structure with direct line-of-sight path from the base station to all the mobile terminals. The only interference that is relevant is the cochannel multiple access interference from other mobile users. Such an environment was assumed in order to analyze the effect of designating slots to each users in order to implement the security enhancing DSS.

Each mobile terminal was assumed to generate packets consisting of several ATM cells at random times. The packets were randomly given a slot to transmit in. All the cells consisting a packet are sent on the same slot in consequent frames. The packet interarrival time was assumed to follow exponential distribution. The packet length was also randomly picked according to exponential distribution. The actual parameters used in simulation are described in table 1.

Table 1. Simulation parameters

Item	Value
Terminal data rate	20 kbps
Packet arrival rate (mobile terminal)	1.842571 packets/sec
Packet arrival rate (base station)	1.228381 packets/sec
Average packet length	8 ATM cells=3392bits
Data slot duration	27.136ms
Information slot duration	2.7136ms
Data slots per frame	10

A Slotted CDMA model without any of the DSS features was also built. All the assumptions about physical channel and traffic are the same as that of the DSS model. The frame structure consisting of 5 upstream slots and 5 downstream slots as well as total channel bandwidth of 1.6 MHz and spread gain of 64 was kept for comparison with the DSS model. The operation of this basic slotted CDMA system is as shown below. There is no information slot in front of each downstream data slots and the packets are not given a particular slot to transmit in.

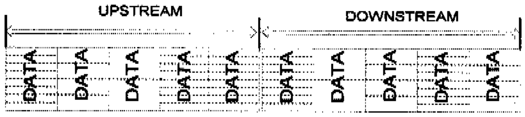


Fig. 8. Slotted CDMA transmission frame

The DSS model's performance measures compared to the basic slotted CDMA model without any security enhancing features are shown in figure 9, 10 and 11. The DSS model's throughput is lower than that of the basic slotted CDMA model. This is in part due to the overhead incurred by the security enhancing protocol, more specifically the information slots. The lower throughput is also due to the fact that all the cells in a packet must be sent in the same slot location in subsequent frames whereas cells in the slotted CDMA model can be transmitted in any slot regardless of the packet it is part of. In DSS model, the situations can arise where empty slots are available and the mobile terminal cannot use the slot because it is not the "right" slot. This has the effect of spreading the traffic in time and leads to lower slot utilization which in turn leads to lower throughput.

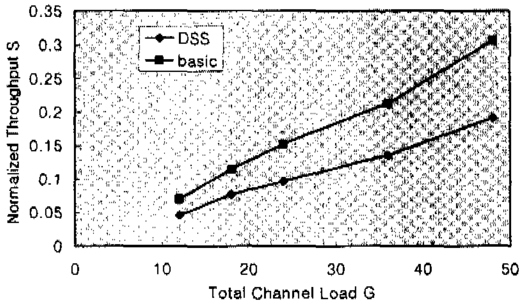


Fig. 9. Upstream data throughput

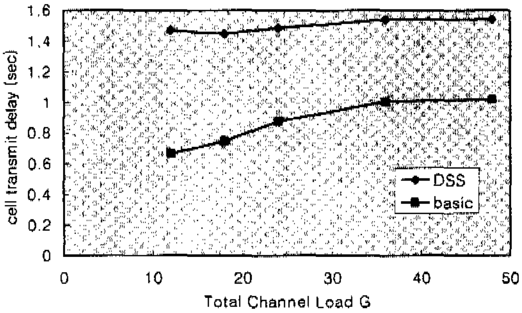


Fig. 10. Cell transmit delay

In figure 10, the delay characteristics of the DSS model is given along with that of the basic slotted CDMA model. The cell transmit delay is measure as time between the generation of the cell within a mobile terminal and the time it is received by the base station. The cell transmit delay of the DSS model stays more or less constant regardless of the total channel load. The reason for the longer delay compared to the basic slotted CDMA model is much the same as that for lower throughput. The difference in transmit delay between the two models, however, decreases as the total channel load is increased.

In figure 11, the cell error rates of the DSS model and the basic slotted CDMA model are depicted. The DSS model exhibits lower cell error rate. This is due in some part to the traffic spreading effect discussed above. There are fewer number of cell transmissions per cell. This obviously leads to less MAI and lower cell error rate. The slot switching algorithm previously introduced also helps in lowering the cell error rate by spreading the traffic between the slots in a frame.

