ELSEVIER

Physics Letters A 303 (2002) 345–351

PHYSICS LETTERS A

www.elsevier.com/locate/pla

Cryptography with cycling chaos

A. Palacios [*], H. Juarez

San Diego State University, Nonlinear Dynamics Group, Department of Mathematics, San Diego, CA 92182-7720, USA

Received 27 June 2002; received in revised form 13 September 2002; accepted 17 September 2002

Communicated by C.R. Doering

Abstract

Periodic switching of cryptographic keys is commonly employed as a mechanism to enhance the security of encryption methods. In this Letter, cycling chaos, in which orbits of certain coupled iterated maps make periodic excursions between chaotic sets, is proposed as a new encryption approach that combines chaotic behavior with periodic switching of keys. The actual encryption process is similar to the one used by Baptista [Phys. Lett. A (1998) 50], except that now different chaotic attractors, and consequently different keys, are periodically switched to encrypt each character of a message. Advantages and disadvantages of this approach are also discussed.

PACS: 05.45.+b

Keywords: Coupled cell systems; Cryptography; Cycling chaos; Message; Security; Symmetry

In the past decade, methods and ideas from the theory of dynamical systems and chaos have gained wide attention in applications to communication and cryptography. For example, the seminal work by Pecora and Caroll [2] first lead to the application of synchronization in chaotic systems to transmit messages. The basic idea requires the transmitter to produce a chaotic signal to mask the message to be transmitted, also called the *plaintext*. At the receiver end, a second chaotic system is induced to synchronize with the incoming masked signal, also called *ciphertext*. A simple subtraction operation would then reveal the message. Other popular ideas for transmitting encoded messages are based on another seminal work in control of chaos [3] and control via targeting [4]. See the works of Hayes et al. [5], Schweizer and Kennedy [6], and Gligoroski [7] for more details. Recently, Kocarev and Jakimoski [8] have proposed a four-step procedure for developing block cipher algorithms based on chaotic maps. The four steps consist of choosing a chaotic map, discretizing the chaotic map, key scheduling, and cryptanalysis, which studies the recovering of plaintexts without access to the key, i.e., security. Also recently, Baptista [1] proposed to exploit the ergodicity property of chaotic systems for encryption purposes as follows. First, a one-dimensional attractor is partitioned into S equally spaced units, where each unit corresponds to a character of the alphabet under consideration. Then, in the simplest implementation version, a character is encrypted based on the initial condition of the orbit and the number of

[*] Corresponding author.
E-mail address: palacios@euler.sdsu.edu (A. Palacios).

0375-9601/02/$ – see front matter © 2002 Elsevier Science B.V. All rights reserved.
PII: S0375-9601(02)01323-3

iterations that are necessary to reach the unit associated with that particular character. Invoking the ergodicity property of chaotic systems allows Baptista to develop an encryption method where almost any orbit is forced to visit each and every one of the S alphabet units many times, thus guaranteeing that each character will eventually become encrypted. Well-known plaintext attacks, however, can be used to break the algorithm and uncover plaintexts without having access to the key. The security of this algorithm is analyzed in great detail by Jakimoski and Kocarev [9].

In this Letter, we propose the use of "cycling chaos" [10–12] to implement the security enhancement suggested by Baptista and other authors [1,13], i.e., security enhancement via periodic switching of cryptographic keys. By cycling chaos me wean orbits of discrete-time systems (or solution trajectories of continuous-time systems) that linger around various chaotic sets. Our implementation is based on discrete-time coupled cell systems but it can also be readily developed with continuous-time cell systems. Each character is also encrypted based on the number of iterations necessary to reach a portion of the attractor associated with that particular character, except that now we propose to periodically switch between several chaotic attractors—just as they are visited by a nearby cycling orbit. Each attractor can be used to form individual partitions of the alphabet. In addition to a periodical switch of keys, another immediate advantage of this approach is a natural increase in the number of keys, and consequently, in the security of the encryption process. Next, we first present a self-contained introduction to the phenomenon of cycling chaos, and then a description of its actual application to cryptography.

