Extraction of Signals from Chaotic Laser Data

John B. Geddes, Kevin M. Short, and Kelly Black
Department of Mathematics, University of New Hampshire, Durham, New Hampshire 03824
(Received 7 June 1999)

Several experimental groups have demonstrated communication with chaotic lasers. We analyze data collected from a message-modulated erbium-doped fiber-ring laser (provided by VanWiggeren and Roy). We show that the transmitted signal is dominated by convolution of the message with the response function of the laser. A simple model based on the topology of the laser allows us to recover a hidden message. While prior estimates indicate that the laser dynamics are high dimensional, we show that only four parameters are required, each of which can be recovered from the transmitted signal alone.

PACS numbers: 05.45.Vx, 05.45.Tp, 42.55.–f, 89.70.+c

A great deal of interest has been generated by the potential to use lasers running in a chaotic regime as the carriers of information in a secure chaotic communication scheme. Several researchers have been working to develop laser transmitter and receiver pairs which synchronize [1–4]. These systems may represent a significant breakthrough for chaotic communication schemes, since they can provide for data transfer rates that are greater than 100 Mbits/sec.

One such laser system was developed by VanWiggeren and Roy [2–4], using an erbium-doped fiber-ring laser (EDFRL). The authors were able to generate a high-dimensional chaotic waveform by message modulating the laser. They also introduced an additional delay loop in the hope of enhancing the privacy of the transmission. Message recovery was achieved by using an appropriately tuned open-loop receiver.

This experiment is novel in two important aspects—the communication rate (100 Mbits/sec) is high and the dynamics appear to be high dimensional (>10) [3]. Previous attempts at secure chaotic communication have been shown to be susceptible to attacks based on nonlinear dynamic (NLD) forecasting [5–8] and return map analysis [9]. However, it has been suggested [10] that transmitting a higher-dimensional waveform may make this difficult, and we will show that an entirely new approach was required in order to extract the message in this case.

In this paper, we report on our investigation of the dynamics and security features of the EDFRL. In order to evaluate the security of the EDFRL, VanWiggeren and Roy provided us with a number of experimental data sets. The application of NLD forecasting was ineffective on this data possibly because subsequent research showed that the signal does not appear to be chaotic on the time scale of the message. Indeed, we will demonstrate that the transmitted signal is dominated by a convolution of the message bit stream with the response function of the laser. This response function is determined by the topology of the laser, i.e., the delay loops and amplification factors. We further show that these parameters are recoverable from the transmitted signal alone, and that first-order estimates of these parameters provide for excellent message recovery.

Underlying model.—Our underlying model assumes that the message-modulated EDFRL can effectively be described in terms of a double echo-feedback loop (see Fig. 1). The transmitter consists of an inner loop with round-trip time T_1, and an outer loop with round-trip time T_2. The inner and outer loops are shared for part of the time. There are erbium-doped fiber amplifiers (EDFA1 and EDFA2) in both the shared inner loop and outer loop. These partly make up for the losses imposed by absorption and loop junctions. We assume that the amplifiers are *linear* and that α and β represent the net effects of amplification and attenuation in the inner and outer loops, respectively. We will ignore any underlying carrier, and focus on the linear response of the laser to the message bit stream. We assume that the transmitted intensity, $I_t(t)$, is dominated by a convolution of the message bit stream $I_m(t)$ with the response function of the laser, $H(t)$.

Consider the evolution of a unit impulse which begins to circulate the laser at $t = 0$. After amplification by EDFA1, this solitary "bit" splits at loop junction A. The inner-loop pulse continues to propagate, while the outer loop pulse is reamplified by EDFA2 before rejoining the inner loop (at loop junction B) as an "echo" of the original pulse. Since the transmitter is a closed-loop system, these pulses are continuously reamplified and resplit, thereby generating multiple echoes of the original pulse. In this way, the effect of a single bit persists for many round-trips; this is analogous to feedback between a microphone and an amplifier in an echo chamber. It is the topology of the laser that dictates the form of the response function.

