A Secure and Robust Self-Encoded Spread Spectrum Multiple-Access Approach for Multimedia Communication System

Kun Hua  
Department of Electrical and Computer Engineering  
Lawrence Technological University  
21000 W 10 Mile Road, Southfield, MI, USA 48075  
khua@ltu.edu  
Senior Member, IEEE

Honggang Wang  
Department of Electrical and Computer Engineering  
University Massachusetts Dartmouth  
Email: hwang1@umassd.edu

Guang-Chong Zhu  
Dept. of Mathematics and Computer Science  
Lawrence Technological University  
21000 W 10 Mile Road, Southfield, MI, USA 48075  
gzhu@ltu.edu

Wei Wang  
Department of Electrical Engineering and Computer Science  
South Dakota State University, USA  
Email: wei.wang@ieee.org

Athanasios V. Vasilakos  
Dept. of Computer and Telecommunications Engineering  
University of Western Macedonia  
Parko Agiou Dimitriou, Kozani, Greece 50100  
vasilako@ath.forthnet.gr  
Senior Member, IEEE

Abstract— In multimedia communication, various data rates, security strategies, and data qualities are required for different content forms such as text, audio, images, video, and interactivity content forms. In this paper, we propose a secure and robust approach to achieve the multimedia multiple access (MA) communication using self-encoded spread spectrum (SESS). In this proposed system, SESS multiple access (SESS-MA) is a novel approach to multimedia system due to its unique secure and flexible spreading nature. Iterative detection is applied for an improved multimedia quality of service (QoS) at the receiver. The number of iterations needed is evaluated separately according to different multimedia contents. Simulation studies demonstrate that the proposed scheme ensures satisfactory data quality, security, and robustness.

Keywords—Multimedia Communication, Self-Encoded Spread Spectrum, Multiple Access, Security.

I. INTRODUCTION

In recent years, wireless multimedia communication has been drawing increasing research interest due to the availability of smart phones, tablets, laptops, and their broad application opportunities [1-2][15-16]. But it is critical to provide security and privacy assurances for multimedia communication in applications including military and civilian surveillance, online gaming and gambling, and personal health care, etc. [3]. Such guarantees will ensure the widespread adoption of above information systems, leading to large-scale societal and economic benefit. To efficiently address these protection and reliability issues, secure processing and communications should be evaluated from system inception. Due to the emerging nature of multimedia communication, this provides fertile research land for proposing more approaches of paradigm shifts.

Traditional CDMA uses a pair of pseudo-noise (PN) code generators on both sides of sender and receiver, which brings more and more security risks with the quick development of computing and digital signal processing techniques. Recently, several researches have been done on hostile detecting by means of data mining methods [8]-[10]. As Jia found in [11], the malicious detection of DSSS watermarks could be completed in 7 second with the successful rate of 95%, via mean-square autocorrelation (MSAC), because MSAC shows periodic peaks due to self-similarity in the modulated traffic caused by homogeneous PN codes that are used in modulating multiple-bit signals.

To solve the problem above, Self-encoded spread spectrum (SESS) as a novel approach was pioneered by Nguyen [4] in 1999 for secured digital communication. Unlike the conventional direct spread spectrum scheme, SESS completely eliminates the need of PN code generators, and achieves security in the transmission of digital contents by exploiting the spread-spectrum nature of the signal as well as the stochastic nature of the unique spectrum spreading and despreading processes [4]. This powerful method has been further investigated at Lawrence Technological University when applied to multimedia communication systems. The capacity of self-encoded multiple access system in additive white Gaussian noise (AWGN) channels was analyzed by Jang and Nguyen in 2000 [5]. In 2010, Ma et al. proposed a multiple-input multiple-output (MIMO) SESS design with iterative detection for Rayleigh fading channels [6]. Furthermore, Chi et al. evaluated SESS for multi-rate multimedia communication in multipath channels [7].
The main contributions of this paper are as follows:

1. We propose a secure and reliable multiple-access approach to multimedia communication using SESS and Unequal Error Protection (UEP) techniques. UEP is a powerful framework for protecting scalable bit streams against bit errors. Specially, the spreading length and the number of iterations for each multimedia application will be fine-tuned to balance energy efficiency, transmission delay, and quality of service (QoS). So far SESS has been successfully designed with MIMO and iterative detections. But little work has been done for adaptive design for various contents of multimedia with multiple users.