A generic pattern of collective behavior of symmetric networks of coupled identical cells is cycling behavior. In networks modeled by symmetric systems of differential (difference) equations, cycling behavior appears via *heteroclinic cycles* [14,15], in which solution trajectories (orbits) linger around symmetrically related steady-states (fixed points) or periodic solutions (orbits). As time evolves, a typical trajectory (orbit) stays for increasingly longer periods near each solution before it makes a rapid excursion to the next solution. Dellnitz et al. [10] have shown that symmetric identical cell systems can also produce, as a feature of the global dynamics of the network, heteroclinic cycling behavior that persists independently of the internal dynamics of each individual cell. Using Chua's circuit equations and Lorenz equations, Dellnitz and collaborators further illustrate this conclusion with simulations of a network of three identical cells connected in a directed ring fashion. In these simulations, solution trajectories can cycle around symmetrically related chaotic sets. Thus producing "cycling chaos". In later work, we demonstrated, first numerically [11] and then analytically [12], that cycling chaos also occurs in symmetric systems of coupled identical cells described by discrete-time maps. In more recent work [16], we generalized the existence of cycling behavior in larger (more than 3 cells) networks of discrete-time and continuous-time cell systems formed by identical and near-identical cells. By "near-identical" cells we mean cells whose internal dynamics is governed by identical model equations but with possibly different parameter values. Cycling behavior in near-identical cell systems is more complex in the sense that it allows for trajectories to connect a wider range of solutions, including steady-states (fixed points), periodic solutions (periodic orbits), and chaotic attractors—all in the same trajectory. And it is precisely the type of cycling chaos produced by near-identical cell systems that we propose next as a basis for a new cryptography method.

We first consider systems with N near-identical cells, where the internal dynamics of each cell is governed by a k-dimensional difference equation of the form

$$X_{i_{n+1}} = f(X_{i_n}, \lambda_i), \tag{1}$$

where $X_i = (x_{i_1}, \ldots, x_{i_k}) \in \mathbf{R}^k$ denotes the state variable of cell i and $\lambda_i = (\lambda_{i_1}, \ldots, \lambda_{i_p})$ is a vector of parameters. A network of N cells is modeled by a system of coupled difference equations of the form

$$X_{i_{n+1}} = f(X_{i_n}, \lambda_i) + \sum_{j \to i} \alpha_{ij} h(X_{i_n}, X_{j_n}), \tag{2}$$

where h is the coupling function between those cells j that are coupled to cell i, $1 \leqslant i \leqslant N$, and α_{ij} represents the strength of the coupling. Observe that f is independent of i because the cells are assumed to be identical. Similarly, h is also independent of both i and j due to identical coupling. Additionally, if we let $X = (X_1, \ldots, X_N)$ denote the state variable of the network, then we can write (2) in the simpler form

$$X_{n+1} = F(X_n, \lambda).$$

Following Dellnitz et al. [10], we distinguish *local* symmetries from *global* symmetries. $\mathcal{L} \subset \mathbf{O}(k)$ is the group of local or internal symmetries of individual cells if, for all $l \in \mathcal{L}$, we have

$$f(lX_i) = lf(X_i).$$

While local symmetries are dictated by f, global symmetries are induced by the pattern of coupling. More precisely, $\mathcal{G} \subset \mathbf{O}(N)$ is the group of global symmetries of the network if, for all $\sigma \in \mathcal{G}$, we have

$$F(\sigma X) = \sigma F(X).$$

Depending on the coupling function h, it is possible for the local symmetries l to be also symmetries of the network equations (2). In particular, when the action of l on each cell individually is a symmetry of the coupling function, so that

$$h(X_i, lX_j) = h(X_i, X_j),$$
$$h(lX_i, X_j) = lh(X_i, X_j),$$

for all $l \in \mathcal{L}$, then the coupling is called *wreath product* coupling [17].

As a representative example, we consider a network of three cells, with state variables x, y, and z, interconnected in a directed ring. The internal dynamics of each individual cell is governed by a $\mathbf{Z}_2$-symmetric cubic map

$$f(x, \lambda) = \lambda x - x^3, \quad \lambda > 0, \tag{3}$$

where $Z_2 = \{1, -1\}$. The bifurcation diagram of Fig. 1 depicts the long-term dynamics of orbits for values of λ in the range $0 \leqslant \lambda \leqslant 3$. A wide range of complex behavior can be observed in this diagram, including period-doubling cascades and chaotic attractors. In fact, the bifurcations in (3) are reminiscent of those found in the *logistic* map [18], except that now local $\mathbf{Z}_2$-symmetry forces two nontrivial fixed points (one with $x > 0$ and one with $x < 0$) to bifurcate from the trivial solution $x = 0$ at $\lambda = 1$. Each fixed point, in turn, undergoes a period-doubling cascade leading to a pair of chaotic attractors. Local $\mathbf{Z}_2$-symmetry again forces the cascades to occur at the same parameter values for each fixed point [19]. For $\lambda < \lambda_c = 3\sqrt{3}/2$, the attractors are confined to opposite sides of the $x = 0$ axis and each attractor has its own basin of attraction. At $\lambda = \lambda_c$, the basins of attraction collide and the two attractors merge into a single one. See Rogers and Whitley [20] for a more comprehensive

