Chapter 11
Conclusions and Future Directions

11.1 Conclusions

In this book, sequence synchronization techniques for single and multiple-access chaotic communication systems have been investigated. In particular, the techniques of sequence synchronization studied include those based on the principles of Pecora-Carroll (PC) chaotic synchronization and those based on the principles of traditional DS-CDMA synchronization.

Based on the principles of PC chaotic synchronization, the novel approaches to chaotic synchronization were proposed and used to design new single-user chaotic communication systems. These new chaotic communication systems include those based on the chaotic parameter modulation (CPM) and initial condition modulation (ICM) techniques. Furthermore, the principles of time division multiplexing (TDM) were used to obtain the CPM and ICM based multi-user TDM systems. The performance of all of the proposed and the existing systems was evaluated in terms of the bit error rate (BER) in the additive white Gaussian noise (AWGN) and the Rayleigh fading channels. Furthermore, it was shown that by implementing certain linear and wavelet filters, one can improve the BER performance of the ICM based systems in the AWGN channel.

The sequence synchronization of chaotic communication systems based on the DS-CDMA principles was then proposed. It was shown how the mutually orthogonal properties between the logistic map chaotic time series and the PRBS pilot signal enable the traditional ideas of the multi-user CDMA sequence synchronization process to be utilized within the multi-user chaos based DS-CDMA system. Furthermore, the system was taken one step further by introducing a chaotic pilot signal in place of the PRBS pilot signal, thus making the CBDS-CDMA system fully chaotic and eliminating the security threat posed by an inherently different PRBS pilot signal. Both phases of the sequence synchronization process, namely the code acquisition and the code tracking, were proposed and investigated. It was shown that in terms of BER the chaos based DS-CDMA systems outperform the CPM and ICM based TDM systems for low number of users in the AWGN channel. However, for larger number of users in the system, the BER curves of the chaos based DS-CDMA systems flatten before reaching the adopted highest acceptable BER level of 10^{-3}. In contrast to this, the BER curves of the CPM and ICM based TDM systems do not flatten and thus outperform the chaos based DS-CDMA system for large number of users. In

B. Jovic: Synchronization Techniques for Chaotic Commun. Syst., SCT 5, pp. 317–324.
springerlink.com

addition, it was found that the chaos based DS-CDMA system outperforms the ICM and CPM based TDM systems in the Rayleigh fading channel. However, they all fail to satisfy the highest acceptable BER level of 10^{-3} in the Rayleigh fading channel. Finally, it was shown that in terms of BER, in the AWGN channel only, the proposed chaotic pilot based CBDS-CDMA systems marginally outperform the PRBS pilot based system for a single user in the system at the BER level of 10^{-4} and below.

In addition to the CPM and ICM based TDM systems and the chaos based DS-CDMA system, the chaos based TDM system with the DS-CDMA correlator receiver was also proposed. It was shown that this system outperforms the CPM and ICM based TDM systems for any number of users. However, the system was outperformed by the chaos based DS-CDMA systems for low number of users and vice versa for large number of users.

In order to mutually exploit the DS-CDMA and TDM benefits, a generalized chaos based TDM communication system with more than one DS-CDMA user per TDM branch was proposed and evaluated in the AWGN channel. In this way, the bandwidth efficiency of a DS-CDMA system was combined with the interuser interference immunity of a TDM system, to allow for an increased number of users in the system while improving the BER performance.

In general, it can be concluded that the multi-user chaotic communication systems based on the acquisition and tracking synchronization scheme, are more robust to AWGN and Rayleigh fading than those based on the principles of chaotic synchronization.

Finally, the security of the proposed, as well as of the existing chaotic communication systems, was evaluated in terms of the average power of the chaotic carriers of the bits transmitted. In order to do so, the two new measures were developed. These were termed the 'Bit Power Parameter Spectrum' (BPPS) and the 'Bit Power Initial Condition Spectrum' (BPICS) measures. Using these measures, it was shown that chaotic communication systems can be optimized in terms of security.