2. In multimedia communication, various QoS features (e.g., data rates, security strategies, delay tolerance, and data qualities, etc.) are required for different content forms such as scalar sensor data, still images, audio and video streaming. Accordingly, a specific spreading length and the number of iteration will be determined via a UEP strategy.

3. We consider incorporating iterative detection technique to achieve additional gain with various numbers of iterations.

In section II, we describe the system model. Section III presents the analytical and simulation results. The conclusion and future work follow in IV.

II. PROPOSED ADAPTIVE SESS-MA MULTIMEDIA COMMUNICATION SCHEME

Fig. 1 shows the block diagram of SESS with iterative detection at the receiver. The spreading code of current bit \( b_{N+1} \) is obtained from the delayed random digital information source itself (\( b_0, b_1, b_2, \ldots, b_{N-1}, b_N \)). At the transmitter, the current bit is spread by the time-varying, \( N \)-chip sequence that has been obtained from the previous \( N \) data bits (to be \( b_{N+1}b_0, b_{N+1}b_1, b_{N+1}b_2, \ldots, b_{N+1}b_{N-1}, b_{N+1}b_N \)). As a result, the dynamic variable spreading sequences assure the transmission security and low probability of detection (LPD) by attackers. At the receiver, the self-decoding process carries out a reversed operation at the receiver. The previously decoded data are fed back to the \( N \)-bit delay shift registers for signal de-spreading (\( b_0, b_1, b_2, \ldots, b_{N-1}, b_N \)) [4].

A bit error would result in a chip error that not only will attenuate received signal strength at the output of the correlator, but will also propagate through the shift registers and affect the following bit decisions [13][17]. The dynamic of the system performance during tracking can be investigated with Markov chain analysis [14][18].

For \( m \) chip errors among total \( N \) bits in the shift registers, the amplitude attenuation at the correlator output is calculated as:

\[
A_{\text{in}}^{m} = 1 - \frac{2m}{N}
\]

Thus, the conditional probability of error given \( m \), \( P_{\text{erm}} \), is given as:

\[
P_{\text{erm}} = Q \left( 1 - \frac{2m}{N} \sqrt{\frac{2E_a}{N_0}} \right)
\]

where \( Q(\cdot) \) is the Q-function and \( E_a/N_0 \) is the symbol SNR under AWGN.
We can write the SESS signals as:
\[
\begin{align*}
    s_1 &= b_0b_1, \quad b_{-1}b_1, \quad \ldots \quad b_{-N+1}b_1 \\
    s_2 &= b_0b_2, \quad b_{-1}b_2, \quad \ldots \quad b_{-N+1}b_2 \\
    s_3 &= b_0b_3, \quad b_{-1}b_3, \quad \ldots \quad b_{-N+1}b_3 \\
    \vdots \\
    s_N &= b_{N-1}b_N, \quad b_{N-2}b_N, \quad \ldots \quad b_0b_N \\
    s_{N+1} &= b_Nb_{N+1}, \quad b_{N-1}b_{N+1}, \quad \ldots \quad b_1b_{N+1}
\end{align*}
\]

where \(b_i\) is the data bit delayed to form the SESS spreading sequences. Since the current bit is spread by \(N\) previous bits, we can observe that current detecting bits \(b_i\) is spread by \(N\) previous symbols \(b_{i-1} \ldots b_{i-N}\) at a rate of \(N/T\).

From above equations, we can see that current detecting bit \(b_i\) is not only related to previous \(N\) information bits, which are stored in the delay shift register \(b_{N+1} \ldots b_0\), but also related to \(N\) future transmitted signals \(s_2, \ldots, s_{N+1}\) containing the information about \(b_i\). By incorporating future transmitted signals together with previous detected bits, we expect to improve the performance over the feedback detector, which only estimates the current bits by correlating with \(N\) previously detected bits.

As an example shown above, if we pick spreading length \(N=4\), we hold the decoded 4 bits of \(b_4\) as shown in the very last row of the following matrix, or feedback decoding process; the future data bits are kept rolling in and decoded by previous \(N\)-bits until \(b_4\) comes in, then we found additional 4 \(b_4\) of all on-diagonal elements. In other words, a single detected information bit (e.g., \(b_4\)) amount is doubled from 4 to 8 with iterative detection, compared to feedback detection. Therefore, a 3dB performance gain can be achieved by the iterative detectors. This is because iterative detection not only uses the last \(N\)-bit sequence to recover data in the receiver, but also employs \(N\) future sequences in decoding decision: the detector SNR is thereby doubled.