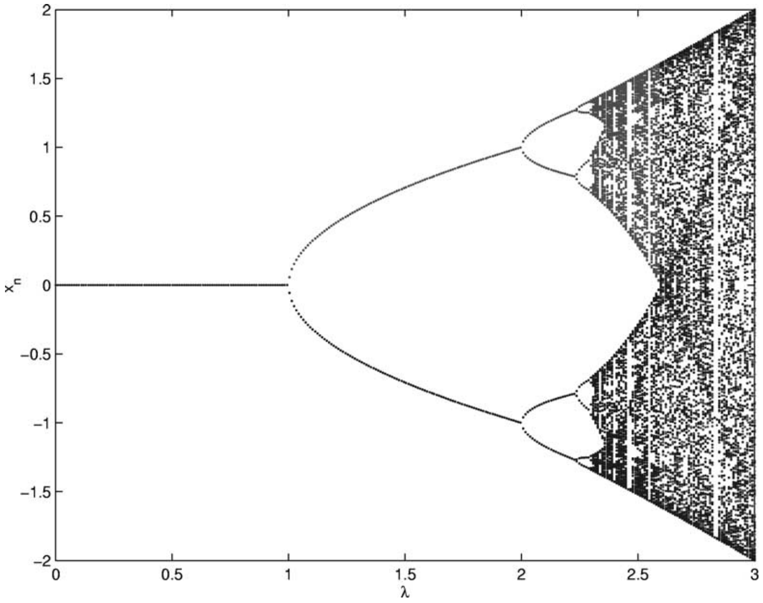

Fig. 1. Bifurcation diagram for a cell with internal dynamics $f(x, \lambda) = \lambda x - x^3$.

analysis of a similar map $f(x,a) = ax^3 + (1-a)x,\ 0 \leqslant a \leqslant 4$.

To form the interconnected network equations (2), we consider a wreath product coupling function of the form

$$h(x_i, x_j) = |x_j|^m x_i, \tag{4}$$

where $0 < m < 1$. We will assume identical coupling strength given by $\alpha_{ij} = -\gamma$, where $\gamma > 0$. Observe that, as expected, h is equivariant under the $\mathbf{Z}_2$ action. The four-cells network, which possesses local $\mathbf{Z}_2$-symmetry, and global $\mathbf{Z}_3$-symmetry when $\lambda_1 = \lambda_2 = \lambda_3$, then takes the form

$$\begin{aligned} x_n &= \lambda_1 x_n - x_n^3 - \gamma |y_n|^m x_n, \\ y_n &= \lambda_2 y_n - y_n^3 - \gamma |z_n|^m y_n, \\ z_n &= \lambda_3 z_n - z_n^3 - \gamma |x_n|^m z_n. \end{aligned} \tag{5}$$

The value of the coupling strength γ and the parameter m are critical for the creation of cycling behavior because they control the global dynamics away from the internal dynamics of an individual cell. More specifically, the fact that $0 < m < 1$ prevents the global dynamics from escaping to infinity and controls the rate at which the excursions from the dynamics of one cell to the next one occur. As m decreases, a typical orbit near a cycle spends longer time lingering around the dynamics of an active cell before it makes an excursion to the dynamics of the next cell. Additionally, if we let $X_n = (x_n, y_n, z_n)$ denote the state variable of the entire network, and $\Lambda = (\lambda_1, \lambda_2, \lambda_3)$ the vector of internal parameters, then we can write (5) in the simpler form

$$X_{n+1} = F(X_n, \Lambda). \tag{6}$$

Numerical simulations of (5) with parameter values for λ_i at which the internal dynamics of each cell is known to yield chaotic behavior were conducted. In particular, we choose $\Lambda = (3.0, 2.98, 2.87)$. Other parameter values are $m = 1/4$, and $\gamma = 3.05$. Fig. 2 depicts the results of the simulation with initial conditions $(x_0, y_0, z_0) = (-0.01, 0.03, 0.02)$. According to Fig. 1 and Lyapunov spectra (not shown for brevity), the long-term dynamics of each cell is captured by three different chaotic attractors, each one covering parts of the $[-2, 2]$ interval. At any given time, however, only one cell is active on one of the chaotic attractors, while the other cells are quiescent. The time that a typical orbit spends on each attractor is, approximately, constant. We now explain this apparent contradiction to our early definition of heteroclinic cycles.

