Eavesdropping in chaotic optical communication using the feedback length of an external-cavity laser as a key

Qingchun Zhao, Yuncai Wang,* and Anbang Wang

Department of Physics, College of Science, Taiyuan University of Technology, Taiyuan 030024, China

*Corresponding author: wangyc@tyut.edu.cn

Received 2 February 2009; revised 7 May 2009; accepted 29 May 2009; posted 4 June 2009 (Doc. ID 107038); published 15 June 2009

An external-cavity laser (ECL) operating in a chaotic state is usually used in a chaotic optical secure communication system and its feedback length (FL) is often regarded as an additional key. Our analyses show that an eavesdropper’s (Eve) laser can synchronize with a transmitter (Alice) without any knowledge of the FL by simply increasing the injection strength. A sequence of a 1 Gbit/s nonreturn-to-zero message encoded by the FL as the key is successfully eavesdropped. The reason for the synchronization deviation between Alice’s and Eve’s lasers is given. Our results indicate that the FL as a key cannot enhance the security of chaotic optical communication using long-ECLs. © 2009 Optical Society of America

OCIS codes: 140.5960, 140.1540, 060.4510.

1. Introduction

With the development of modern communication networks, the demand of security for communication services has been growing rapidly. Public key encryption algorithms are widely used in modern cryptography and some novel encryption schemes were proposed [1,2]. Among these schemes, chaotic communication has drawn intensive attention because it is a physical layer (hardware) encryption scheme and it can be compatible with current public key (software) encryption and quantum cryptography [3].

Chaotic communication based on chaotic synchronization was first achieved by circuits [1] and then implemented by lasers [4–6]. In this encryption protocol, a message is embedded within a chaotic carrier generated by a transmitter (Alice), and recovered by a receiver (Bob) upon synchronization with Alice. An external-cavity laser (ECL) is widely used as the transmitter and receiver in chaotic optical communication because it can easily generate a chaotic carrier with high dimension and broad bandwidth. It is well known that realization of chaotic synchronization needs the parameters to match between the transmitter and receiver. Hence, the laser parameters (e.g., configuration of laser cavity, central wavelength, threshold current, etc.) are the natural candidates as the key. Unfortunately, these parameters are controlled mainly by the laser manufacturer instead of the client. From the viewpoint of practice, an additional key—an easily adjusted external parameter—is desirable for Alice and Bob if they do not expect the manufacturer to hold the security authority alone. Thereby the feedback length (FL) of an ECL is the preferred element as the additional key to enhance the security of chaotic optical communication systems [7–10]. Sivaprakasam et al. first demonstrated that a message can be successfully transmitted using ECLs [7]. Soriano et al. illustrated that a closed-loop is more secure than an open-loop scheme in all-optical chaos-based communication systems [10]. Recently, Bogris et al. have reported that fast variation of the feedback phase of a short ECL can be used as a key for cryptography [11]. Nevertheless, the feedback phase of a short ECL is difficult to precisely control because of the influence...
of environmental vibration and temperature fluctuation. Reference [12] illustrates that the information of the FL of a chaotic carrier generated by an ECL can be masked in the power spectrum and autocorrelation function under the moderate feedback strength.

In this paper, we examine the effect of the FL of the transmitter on the chaotic synchronization between Alice’s and an eavesdropper’s (Eve) laser. We find that the security of chaotic optical communication cannot be actually enhanced when the FL of an ECL is used as an additional key. A sequence of nonreturn-to-zero (NRZ) messages is successfully extracted by Eve in demonstration.

2. Principle

According to Kerckhoffs’ principle, a cryptosystem should be secure even if everything about the system, except the key, is public knowledge. The cryptography is secure if Eve cannot break the plaintext under this principle. During the following analyses, we assume that Eve knows everything about the parameters of Alice’s laser except the FL according to Kerckhoffs’ principle, i.e., Eve obtains a similar laser, just like Alice’s and Bob’s, from the same manufacturer, but without Alice’s authorization.

Open-loop and closed-loop are two main schemes for chaotic optical communication using ECLs. In the open-loop scheme, Bob recovers the message after transmission by using a solitary laser without an external cavity. Hence, Eve can also break the open-loop communication system using a solitary laser with the same parameters as Bob’s though she has no knowledge of the FL of Alice’s laser. Thus, we concentrate on whether the key of FL can enhance the security of a closed-loop chaotic optical communication system in the following parts.