After one round-trip, a single pulse generated at $t = 0$ will produce two first generation echoes, the first at T_1 with amplitude α, and the second at T_2 with amplitude β. After another round-trip, the former echo will produce second-generation echoes at $2T_1$ with amplitude α^2, and at $T_1 + T_2$ with amplitude $\alpha\beta$. The latter echo will likewise split and produce second-generation echoes at $T_1 + T_2$ with amplitude $\alpha\beta$, and at $2T_2$ with amplitude β^2. The pulses at each subsequent generation will again

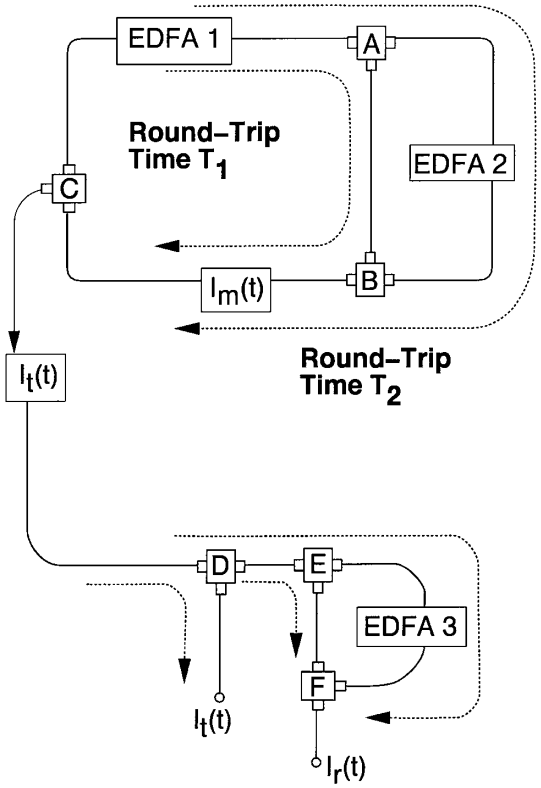

FIG. 1. Schematic of the transmitter and receiver. The message bit stream $I_m(t)$ is sent through the delay loops of the transmitter to produce the transmitted signal $I_t(t)$. The receiver signal $I_r(t)$ is generated by passing the transmitted signal through a receiver. Proper delay times and amplification factors allow recovery of the message.

be split into two, forming a binary tree. The response function, $H(t)$, of the laser can therefore be written as a sum of discrete delta functions

$$H(t) = \sum_{n=0}^{\infty} \sum_{m=0}^{n} \binom{n}{m} \alpha^m \beta^{n-m} \delta[t - mT_1 - (n - m)T_2] \tag{1}$$

while the transmitted intensity is simply the convolution $I_t(t) = H(t) * I_m(t)$,

$$I_t(t) = \left(\sum_{n=0}^{\infty} (\alpha S_{T_1} + \beta S_{T_2})^n \right) I_m(t), \tag{2}$$

where S_{T_1} and S_{T_2} are left-shift operators, i.e., $S_{T_1} I_m(t) = I_m(t - T_1)$ and $S_{T_2} I_m(t) = I_m(t - T_2)$.

Any communication scheme requires a receiver that can effectively decode the transmitted signal. If the transmitter and receiver are synchronized, then the message can be recovered by simply dividing the transmitted signal $I_t(t)$ by the receiver signal $I_r(t)$. This is the algorithm adopted by VanWiggeren and Roy in their experiments. In this case, however, it is more appropriate to consider whether we can invert the convolution produced by the transmitting laser. For convenience, define $A = (\alpha S_{T_1} + \beta S_{T_2})$. Then the convolution can be expanded as $I_t(t) = (I + A + A^2 + A^3 + \cdots) I_m(t)$. Assuming that the response is bounded, i.e., $\alpha + \beta < 1$, this convolution is exactly invertible and the message may be recovered via $I_m(t) = (I - A) I_t(t)$, or

$$I_m(t) = I_t(t) - [\alpha I_t(t - T_1) + \beta I_t(t - T_2)]. \tag{3}$$

This can be accomplished by passing the transmitted signal through an open-loop (i.e., no feedback) receiver with appropriate delays and attenuation factors in order to generate a receiver signal $I_r(t)$ (see Fig. 1). These parameters must be chosen to match that of the transmitting laser. The message is then obtained by simple subtraction, $I_m(t) = I_t(t) - I_r(t)$. Although this is not the method used by VanWiggeren and Roy, it is closely related. We have used this inversion method to decode their transmitted signal and found excellent results.

