Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2010, Article ID 361860, 18 pages
doi:10.1155/2010/361860

Research Article

Cryptanalysis of a Chaotic Communication Scheme Using Parameter Observer

Haipeng Peng,[1, 2, 3] Yan Shao,[1, 2, 3] Lixiang Li,[1, 2, 3] and Yixian Yang[1, 2, 3]

[1] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, P.O. Box 145, Beijing 100876, China*
[2] *Key Laboratory of Network and Information Attack and Defence Technology of MOE, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[3] *National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China*

Correspondence should be addressed to Lixiang Li, lixiang@bupt.edu.cn

Received 17 October 2009; Accepted 3 December 2009

Academic Editor: Massimo Scalia

This paper addresses the cryptanalysis of a secure communication scheme proposed by Wu (2006), where the information signal is modulated into a system parameter of a unified chaotic system. It is demonstrated that a parameter observer can be designed to identify the parameter determined by the transmitted information and then the transmitted information can be obtained. Compared with the existing analysis using adaptive observer, the cryptanalysis based on parameter observer is much simpler and needs less structure information of the transmitter system. With numerical simulations, it is shown that the parameter observer has stronger practicality and robustness. Furthermore, it is still possible to obtain the transmitted information, even if the derivative of the transmitted signal is unknown.

1. Introduction

Over the past two decades, increasing attentions are drawn on utilizing chaos theory on secure communication based on synchronization technique [1–4]. At the meantime, cryptanalysis of chaotic secure communication scheme is proposed with different methods [5, 6]. Recently, a new secure cryptosystem based on adaptive synchronization has been proposed by Wu [7]. In this paper, we carry out a security analysis of the cryptosystem on the concept of parameter identification. It is demonstrated that a parameter observer can be designed to identify the parameter and then the information can be obtained. Compared with the existing analysis using adaptive observer, the parameter observer is much simpler and needs less structure information of the transmitter system. With numerical simulations, it is shown that the parameter observer has stronger practicality and robustness.

Wu proposed a new secure communication scheme in [7]. The secure communication scheme utilizes adaptive synchronization of a unified chaotic system. The transmitter is designed as follows:

$$\begin{aligned}\dot{x}_m &= \left(25\beta(t) + a\right)\left(y_m - x_m\right),\\ \dot{y}_m &= \left(b - 35\beta(t)\right)x_m - x_m z_m + \left(29\beta(t) - c\right)y_m,\\ \dot{z}_m &= x_m y_m - \frac{\beta(t) + d}{3} z_m,\end{aligned} \tag{1.1}$$

where the lower scripts m stands for the transmitter system, a, b, c and d are user-specific parameters. The information signal $f(t)$, which satisfies $m \le f(t) \le M$, is modulated into the function as follows:

$$\beta(t) = \frac{f(t) - m}{M - m}. \tag{1.2}$$

It is obvious that $\beta(t)$ varies from 0 to 1 according to $f(t)$. As it was shown in [7], system (1.1) then exhibits chaotic behavior with different chaotic attractors, such as Lorenz, Lü and Chen attractors.

The identical receiver system can be constructed at the receiving end as follows:

$$\begin{aligned}\dot{x}_s &= \left(25\beta_1(t) + a\right)\left(y_s - x_s\right) + u_1,\\ \dot{y}_s &= \left(b - 35\beta_1(t)\right)x_s - x_s z_s + \left(29\beta_1(t) - c\right)y_s + u_2,\\ \dot{z}_s &= x_s y_s - \frac{\beta_1(t) + d}{3} z_s + u_3,\end{aligned} \tag{1.3}$$

where the lower scripts s stands for the receiver system. u_1, u_2 and u_3 are the nonlinear controllers and $\beta_1(t)$ is the estimator for $\beta(t)$ and is updated adaptively. With the assumption that $\dot{\beta}(t)$ or $\dot{f}(t)$ is known, it is proved in [7] by the Lyapunov stability theorem that the receiver is synchronous with the transmitter, and the covered message can be obtained with a reverse transformation of (1.2).