The dynamical characteristics of lasers are described by the well-known Lang–Kobayashi rate equations [13]:

\[
\begin{align*}
\frac{dE_A(t)}{dt} &= \frac{1}{2}(1 + i\alpha) \left(g[N_A(t) - N_0] - \frac{1}{\tau_p}E_A(t)\right) + k_AE_A(t - \tau_A)\exp(-i\omega_A \tau_A), \\
\frac{dE_E(t)}{dt} &= \frac{1}{2}(1 + i\alpha) \left(g[N_E(t) - N_0] - \frac{1}{\tau_p}E_E(t)\right) + k_EE_E(t - \tau_E)\exp(-i\omega_E \tau_E) + k_{inj}E_A(t - \tau_{inj})\exp(-i\omega_A \tau_{inj}), \\
\frac{dN_{AE}(t)}{dt} &= \frac{I_{AE}(t)}{qV} - \frac{1}{\tau_N}N_{AE}(t) - g[N_{AE}(t) - N_0]E_{AE}(t)^2,
\end{align*}
\]

where \(E\) and \(N\) are the slowly varying complex electronic field amplitude and the carrier density in the laser cavity. The subscripts A and E denote Alice and Eve, respectively. \(\omega\) is the angular frequency of the free-running laser. \(\tau_{AE}\) is the delay time of feedback light in the external cavity. The relationship between the delay time and the FL is \(\tau_{AE} = 2L_{AE}/c\), where \(L_{AE}\) is the FL and \(c\) is the light speed in vacuum. \(I(t)\) is the pump current of the laser. The feedback coefficient \(k_{AE}\) of the ECLs and the injection coefficient \(k_{inj}\) from Alice’s laser to Eve’s are defined as follows:

\[
k_{AE} = \frac{1}{\tau_{in}} \left(\frac{1 - r_0}{r_0}\right)^2 r_{AE},
\]

\[
k_{inj} = \frac{1}{\tau_{in}} \left(\frac{1 - r_0}{r_0}\right)^2 r_{inj},
\]

where the injection rate \(r_{inj}\) represents the percentage of Alice’s laser output electronic field amplitude injected into Eve’s laser cavity. The other parameters and their values used in the simulation are listed in Table 1.

It is feasible for Eve to break the hidden message if Eve’s laser can achieve synchronization with Alice’s. We use the correlation coefficient to quantify the synchronization quality, which is defined as

\[
\rho = \frac{\langle[A(t) - \langle A(t)\rangle][E(t) - \langle E(t)\rangle]\rangle}{\sqrt{\langle[A(t) - \langle A(t)\rangle]^2\rangle}\sqrt{\langle[E(t) - \langle E(t)\rangle]^2\rangle}}}.
\]

where \(A(t)\) and \(E(t)\) are the outputs of Alice’s and Eve’s lasers, respectively, and \(\langle \cdot \rangle\) denotes the time average.

3. Static Key

The scheme for chaotic optical communication and message eavesdropping using the FL as a static key is shown in Fig. 1. The structure and parameters of Bob’s setup are the same as Alice’s to decode the