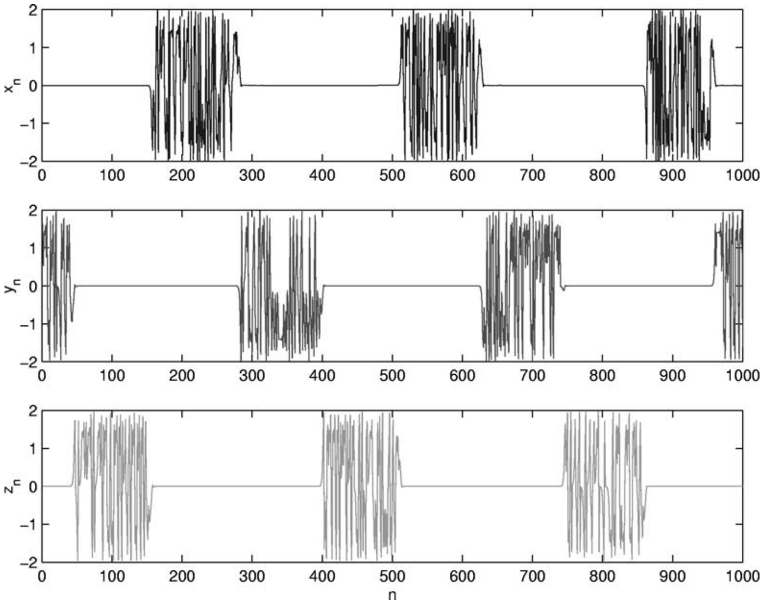

Fig. 2. Cycling chaos in a network of three near-identical discrete cells. The internal dynamics of each cell is governed by the cubic map $f(x,\lambda) = \lambda x - x^3$. A single trajectory cycles around three different chaotic attractors.

The fact that the internal parameters λ_1, λ_2, and λ_3, are all distinct can be considered as a symmetry-breaking perturbation of the global $\mathbf{Z}_3$-symmetry of the network, and of the saddle-sink connections that make up the heteroclinic cycles. Recall also that saddle-sink connections are structurally stable. Thus, a perturbation might destroy certain connections, and consequently the exponential increase in the time that a nearby trajectory spends around each attractor, but the overall cycling behavior would persist in the form of intermittency.

We now turn to the actual application of cycling chaos to cryptography. We use a similar encryption mechanism to the one used by Baptista, where each character is encrypted based on the number of iterations necessary to reach a portion of the attractor associated with that particular character. However, we now use a cycling chaos orbit of (6) to periodically switch the bifurcation parameter key λ, and consequently, the chaotic attractor and alphabet partition, which also play the role of cryptographic keys. On each attractor, we form individual partitions of the alphabet as follows. We denote by $[X_{i_{\min}}, X_{i_{\max}}]$ the portion of attractor i to be used for an individual alphabet partition. Similarly, we use S_i to denote the number of partition units or alphabet units associated with attractor i, and $\epsilon_i = (X_{i_{\max}} - X_{i_{\min}})/S_i$ to denote the size of each partition unit. It follows that $(X_{i_{\min}} + (S_i - 1)\epsilon_i, X_{i_{\min}} + S_i\epsilon_i)$ defines the range of each chaotic attractor that is used to form each alphabet. A discussion of the advantages of this approach is postponed for the closing remarks of this Letter.