In chapter 1, the three main categories of the multi-user mobile communication systems (FDMA, TDMA and CDMA), as well as some of their hybrids, were introduced. Furthermore, the disturbances encountered within the physical transmission channel, such as the additive white Gaussian noise and Rayleigh fading, were presented. The concept of the bit error rate, which is used to measure the effects of the channel imperfections on the transmitted signal, was then outlined. In addition, the procedure of evaluating the bit error rate was then demonstrated when noise and fading are present in the channel. Finally, the motivation of the book was stated by demonstrating the importance of synchronization among the transmitter and the receiver through its effect on the BER performance of the system.

In chapter 2, the phenomenon of chaos was introduced. The Lyapunov exponents which are used to diagnose and characterize the system were then presented. Furthermore, the two different approaches of implementing chaotic systems within secure communication systems were outlined. These include

chaotic communication systems based on the principles of chaotic synchronization and those based on the DS-CDMA principle. Finally, some of the filtering techniques that can be used within chaotic communication systems were briefly introduced.

Chapter 3 examined synchronization of chaotic systems. The concept of the Pecora-Carroll chaotic synchronization was described and its properties examined in terms of the conditional Lyapunov's exponents and Lyapunov's direct method. These demonstrate two different, yet most common approaches to the analysis of chaotic synchronization. Furthermore, Lyapunov's direct method was then used to show a general approach to the design of nonlinear controllers for the master-slave chaotic systems.

In chapter 4, a method of designing the nonlinear control laws for the synchronization of the chaotic map master-slave systems was proposed. The nonlinear control laws were designed in such a way to ensure that the eigenvalues of the error system matrix always fall within the unit circle in the z domain. This ensures the global asymptotic stability of the error system and thus causes the master-slave system of any complexity to synchronize. The general approach to the master-slave chaotic map synchronization was demonstrated on the $\Re^1$ cubic map master-slave system, the $\Re^2$ tinkerbell map master-slave system and the Lorenz $\Re^3$ chaotic map master-slave system. Furthermore, it was shown that it is always possible to achieve instant synchronization, within a single iteration of the master-slave system, when the control laws are designed in such a way to reduce the error system matrix to zero.

In chapter 5, the master-slave synchronization properties of the simplest quadratic chaotic flow and the Ueda chaotic system were investigated by a newly proposed mathematical analysis. It was shown that when the z signal drives, the synchronization error of the simplest quadratic master-slave y signals is constant whereas the synchronization error of the master-slave x signals increases linearly. Using numerical simulations, in conjunction with mathematical analysis, it was demonstrated that the simplest quadratic master-slave chaotic flow does not synchronize when the y signal drives; however, the synchronization error of the master-slave z signals tends to a constant value which is predictable and can be expressed as a combination of the master-slave x signals' initial conditions and the system's parameter value. It was found that the simplest quadratic master-slave chaotic flow synchronizes when the x signal drives.

Furthermore, it was found that the Ueda master-slave chaotic system does not synchronize when the master y or the master z signal drives. However, it was shown that the master-slave y signals do synchronize under certain conditions when the master x signal drives. When the signal x drives, mathematical manipulation of the system's dynamics allows one to determine a useful mathematical expression for the error of the master-slave y signals. This expression, along with the numerical simulations, allows one to predict that if the difference between the master-slave z signals' initial conditions equals $\pm 2n\pi$, the master-slave y signals will always synchronize. When the y signal drives, the synchronization error is constant and was mathematically expressed.

In general, it can be concluded that the synchronization properties of chaotic systems, in particular Pecora-Carroll synchronization properties, do not necessarily have to be investigated by Lyapunov's stability theory, or by evaluation of conditional Lyapunov exponents. Instead, direct mathematical analysis can be used in certain cases, as was demonstrated in chapter 5 for the simplest quadratic chaotic flow and the Ueda chaotic system.

