Multiaccess scheme to ensure security in CDMA-based wireless LANs

Youngkook Kim and Saewoong Bahk

A new slotted CDMA-based multiple access scheme for wireless LANs is proposed to provide enhanced security. The new multiple access scheme significantly improves the security of the system by creating chip sequences from two linear feedback shift registers.

Introduction: As more data are transmitted over the air, the privacy of the communication becomes a very serious issue. 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 wireless 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 wireless environments, no such obstacles exist.

Under an environment where any potential attacker can receive the transmitted signals, the only way to ensure security and privacy is through cryptographic techniques. The general procedure for the 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 (most often private) key. The eavesdropper can determine which bits have been sent, yet the communication can be considered relatively safe as the eavesdropper would not be able to make any sense of the bits that he has received without knowledge of the scrambling algorithm being used.

Slotted CDMA protocol and random number generation: In direct sequence (DS) CDMA systems, the data bit is multiplied by a chip sequence before being transmitted over the air. The signal received at the receiver is a combination of these multiplied signals from several transmitters. The receiver can determine which bits the transmitter has sent by multiplying the received signal with its chip sequence and integrating it. For this operation to work in a correct determination of the transmitted data bits, the receiver’s chip sequence must be perfectly synchronised to that of the transmitted signal. Note the similarity between the generalised cryptographic architecture and the CDMA system. The chip sequence can be viewed as a key, and the multiplication of the chip sequence to the data bit as an encryption function.

DSS (Double Sequence Scheme): Here we propose a new multiaccess protocol based on slotted CDMA that provides security by making unintended acquisition of the signal by eavesdroppers extremely difficult. To date, in most attempts at providing security, the attacker has been allowed to 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 obtained. We propose adding another layer of security to the system by making the acquisition and thereby the determination of the transmitted bits itself difficult.

The basic frame of the DSS protocol follows that of slotted CDMA. We concentrate on the use of CDMA chip sequences as security measures to dramatically reduce the ability of the eavesdroppers to correctly synchronise the signals sent, thereby making correct detection of the transmitted bits difficult.

Unlike conventional CDMA systems, DSS utilises 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 term each of these two sequences the slot sequence (SS) and terminal sequence (TS), respectively. The SS 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. We assume that this information is protected by some error control scheme and that each terminal receives it correctly. The TS, on the other hand, is different for all the active terminals and is used throughout the duration of communication. Fig. 1 depicts how the SS and the TS vary between the terminals and over time.

The chip sequence is produced from the slot and terminal sequence as follows. When the SS is $a_1, a_2, \ldots$ and the TS is $b_1, b_2, \ldots$, the chip sequence is determined to be $Z = a_i b_j$, where $i$ is the position of the $i$th ‘1’ in the sequence $a_i$, $b_j$, $\ldots$. This method of pseudorandom chip generation is very fast and is resistant to various known attacks [6].

If the TS generating LFSR has $R$ stages and the SS generating LFSR has $S$ stages, there are $(2S - 1)^R$ combinations of intervals between the $2R$ chips. If the number of skipped TS chips is $(k_0, k_1, k_2, \ldots, k_{2R})$ then the number of calculations necessary is $\frac{1}{3} \times (k_0 + k_1 + \ldots + k_{2R})^3$. Therefore, the number of calculations necessary for an exhaustive search of the correct LFSR setting is as follows:

$$\text{number of calculations} = \sum_{i=0}^{2R}\frac{2}{3}(k_i + k_{i+1} + \cdots + k_{i+2R})^3$$

(1)
Conclusion: A new multiaccess scheme termed DSS has been proposed to enhance the security of wireless LAN systems. The DSS scheme improves the security of the radio link by making acquisition by unintended listeners extremely difficult. The number of calculations that an attacker must go through in order to correctly synchronize chip timing has been greatly increased by the simple addition of another LFSR.

The performance of the DSS model has been compared with those of the basic slotted CDMA model. The DSS protocol exhibited lower cell error rate compared with the basic slotted CDMA protocol but it resulted in ~30% decrease in throughput and longer cell transit delay. 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 fit this description.

Indoor wireless LAN systems are often separated from adjacent wireless systems by physical walls and the number of users within range are often small. As such, bandwidth efficiency is not as big an issue as in other wireless systems. Moreover, the data that is transferred through the indoor wireless LAN is often of sensitive nature.

© IEE 1999
Electronics Letters Online No: 19990650
DOI: 10.1049/el:19990650

Youngkook Kim and Saewoong Bahk (School of Electrical Engineering, Seoul National University, Shinlim-dong, Kwanak-gu, Seoul, 151-742, Korea)

Saewoong Bahk: Corresponding author
E-mail: sbahk@ee.snu.ac.kr

References
2. JANSSEN, P., TROJOK, D., and YUNG, M.: 'Scalability and flexibility in authentication services: The KryptoKnight approach', IEEE Infocom’97, 1997,
3. HUNG-MIN SUN, and SHU-HUANG SHEE: 'Secret sharing in graph-based prohibited structures', IEEE Infocom’97, 1997

Multidimensional TCM schemes for ADSL

M. Cao, K.R. Subramanian and V.K. Dubey

Multidimensional TCM schemes can be used to improve the performance of the asymmetrical digital subscriber line (ADSL). The operating principle of how M-D (multidimensional) TCM works in an ADSL channel is analyzed and criteria for evaluating and choosing effective multidimensional TCM schemes are described. The results of a simulation for evaluating the performance is presented.

Introduction: Among the many error-correction coding schemes proposed for the DMT asymmetrical digital subscriber line (ADSL) channel, one approach is to combine TCM with Reed-Solomon codes to design a concatenated system [1]. To further improve the performance of TCM schemes, more powerful convo-