Denote by $p = (p_1, \ldots, p_M)$ the plaintext or message to be encoded. Following Baptista's work, to encrypt the first character of the plaintext, p_1, we start with an initial condition $X_0 = (x_0, y_0, z_0)$, and iterate (6) until the dynamics of either one of the three cells in $F^{n_1}(X_0, \Lambda)$ falls within the alphabet unit associated with p_1, where F^{n_1} denotes the n_1-iterate of (6). Since at any given time only one cell is active, while the others are quiescent, there is no conflict of which cell to choose. The ciphertext of p_1 is then n_1. To encode the next character, p_2, we set $X_0' = F^{n_1}(X_0, \Lambda)$ and iterate again until $F^{n_2}(X_0', \Lambda)$ falls within the alphabet unit associated with p_2. The ciphertext of p_2 is then n_2. This process is repeated until the last character, p_M, is encrypted. At the end, the ciphertext is composed by the sequence $\{n_1, \ldots, n_M\}$. For instance, using $S_i = 256$ alphabet units, $X_{i_{\min}} = 0$, $X_{i_{\max}} = 2$, transient time $N_0 = 250$, and the coupled cell system (6) with $\Lambda = (3.0, 2.98, 2.87)$, the plaintext "hello san diego" gets encoded (including spaces) as is shown below:

$$\begin{aligned}&\text{hello san diego}\\&\quad= (204, 69, 41, 160, 126, 404, 215, 34,\\&\qquad 117, 531, 57, 186, 95, 45, 154).\end{aligned}$$

The transient time N_0 is the number of pre-iterations before we start testing whether the iterations fall or not within a particular alphabet interval. As in [1], variations of the basic encryption method with additional parameters can also be readily implemented with the cycling chaos method. For instance, a random number κ and a threshold value η so that the ciphertext n_k is accepted only if $\kappa > \eta$, can also be used as a one-to-many encryption function. Thus guaranteeing that the resulting ciphertext is not unique—even if a plaintext, or portions of it, are repeated. Under this scheme, and with $\eta = 0.7$, our previous plaintext can be encrypted as follows (only two different ciphertexts are shown for brevity)

$$\begin{aligned}&\text{hello san diego}\\&\quad= (786, 2135, 598, 120, 84, 443, 626, 1122,\\&\qquad 135, 80, 37, 171, 361, 85, 349),\\&\text{hello san diego}\\&\quad= (745, 984, 984, 923, 174, 356, 763, 520,\\&\qquad 600, 452, 560, 1095, 64, 1243, 209).\end{aligned}$$

Similar ergodicity principles to those invoked in Baptista's work, which guarantee that each of the ϵ-intervals is visited many times, also apply to our implementation with cycling chaos. Recall now that using distinct internal parameters λ_i in (6) is considered a symmetry-breaking perturbation of the global $\mathbf{Z}_3$-symmetry of the network. This in turn, leads to intermittent cycling behavior instead of ciphertexts cycles. That is, a typical orbit spends, approximately, similar amounts of time around each chaotic attractor. It follows that the natural invariant measure of the cycling chaos attractors is, approximately, a scaled version of the measure of each individual attractor. In the particular case where the internal dynamics of each cell in (6) is governed by the cubic map (4), the natural measure of the chaotic attractors generated with $\Lambda = (3.0, 2.98, 2.87)$ exhibit a flat profile (not shown for brevity) similar to that of the logistic map. Consequently, each of the ϵ_i intervals in our approach is also visited many times and with almost constant frequency.

In summary, we have presented a modified approach of encryption through cycling chaos, in which individual characters are encrypted based on Baptista's method. Our approach incorporates, however, a periodical switching of the bifurcation parameter keys that control the type of attractor that is used to form a partition of the alphabet. The main advantage of our approach is to enhance the security of the encryption process via a periodic switching of keys—chaotic attractors in our case. An intruder who might attempt to break the code by reconstructing the dynamics, now faces the extra challenge of having to reconstruct more than one attractor. If the attractors are not symmetrically related, then this task becomes even more complicated. To a potential intruder, an intercepted signal produced by the cycling chaos method would appear to have similar characteristics as if it was generated by a single chaotic attractor. Thus, not knowing how many chaotic attractors are part of the encryption scheme will add an extra level of security. In this way, cycling chaos can be used to mask the existence of more than one chaotic signal under one single orbit.

Although the results presented in this Letter were obtained with a network of three cells, cycling chaos in bigger networks is also possible. The interconnection scheme with similar coupling function $h(x_i, x_j) = -\gamma \|x_j\| x_i$, however, should include an all-to-all coupling between those cells that are not nearest neighbors (see Fig. 3). Otherwise, more than one cell might become active simultaneously. A disadvantage of the cycling chaos approach is the fact that the switching of attractors can potentially increase the encryption time of each character. We do not attempt to quantify such delay in this Letter.