Although message security has not been a primary concern, estimates of the dimensionality of the laser dynamics have been made. The analysis in [3] suggests a dimension of 10 or greater. As indicated earlier, it is suspected that this may foil eavesdropping attacks based on nonlinear dynamic forecasting. Assuming, however, that our model is valid, then only four parameters are required at most to deconvolve the message from the transmitted signal—α, β, T_1, and T_2.

Testing the model.—To test our underlying model we first adopted what may be termed as a "plain-text" attack. VanWiggeren and Roy provided us with both a transmitted signal and a receiver signal. We recovered the message, consisting of a pseudorandom return-to-zero bit stream, by division of these two data sets. The data sets were 1 ms in duration, and were sampled at 1 ns intervals. Only three decimal-digits of precision were available. For reference, a section of the transmitted signal, the receiver signal, and the recovered message are shown in Figs. 2A, 2B, and 2C.

Having access to both the "message" and the transmitted signal allowed us to test our model. Using the recovered message as a proxy for the original bit stream, we deconvolved it with a short section (65 536 points beginning at 0.9 ms) of the transmitted signal in order to estimate the response function of the laser. This section was chosen arbitrarily. The result is shown in Fig. 2D. As expected, the response function is dominated by discrete peaks. The first two peaks are approximately at 215 and 383 ns, respectively. According to our model, the others should lie at 430, 598, 645, 766 ns, and so forth. Close inspection reveals that this is indeed the case, and that the amplitude sequence is as predicted by our model. Although there is some low-level "noise" present, which may correspond to a weakly chaotic carrier, we were able to ignore this completely and still fully recover the message bit stream.

Using this approximate response function, we deconvolved the transmitted signal in various sections of the time series, and in a number of different ways: (i) We used the entire response function (including the noise). (ii) We used only values above a certain threshold. (iii) We used response values at the predicted echo times

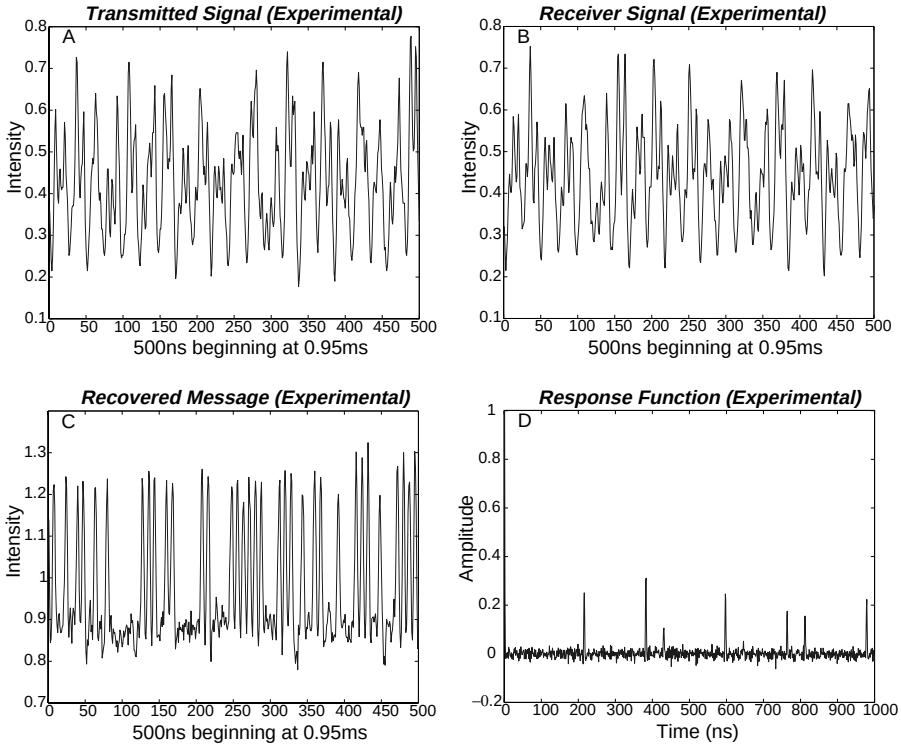

FIG. 2. (A) Transmitted signal. (B) Receiver signal. (C) Recovered message. (D) 1000 ns of the response function recovered by deconvolving the transmitted signal with the recovered message.