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>(V)</td>
<td>Volume of the active region</td>
<td>(1.2 \times 10^{-16}) m(^3)</td>
</tr>
<tr>
<td>(\tau_N)</td>
<td>Carrier lifetime</td>
<td>2 ns</td>
</tr>
<tr>
<td>(\tau_p)</td>
<td>Photon lifetime</td>
<td>2 ps</td>
</tr>
<tr>
<td>(\tau_{in})</td>
<td>Round-trip time in the internal laser cavity</td>
<td>10 ps</td>
</tr>
<tr>
<td>(r_0)</td>
<td>Delay time of injected light</td>
<td>1 ns</td>
</tr>
<tr>
<td>(r_{AE})</td>
<td>Reflection rate of the laser facet</td>
<td>(30%)</td>
</tr>
<tr>
<td>(\alpha)</td>
<td>Reflection rate of external mirror</td>
<td>(0.3%)</td>
</tr>
<tr>
<td>(N_{th})</td>
<td>Carrier density at threshold</td>
<td>(2 \times 10^{24}) m(^{-3})</td>
</tr>
<tr>
<td>(N_0)</td>
<td>Carrier density at transparency</td>
<td>(10^{24}) m(^{-3})</td>
</tr>
<tr>
<td>(g)</td>
<td>Gain coefficient</td>
<td>(2 \times 10^{12}) m(^3)/s</td>
</tr>
<tr>
<td>(\alpha)</td>
<td>Linewidth enhancement factor</td>
<td>4.5</td>
</tr>
<tr>
<td>(I_{th})</td>
<td>Threshold current</td>
<td>17.5 mA</td>
</tr>
<tr>
<td>(\lambda)</td>
<td>Wavelength</td>
<td>850 nm</td>
</tr>
<tr>
<td>(q)</td>
<td>Charge quantity</td>
<td>(1.6 \times 10^{-19}) C</td>
</tr>
</tbody>
</table>
hidden message. Eve’s setup consists of an ECL and an erbium-doped fiber amplifier (EDFA). The EDFA is utilized to increase the injection rate to Eve’s laser. Note that the FL of Eve’s laser can vary to break the key of the communication system.

To mask the FL in the chaotic carrier, we set the bias current of Alice’s laser as $I_b = 1.2I_{th}$ and the reflection rate of external mirror as $r_A = 0.3\%$. Figure 2 exhibits the chaotic carrier characteristics when the FL of Alice’s laser is 0.6 m, and the corresponding time delay is 4 ns. As can be seen, the FL and corresponding time delay are perfectly masked.

In the static key case, although Eve has no knowledge of the FL of Alice’s laser, she holds other parameters except the key. Thereby, she may attempt to adjust the FL of her laser to break the key. Figure 3 shows the correlation coefficient between Alice’s and Eve’s lasers for different injection rates when the key is 0.6 m. When Eve scans her FL between 0.1 and 1.5 m, there is a distinct peak at 0.6 m because of the complete symmetry between the two lasers. The correlation coefficient remains above 84% during the whole scanning process. With increasing the injection rate, the correlation coefficient increases steadily no matter what Alice’s FL is. For the high injection rates, this kind of synchronization is the so-called generalized synchronization [14]. From the above analyses, Eve’s laser with a certain FL can maintain chaotic synchronization with Alice’s in the condition of an adequate injection rate provided by the EDFA.

The 1 Gbit/s NRZ message is encoded by chaos shift keying (CSK). Note that the modulation depth for the message encoding is 8%. Figures 4(a) and 4(b) illustrate the time series and the power spectrum of Alice’s laser output after the message is encoded. There is no evidence of a NRZ message from the output. The original NRZ message is shown in the top panel of Fig. 4(c). Bob uses a laser with the same FL (i.e., 0.6 m in this simulation) as Alice’s laser to obtain good recovery of the message, shown in the middle panel. Meanwhile, Eve uses a laser with a variable FL to attempt to break the message. The bottom panel exhibits the extracted message when the FL of Eve’s laser is 0.7 m, and the corresponding correlation coefficient is minimal during the variation of the FL of Eve’s laser. As can be seen, the recovered messages between Bob’s and Eve’s lasers have no distinct difference.

The average mutual information (AMI) [15], a concept of information theory to measure the similarity of two variables, is used to quantitatively evaluate the message eavesdropping results, since the FL variation of Eve’s laser can hardly cause slight change of bit-error rate (BER). The more similar two variables are, the lower the AMI curve is. Figure 4(d) shows three AMI curves for 10 kbits message transmission and eavesdropping using the static key. The AMI curve between the eavesdropped message and original message (real line) is nearly the same as that between Bob’s recovered message and original message (dotted line). The AMI curve between the eavesdropped message and Bob’s recovered message is the lowest one among the three curves, which indicates that the eavesdropping process can always be successful for a long time span.
4. Dynamic Key

Generally speaking, a dynamic key is more secure than a static key in cryptanalysis. Here we consider the case that the FL of Alice’s laser is a dynamic key instead of a static key to enhance the security. The dynamic key is supposed to be two switched fiber feedback rings controlled by an optical switch. The optical switch is used to realize the high speed switch between different fiber feedback rings, because mechanical means cannot obtain the high speed switch of the FL of Alice’s laser. Figure 5 shows the detailed setup for chaotic optical communication and message eavesdropping using the FL as a dynamic key. Eve uses a variable delay line (VDL) to vary the FL of her laser to break the hidden message.