The adaptive SESS-MA multimedia communication system investigated in this paper is schematically shown in Figure 2. All bandwidth expansion is achieved by a different SESS modulator for each individual user, producing \(N\) encoded chips per information bit. These chips are then transmitted over mobile radio channel to the receiver side. Similar signals from other users (MAI) are added, producing the resulting received signal. Unlike code-spreading CDMA system, where non-spreading user-specific long PN scrambling sequences are required for user separation, SESS-MA does not require additional PN codes. The self-encoded structure not only spread the information bits but also separate signals from each individual user. Here we can raise two applications as examples:

(1) For real time video stream transmission, large data rate and small transmission delay are expected. Thereby we pick a relevant smaller spreading length \(N\) and also a smaller iteration number (e.g. \(IT=1\), which means one loop iteration) at the receiver.

(2) For private and emergent Electrocardiogram (ECG) signal transmission with much lower transmission rate, high signal quality and transmission security are expected. Thereby we pick a relevant larger spreading length \(N\) and also a larger iteration number (e.g. \(IT=4\)) at the receiver.

From eq.(2), we can derive spreading length \(N\) as:
\[
N = \frac{2m}{1 - \sum_1^N \frac{1}{(P_{\text{err}})^{\alpha}}}
\]

If we also consider the average \(Arq\) retry limit and symbol rate \(R_s\), eq. (3) will be changed to:
\[
N = \frac{2m}{\alpha R_s \cdot Arq \cdot \left(1 - \sum_1^N \frac{1}{(P_{\text{err}})^{\alpha}} \right)}
\]

where \(\alpha\) is the constant coefficient to make sure \(N\) in a reasonable range (e.g., 4-1024).

III. Simulation Results

![Fig.3. Self-Encoded Spread Spectrum BER Performance, Feedback Detection, N=128 and 1024.](image)

In the SESS system, spreading sequence is derived from data source itself and the receiver does not need to know it ahead of time. Fig 3 shows that self-interference causes a performance degradation compared to binary phase-shift...
keying (BPSK) modulation at low SNR. Also at low SNR region, the BER performance degrades as N decreases. The degradation is caused by error propagation, as each detection error contributes to higher attenuation of the signal strength for shorter N cases. As SNR increases, the performance curves converge into one. The effect of self-interference is reduced as the spreading length increases, and is practically eliminated for N>64.

In Fig. 4, we set iteration number IT=1. By comparing BER performance of N=128 with Fig.3, we can conclude that iterative detection can achieve a 3dB gain when compared to a feedback detector. This is because in iterative detection, by not only using the last N-bit sequence to recover data in the receiver, but also exploiting the next N-bit sequence to make an improved decoding decision. Signal’s energy is doubled but noise energy remains the same value.

In Fig.5, when iteration is repeated more than once, for every loop of the iteration, we need N more future bits to make decisions. The most significant improvement in terms of BER is achieved between iteration 1 and 2. We observe that very limited performance gain can be further achieved by increasing the number of iterations. Comparing to DBPSK, iteration detector can achieve 3dB gain. And BPSK performance curve achieves the upper bound.

As expected, the effect of self-interference is worsening as the number of users increases, which introduces higher MAI. The BER performance degrades gradually as user number increases from 1 to 16. But increasing spreading length will reduce system load, so we can mitigate the effects of both MAI and self-interference.
In this paper, we propose an SESS-MA approach to achieve secure and robust transmission for multimedia systems under various QoS requirements. The adaptive parameters for multimedia transmissions are well designed and simulated, and their BER performances are compared. In SESS-MA, we observe that SESS significantly improves the security and robustness of multimedia communication for AWGN channels, and that SESS iterative detection outperforms feedback detection. Simulation studies demonstrate that the proposed scheme ensures satisfactory data quality, security, and robustness. We plan to extend our experiments to cross-layer design in cooperative communication system. Our future research also includes performance analysis of SESS with iterative detection under frequency-selective fading channels.

![Fig. 7 BER Performance of SESS-MA for K=1,2,4,8,16 N=64, Iterative Detection, IT=1 (one loop iteration).]

**REFERENCES**