only. (iv) We retained short windows centered on the echo times as a means of simulating any dispersion effects. In each and every case, we were able to recover the message *throughout the entire data set* with only very rare bit errors. This is remarkable when we consider that only a short section of the data was required (to estimate the response function) and that the experimentally recovered message is only an approximation to the original bit stream.

Figure 3 demonstrates the validity of our model. Figure 3A shows 500 ns of the message recovered from the experiment. Figure 3B shows our recovered message, obtained by using the response function (after thresholding) on a temporally distant section of the data. Although by no means perfect, the bits are easily identified, and the waveform agrees well with that in Fig. 3A. Figure 3C was obtained using response values at the predicted echo times only. Once more, the bits are easily identified. The agreement with the recovered message in Fig. 3A is surprising when we recall that only a short section of data at 0.9 ms has been used to recover a message at 0.45 ms. This suggests that our model is not only valid, but provides an accurate description of the message-modulated EDFRL.

Parameter estimation.—The previous tests indicate that our linear double echo-feedback loop model of the EDFRL is sufficient to deconvolve a hidden message from a transmitted signal. The only requirements are that we obtain the four laser parameters—α, β, T_1, and T_2. In the absence of a plain-text attack, we are restricted to examining the transmitted signal only. Fortunately, the signal is so heavily dominated by the pulse echoes that any echo-detection algorithm is likely to succeed. We

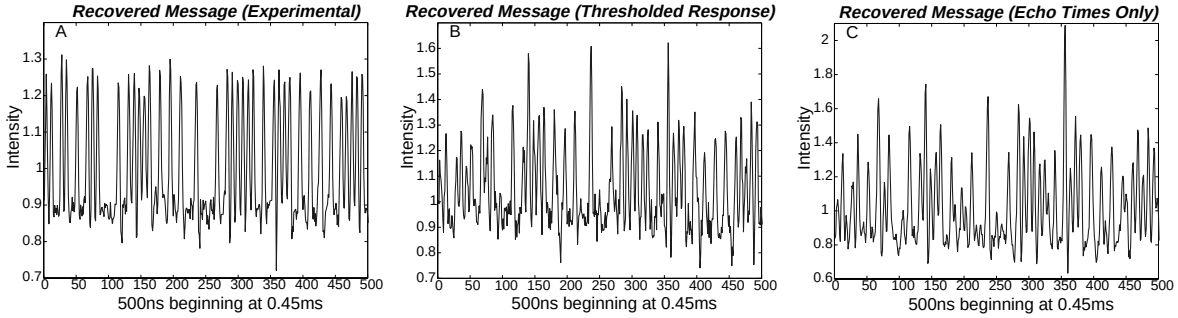

FIG. 3. (A) 500 ns of the recovered message at 0.45 ms (experimental). (B) The recovered message found using the response function after thresholding. (C) The recovered message found using the response function at the echo times only.

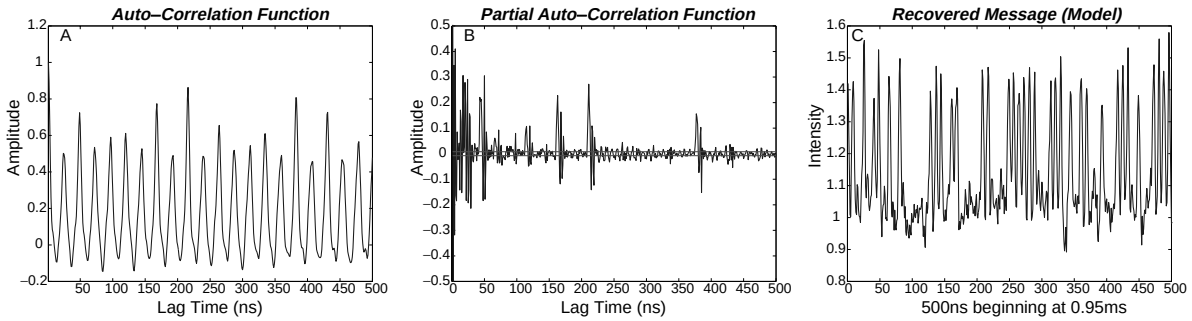

FIG. 4. (A) Autocorrelation function estimate found using 65 536 points of the transmitted signal. (B) Partial-autocorrelation function estimate found using the same 65 536 points of the transmitted signal. (C) The recovered message found using our model with first-order parameter estimates gathered from the PACF.