In chapter 6, several chaotic communication systems with the receiver based on chaotic synchronization were described. These include the chaotic communication schemes of chaotic masking, chaotic modulation and the new chaotic communication scheme of initial condition modulation.

It was shown how Lyapunov's direct method, presented in chapter 3, can be used in the design of the CPM based communication systems. In particular, this was shown on the Ueda master-slave chaotic system.

Furthermore, a method of implementing the synchronized chaotic map master-slave system of chapter 4 within a CPM based secure communication system, was demonstrated on the $\mathfrak{R}^1$ cubic map. It was shown that instant synchronization within the chaotic map CPM based communication system allows for the highest level of discrimination among bits 0 and 1.

On the basis of findings of chapter 5, a secure communication system based on the initial condition modulation of the chaotic carrier by the binary message was then proposed. In particular, this system utilizes a novel approach to the master-slave synchronization properties of the three chaotic flows investigated. The empirical BER curves for the proposed communication systems were then produced and compared to the empirical BER curve of the Lorenz CPM based communication system, demonstrating a significant improvement. It was shown that the communication system based on the simplest quadratic master-slave chaotic flow exhibits the best performance in terms of BER, as compared to the other two proposed systems based on the Ueda and the simplest piecewise linear master-slave chaotic flows. From the security point of view it was observed that the communication system based on the Ueda master-slave chaotic system may be the most secure of the three systems proposed.

Finally, the overall performance of the chaotic parameter and initial condition modulation techniques was examined and compared in the presence of AWGN. It was shown in terms of BER that the ICM based chaotic communication systems exhibit better noise performance than the CPM based ones. Furthermore, it was shown on the Ueda ICM based chaotic communication system that the denoising techniques can be used to further improve the BER performance. The denoising techniques, including linear and wavelet filters, were presented in the appendix.

In chapter 7 chaotic carriers were embedded within a practical multi-user DS-CDMA chaotic communication system and its performance evaluated in the presence of noise and interuser interferences. It was shown how the mutually orthogonal properties between the chaotic time series produced by the logistic map and the PRBS pilot signal enable the traditional ideas of the multi-user CDMA sequence synchronization process to be utilized within the multi-user chaos based DS-CDMA (CBDS-CDMA) system. Furthermore, the system was taken one step further by introducing a chaotic pilot signal in place of the PRBS

pilot signal, thus making the CBDS-CDMA system fully chaotic. In this way, the security of CBDS-CDMA systems is significantly improved by eliminating the security threat posed by an inherently different PRBS pilot signal used in the otherwise chaotic CBDS-CDMA systems. Both phases of the sequence synchronization process, namely the code acquisition and the code tracking, were proposed and investigated.

The code acquisition phase was evaluated in terms of the probability of detection and the probability of false alarm at the chip energy to noise power spectral density ratio of -15 dB for the three different pilot signals and varying number of chaotic users in the system. The theoretical upper bound on the probability of detection was derived and compared to the empirically determined results with the chaotic interferences present. The subsequent empirical curves associated with the increasing number of users in the system have demonstrated the expected degradation in the system performance with the increasing level of interference. In addition, the expected increase of the probability of detection, with the increase in the integration time, was demonstrated. Furthermore, it was shown that the best code acquisition performance is achieved when the PRBS is used as the pilot signal as compared to the logistic and Bernoulli chaotic maps.

The mathematical models for the investigation of the code tracking loops were presented and used to derive the control laws used for the generation of the time offset estimates for PRBS and, periodic and non-periodic chaotic pilot signals. Their validity was then demonstrated by means of a simulation. The performance of the proposed code tracking circuits was primarily evaluated in terms of the bit error rate for varying levels of the chaotic interuser interferences, that is, for different numbers of chaotic users in the system. It was shown that the system is reasonably robust to noise as compared to the performance under the assumption of perfect synchronization. The overall BER performance degradation in an AWGN channel for a multi-user system is characterised by the flattening of the BER curves at low levels of noise due to the prevailing effects of the interuser interferences.