The chaotic communication system takes a certain time to recover the synchronized state when the FL of Alice’s laser varies. This value is of at least several nanoseconds for the closed-loop system [16]. If the switching time of the key is less than the synchronization recovery time, the system security may be enhanced. Here we suppose the key switches between 2 and 4 m, and the switching rate is controlled by the optical switches. Figure 6 shows the correlation coefficient between Alice’s and Eve’s lasers when the switching rate is 1 Gbit/s and the variation step of the VDL is 0.2 m, while the variation span is between 1 and 5 m. One correlation coefficient is obtained for a time span and a certain length of VDL during its variation. There are two distinct peaks at the FLs of Alice’s laser during the whole scanning. These two peaks are the switching key values. Although...
Eve cannot break the switching rate, her laser can still synchronize with Alice’s.

Figure 7 shows the message transmission and eavesdropping using the dynamic key. The 1 Gbit/s NRZ message is encoded by CSK all the same, and the modulation depth is also chosen as 8%. Although the time series of Alice’s laser output is changed compared with the static key case, the power spectrum remains nearly the same as Fig. 4(b). The message can still be masked in chaotic carrier using the dynamic key. Figure 7(c) presents the message recovered by Bob using the authorized key (i.e., the key switches between 2 and 4 m, and the switching rate is 1 Gbit/s) and eavesdropped by Eve using a 1.2 m fiber feedback ring, as shown in the middle and bottom panel, respectively. To indicate the long-time successful eavesdropping, the AMI curves are also plotted in Fig. 7(d). To the 10 kbits message encoded by the dynamic key, the AMI curve between the eavesdropping message and original message (real line) is nearly superposable as that between Bob’s recovered message and the original message (dotted line). This result denotes that Eve can break the message encoded by the dynamic key using a laser with a certain FL fiber feedback ring.

5. Discussion

Compared with Fig. 3, the correlation coefficients in Fig. 6 slightly decline, which is caused by Alice’s switching fiber feedback ring. However, this decline cannot be used to transmit a message securely because Eve’s laser can still synchronize with Alice’s.

The synchronization deviation between Alice’s and Eve’s lasers is induced by the increase of high-frequency intensity of Eve’s laser output. The RF spectra of output powers of Alice’s and Eve’s lasers are shown in Fig. 8. The dashed ellipse part is corresponding to the increase of high-frequency intensity of Eve’s laser after injection. The increased high-frequency intensities result in the synchronization deviation. However, these high-frequency intensities have little effect on message eavesdropping for Eve because they are beyond the bandwidth of the chaotic carrier.

Using a single static FL of ECL as a key in chaotic optical communication is insecure because it can be extracted by Eve. Thereby, using a rapidly switching FL of an ECL as a dynamic key is proposed to enhance the security performance. But according to the above demonstrations, Eve’s laser can also synchronize with Alice’s even though the key is dynamic. Thus, chaotic optical communication using the FL of an ECL as an additional key is debatable for security enhancement since the message eavesdropping at Eve’s side can be achieved easily.

6. Conclusions

In summary, the security of chaotic optical communication using the FL of ECLs as a key is analyzed in detail. By simply increasing the injection strength using an EDFA, Eve’s laser can synchronize with Alice’s no matter if the key is static or dynamic.
The reason for the synchronization deviation between Alice’s and Eve’s lasers is the increase of high-frequency intensity of Eve’s laser. A sequence of 1 Gbit/s NRZ message encoded by the FL as a key is successfully eavesdropped, which means that using the FL of long-ECLs as a key is not suitable to chaotic optical communication. Hence, to find practical and secure keys for chaotic optical communication, such as feedback strength, bias current, or combination of some laser parameters is extremely necessary and essential, which is in progress.

This work is supported by the National Natural Science Foundation of China (NNSFC) under grant 60777041 and the International Cooperation Project of Shanxi Province under grant 2007081019.

References