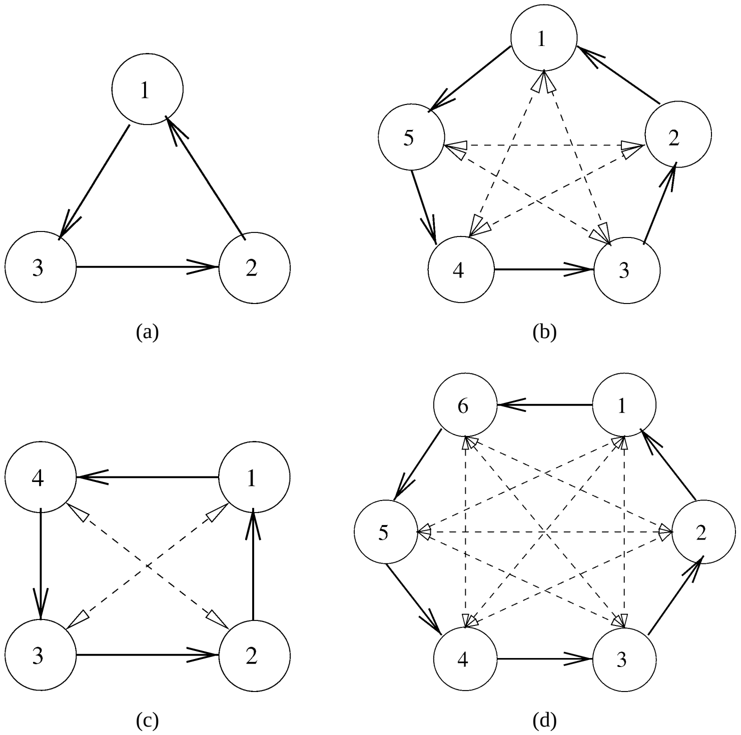

Fig. 3. Interconnection scheme that supports cycling chaos. Nearest neighbors are connected in a directed ring fashion, while all remaining cells are connected in an all-to-all fashion. All couplings are identical.

Acknowledgements

I would like to thank Marty Golubitsky and Ian Melbourne for many stimulating conversations.

References

[1] M.S. Baptista, Phys. Lett. A (1998) 50.

[2] L. Pecora, T.L. Caroll, Phys. Rev. Lett. 64 (1990) 821.

[3] E. Ott, C. Greboggi, J.A. Yorke, Phys. Rev. Lett. 64 (1990) 1196.

[4] T. Shinbrot, E. Ott, C. Greboggi, J.A. Yorke, Phys. Rev. Lett. 65 (26) (1990) 3215.

[5] S. Hayes, C. Grebogi, E. Ott, A. Mark, Phys. Rev. Lett. 73 (1994) 1781.

[6] J. Schweizer, M.P. Kennedy, Phys. Rev. E 52 (1995) 4865.

[7] D. Gligoroski, D. Dimovski, L. Kocarev, V. Urumov, L.O. Chua, Int. J. Bifurc. Chaos 6 (1996) 2119.

[8] L. Kocarev, G. Jakimoski, Phys. Lett. A 289 (2001) 199.

[9] G. Jakimoski, L. Kocarev, Phys. Lett. A 291 (2001) 381.

[10] M. Dellnitz, M. Field, M. Golubitsky, J. Ma, A. Hohmann, Int. J. Bifurc. Chaos 5 (4) (1995) 1243.

[11] A. Palacios, Int. J. Bifurc. Chaos 12 (8) (2002), in press.

[12] A. Palacios, Int. J. Diff. Eq. Appl. (2002), in press.

[13] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Appl. Cryptography, CRC Press, New York, 1996.

[14] P.L. Buono, M. Golubitsky, A. Palacios, Physica D 143 (2000) 74.

[15] M.J. Field, Trans. Am. Math. Soc. 259 (1) (1980) 185.

[16] A. Palacios, P. Longhini, Int. J. Bifurc. Chaos 12 (8) (2002), in press.

[17] B. Dionne, M. Golubitsky, I. Stewart, Nonlinearity 9 (1996) 559.

[18] R.M. May, Nature 261 (1976) 459.

[19] P. Chossat, M. Golubitsky, SIAM J. Math. Anal. 19 (6) (1988) 1259.

[20] T. Rogers, D.C. Whitley, Math. Modelling 4 (1983) 9.