Furthermore, it was demonstrated that the CBDS-CDMA communication systems implementing the proposed sequence synchronization schemes, with a single user in the system, in general exhibit better noise performance in terms of the bit error rate than the Pecora-Carroll CS based communication techniques. It was shown that although the systems are robust to the influence of AWGN and interuser interferences, they all fail to satisfy the maximum allowable bit error rate limit of 10^{-3} in the Rayleigh fading channel, exbhibiting identical BER performance.

Finally, it was shown that in terms of BER, in the AWGN channel only, the proposed chaotic pilot based CBDS-CDMA systems outperform the PRBS pilot based system for a single user in the system at the BER level of 10^{-4} and below. In particular, an improvement of 0.175 dB was demonstrated at the BER level of 10^{-6}. Therefore, in addition to the added security, it was demonstrated that by introducing the chaotic pilot based tracking unit in place of the corresponding

PRBS unit makes the CBDS-CDMA system more robust. The BER performance of all systems was shown to be identical for more than one user in the system.

In chapter 8, a chaos based multi-user TDM system was proposed and evaluated in terms of the bit error rate. Its performance was investigated with and without the assumption of perfect sequence synchronization in the noisy and Rayleigh fading channels. Furthermore, the BER performance of the chaos based DS-CDMA system was compared to the performance of the chaos based multi-user TDM system. The chaotic spreading signals, used to encrypt the binary messages, were generated using the logistic map. As in chapter 7, the mutually orthogonal properties, between the chaotic time series produced by the logistic map with different initial conditions, were used to decrypt messages sent across the channel.

Assuming perfect sequence synchronization, it was shown that in the AWGN and Rayleigh fading channels the TDM system reaches the adopted minimum allowable BER level of 10^{-3} for 1-5, 10, 15 and 20 users in the system. Furthermore, it was shown that in terms of BER the chaos based multi-user TDM system outperforms the chaos based DS-CDMA system for large number of users in the system, while the chaos based DS-CDMA system yields better performance for low number of users in the system.

The proposed chaos based TDM system was then investigated without the assumption of perfect sequence synchronization in the AWGN and Rayleigh fading channels. Again, it was shown that in terms of BER the chaos based TDM system outperforms the chaos based DS-CDMA system for large number of users in the system and vice-versa for low number of users in the system. In order to obtain the full characterization of the system, the sequence synchronization was also assumed with the PRBS pilot signal present on top of each user signal. The effect of the pilot signal on the performance of the system was thus demonstrated in AWGN and Rayleigh fading channels. Furthermore, it was shown that both chaos based TDM and chaos based DS-CDMA systems are insufficiently robust in the Rayleigh fading channel when the perfect sequence synchronization is not assumed.

In order to mutually exploit the DS-CDMA and TDM benefits, a generalized chaos based TDM communication system with more than one DS-CDMA user per TDM branch was proposed and evaluated in the AWGN channel. In this way, the bandwidth efficiency of a DS-CDMA system was combined with the interuser interference immunity of a TDM system, to allow for an increased number of users in the system while improving the BER performance.

In chapter 9, the chaotic synchronization based multi-user TDM systems were proposed and evaluated in terms of BER in AWGN and Rayleigh fading channels. In particular, the proposed systems include the Lorenz and Ueda CPM based TDM systems and the Ueda ICM based TDM systems. It was shown that in terms of BER, the ICM based TDM systems outperform the CPM based TDM systems in both AWGN and Rayleigh fading channels. Furthermore, it was found that the Ueda ICM based TDM system with only the master signal x transmitted, outperforms the Ueda ICM based TDM system with both master signals x and y transmitted. However, the BER analysis in the Rayleigh fading channel revealed

that both CPM and ICM based systems fail to satisfy the highest acceptable BER level of 10^{-3} for any number of users in the system and any E_b / N_o. In addition, two different receiver architectures were implemented and evaluated in terms of BER on all of the CPM and ICM based TDM systems. These include the predetermined threshold receiver architecture and the receiver architecture implementing the two slave systems. It was shown that in terms of BER only in the case of the Lorenz CPM based TDM system the two slave receiver architecture outperforms the predetermined threshold architecture.