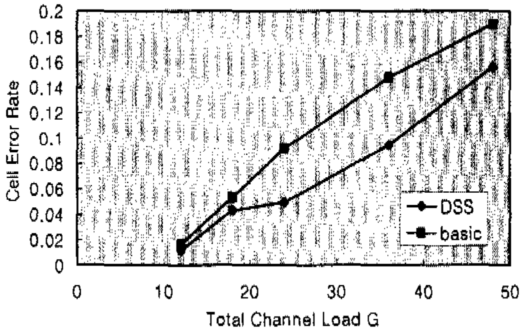


Fig. 11. Cell error rate

Ⅳ. Conclusion

A new multiple access scheme to enhance the security of wireless communication systems has been proposed. The proposed scheme, DSS, improves security of the radio link by making acquisition by unintended listeners more difficult. The number of calculations that an attacker must go through in order to correctly synchronize chip timing has been greatly increased by simple addition of another LFSR. The throughput, delay and error rates of the DSS model has been compared to that of the basic slotted CDMA model. The DSS protocol exhibited lower cell error rate compared to the basic slotted CDMA protocol but it also resulted in lower throughput and longer cell transmit delays. Therefore, the DSS protocol would be appropriate where security is critical and lower cell error rates are required and large bandwidth can be allocated, indoor wireless LANs for example. Indoor wireless LAN systems are often within range are often small. As such, bandwidth efficiency is not at big an issue as in other wireless systems. Moreover, the data that is transferred through the indoor wireless LAN is often of sensitive nature.

References

[1] M. Beller, L. Chang, Y. Yacobi, "Privacy and Authentication on a Portable Communications System", IEEE JSAC, Aug. pp. 821-830, 1993.

[2] Philippe Janson, G. Tsudik, M. Yung, "Scalability and Flexibility in Authentication Services: The KryptoKnight Approach", IEEE INFOCOM'97.

[3] Hung-Min Sun, Shiuh-Pyng Shieh, "Secret Sharing in Graph-Based Prohibited Structures", IEEE INFOCOM'97.

[4] Newman D. Wilson, R. Ganesh, K. Joseph and D. Raychaudhuri, "Packet CDMA Versus Dynamic TDMA for Multiple Access in an Integrated Voice/Data PCN", IEEE JSAC, Aug. pp. 870-883, 1993.

[5] A. Viterbi, CDMA: Principles of Spread Spectrum Communications, New York: Addison-Wesley, 1995.

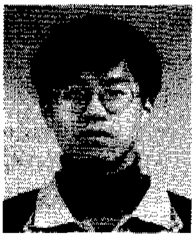
[6] D. Stinson, Cryptography: Theory and Practice, London: CRC Press, 1995.

[7] A. Polydoros, S. Glisic, "Code Synchronization: A Review of Principles and Techniques", ISSSTA'94.

[8] A. Polydoros, M. Simon, "Generalized Serial Search Code Acquisition: The Equivalent Circular State Diagram Approach", IEEE Trans. on Comm. Dec. 1984.

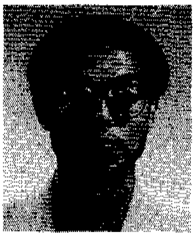
[9] C. Kaufman, R. Perlman, M. Speciner, Network Security: Private Communications in a Public World, New Jersey: Prentice-Hall, 1995.

김 영 국(Young-Kook Kim) 정회원



1994년 2월 : 서울대학교 전자공학과 졸업(학사)
1996년 2월 : 서울대학교 전자공학과 졸업(석사)
1996년 3월~현재 : 서울대학교 전기공학부 박사과정

박 세 웅(Sae-Woong Bahk) 정회원



1984년 2월 : 서울대학교 전기공학과 졸업(학사)
1986년 2월 : 서울대학원 전기공학과 졸업(석사)
1991년 12월 : University of Pennsylvania(박사)
1991년 12월~1994년 2월 : AT&T Bell 연구소 연구원
1994년 3월~현재 : 서울대학교 전기공학부 조교수