chose to use the partial-autocorrelation function (PACF) in conjunction with the autocorrelation function (ACF) as a means of estimating the laser parameters. Using these rough estimates we were able to recover successfully the hidden message throughout the entire data set.

In Figs. 4A and 4B, we show the ACF and PACF estimates, along with 95% confidence bounds, found using only 65 536 points of the transmitted signal and a maximum lag of 500 ns. Because of the echoes, the signal is strongly autocorrelated and the ACF is periodic. The PACF removes these "false" periods and allows a fairer estimate of the actual correlation times. Because of the arbitrariness of $t = 0$, first-generation echoes at 215 and 383 ns can appear as correlations at $168 = (383-215)$ ns, $48 = (215-168)$ ns, and so forth. Finding the actual echo times requires both the ACF and PACF functions as the bits are of finite width. As a result, the leading edge of a single bit is correlated with its own trailing edge, and this leads to a spreading of the PACF about each discrete echo. Comparing the peaks in the PACF and the ACF however, allows us to determine the echo times to within 1 ns. In this case a crude estimate of $T_1 \approx 215$ ns, $\alpha \approx 0.22$, $T_2 \approx 383$ ns, and $\beta \approx 0.29$ is good enough for clear message recovery. In Fig. 4C we show our recovered message obtained using the parameter values listed above. The recovery is again remarkable considering that these are first-order parameter estimates.

Conclusions.—We have demonstrated that a message-modulated erbium-doped fiber-ring laser can be modeled as a simple double echo-feedback loop. This allows us to deconvolve a hidden message from a transmitted signal, assuming that the laser parameters, α, β, T_1, and T_2, are known. An echo-detection attack on the transmitted signal reveals first-order estimates of the laser parameters, allowing excellent message recovery.

The laser communication scheme suffers from a fundamental weakness—any chaos which may be present seems to be too slow to affect our method of message recovery. While the laser echo chamber effectively wraps the message into a "high-dimensional" space, this can be inverted once the laser parameters are recovered from the transmitted signal. This raises questions about other high-dimensional chaotic lasers of similar design. Perhaps the dynamics can be unfolded onto a low-dimensional space by removing the echoes. In any case, it seems unlikely that any message security can be provided using the current configuration. We hope that future experiments will address this issue.

This work was supported, in part, by a research grant through the Center for Research on Applied Signal Processing at the University of Southern California, Subcontract No. 012132, and by NSF Grant No. DMS-9704911.

[1] J. P. Goedgebuer, L. Larger, and H. Porte, Phys. Rev. Lett. **80**, 2249 (1998).
[2] G. D. VanWiggeren and R. Roy, Science **279**, 1198 (1998).
[3] G. D. VanWiggeren and R. Roy, Phys. Rev. Lett. **81**, 3547 (1998).
[4] G. D. VanWiggeren and R. Roy, Int. J. Bifurcation Chaos Appl. Sci. Eng. (to be published).
[5] K. Short, Int. J. Bifurcation Chaos Appl. Sci. Eng. **4**, 957 (1994).
[6] K. Short, Int. J. Bifurcation Chaos Appl. Sci. Eng. **6**, 367 (1996).
[7] K. Short, Int. J. Bifurcation Chaos Appl. Sci. Eng. **7**, 1579 (1997).
[8] K. M. Short and A. T. Parker, Phys. Rev. E **58**, 1159 (1998).
[9] G. Perez and H. A. Cerdeira, Phys. Rev. Lett. **74**, 1970 (1995).
[10] M. Ding *et al.*, Chaos **7**, 1054 (1997).