Furthermore, the BER performance of the CPM and ICM based TDM systems was compared to the BER performance of the chaos based DS-CDMA system of chapter 7 and the chaos based TDM system of chapter 8. Again, the comparison was conducted in both AWGN and Rayleigh fading channels. It was shown that in terms of BER the chaos based DS-CDMA system of chapter 7, outperforms the CPM and ICM based TDM systems for low number of users in the AWGN channel. However, for larger number of users in the system, the BER curves of the chaos based DS-CDMA system flatten before reaching the highest acceptable BER level of 10^{-3}. In contrast to this, the BER curves of the CPM and ICM based TDM systems do not flatten and thus outperform the chaos based DS-CDMA system for larger number of users. Furthermore, it was shown that the chaos based TDM communication system of chapter 8, outperforms the CPM and ICM based TDM systems for any number of users and any E_b / N_o. Finally, it was shown that the chaos based DS-CDMA system of chapter 7 and the chaos based TDM system of chapter 8; outperform the CPM and ICM based TDM systems in the Rayleigh fading channel. Therefore, it can be concluded that in general, the multi-user chaotic communication systems based on the acquisition and tracking synchronization scheme of chapter 7, are more robust to AWGN and Rayleigh fading than those based on the principles of chaotic synchronization of chapters 3, 5 and 6.

In chapter 10, the security of the proposed, as well as of the existing chaotic communication systems, was evaluated in terms of the average power of the chaotic carriers of the bits transmitted. In order to do so, the two newly proposed measures were used. These were termed the 'Bit Power Parameter Spectrum' (BPPS) and the 'Bit Power Initial Condition Spectrum' (BPICS) measures.
Initially, the method of implementing the synchronized master-slave system within a CPM based secure chaotic communication system was demonstrated on the two dimensional Burgers' map. The nonlinear control laws were designed in such a way to force the synchronization among the master and slave systems using only one signal of the master system. This is of particular importance for communications as only one signal needs to be transmitted thus reducing the required bandwidth.

The security of the Burgers' and the Lorenz CPM, as well as of the Ueda ICM, chaotic communication systems was then evaluated. The security of the proposed and the existing systems was evaluated in terms of the average power of the chaotic carriers of the bits transmitted, that is, in terms of the BPPS and the BPICS. It was shown that due to the largest BPPS and BPICS overlap region of

the chaotic carriers of the transmitted bits, the Ueda ICM based chaotic communication system is more secure than the CPM based chaotic communication systems. Furthermore, it was shown that the BER performance of the CPM based chaotic communication system, implementing Burgers' map system, can be optimized. The optimization is achieved by choosing the parameter sets, representing bits 0 and 1, to be as far apart as possible within the secure operating region.

11.2 Future Directions

Wide scale research into chaotic communications was triggered by the discovery that chaotic systems can be synchronized, which is a necessary requirement for many communication systems. However, due to the lack of sufficiently robust synchronization techniques, the chaotic communication systems have thus far only been of academic interest. In order for the chaotic communication systems to become of practical interest, more robust synchronization techniques must be developed for the future. In this book, the techniques for robust synchronization of chaotic communication systems have been developed, thus powering the way for future research in this area.

Furthermore, with the development of secure communication techniques based on the concept of chaotic synchronization, eavesdropping techniques have also been developing.

Eavesdropping techniques such as those based on the prediction attacks, short-time zero-crossing rate (STZCR) attacks, generalized synchronization attacks, return map attacks, spectral analysis attacks, parameter estimation attacks, among other, highlight the lack of security in many of the proposed systems. For secure chaotic communication systems of the future it is also necessary to seriously address the practical issues of eavesdropping.