In [6], Liu and Tang addresses a cryptanalysis of the cryptosystem performed with adaptive control theory. To obtain the transmitted information, an adaptive observer with three state observers (x_m, y_m and z_m) and five parameter estimators (a, b, c, d and $\beta(t)$) are designed. Assuming that the dynamical evolution of the information signal is available, it is proved that both state variables and unknown parameters of the adaptive observer will asymptotically converge to their true values, respectively, justified by the Lyapunov stability theory. As the result, the transmitted information can be retrieved.

In this paper, we are interested in performing the cryptanalysis of the same cryptosystem in a simpler way, based on two questions as follows.

Firstly, since it is $\beta(t)$ that we only need to obtain the transmitted information, can we identify $\beta(t)$ without achieving the true values of the user-specific parameters a, b, c and d?

Secondly, if the structure of the system (1.1) is partly available, for instance, only the structure of the third equation is known, is it possible to obtain the transmitted information?

Our answer is positive, and it is demonstrated in the following sections that it can be achieved based on the concept of parameters observer.

The paper is organized as follows. In Section 2, a parameter observer is designed for the cryptanalysis of the secure communication system (1.1) with both theoretical analysis and numerical simulations. In Section 3, a more practical case is considered, for which the derivative of the information signal is kept secret from attackers. Finally, the conclusion of the paper is given in Section 4.

2. Cryptanalysis Using the Parameter Observer

Let us consider the conditions of the secure communication scheme proposed in [7], where system (1.1) with parameters a, b, c, d and $\beta(t)$ being unknown, in this section, we will show that a parameter observer can be designed to retrieve the transmitted information.

2.1. Design of the Parameter Observer

Assuming all the state variables in system (1.1) and the dynamical evolution of the information signal are available, let

$$g(t) = \frac{\beta(t) + d}{3}, \tag{2.1}$$

and the third equation of (1.1) can be written as follows:

$$g(t) z_m = x_m y_m - \dot{z}_m. \tag{2.2}$$

A parameter observer is proposed as follows:

$$\frac{d\widehat{g}(t)}{dt} = \dot{g}(t) - z_m l(z_m) \widehat{g}(t) + l(z_m)\left(x_m y_m - \dot{z}_m\right), \tag{2.3}$$

where $\widehat{g}(t)$ is the estimators for $g(t)$, and $l(z_m)$ is a designed gain function. Let

$$e_g(t) = g(t) - \widehat{g}(t), \tag{2.4}$$

then

$$\dot{e}_g(t) = \dot{g}(t) - \frac{d\widehat{g}(t)}{dt} = -z_m l(z_m) e_g(t). \tag{2.5}$$

$l(z_m)$ is the chosen function verifying that the system

$$\dot{e}_g(t) + z_m l(z_m) e_g(t) = 0 \tag{2.6}$$

is exponentially stable. Then $\widehat{g}(t)$ will exponentially converge to $g(t)$ when $t \to \infty$. A possible choice for $l(z_m)$ is k/z_m, then system (2.6) can be written as follows:

$$\dot{e}_g(t) + k e_g(t) = 0, \tag{2.7}$$

where $k > 0$ determines the converging speed.

However, it is not practical to get the information of $\dot{z}_m$, which makes observer (2.3) practically useless. To overcome the defect, we define an instrumental variable as follows:

$$\delta = \widehat{g}(t) + p(z_m), \tag{2.8}$$

where $p(z_m)$ is a designed function verifying

$$l(z_m) = \frac{dp(z_m)}{dz_m}. \tag{2.9}$$

We can obtain

$$\dot{\delta} = \frac{d\widehat{g}(t)}{dt} + \frac{dp(z_m)}{dz_m}\dot{z}_m = \dot{g}(t) - z_m l(z_m)\left(\delta - p(z_m)\right) + l(z_m) x_m z_m, \tag{2.10}$$

that is,

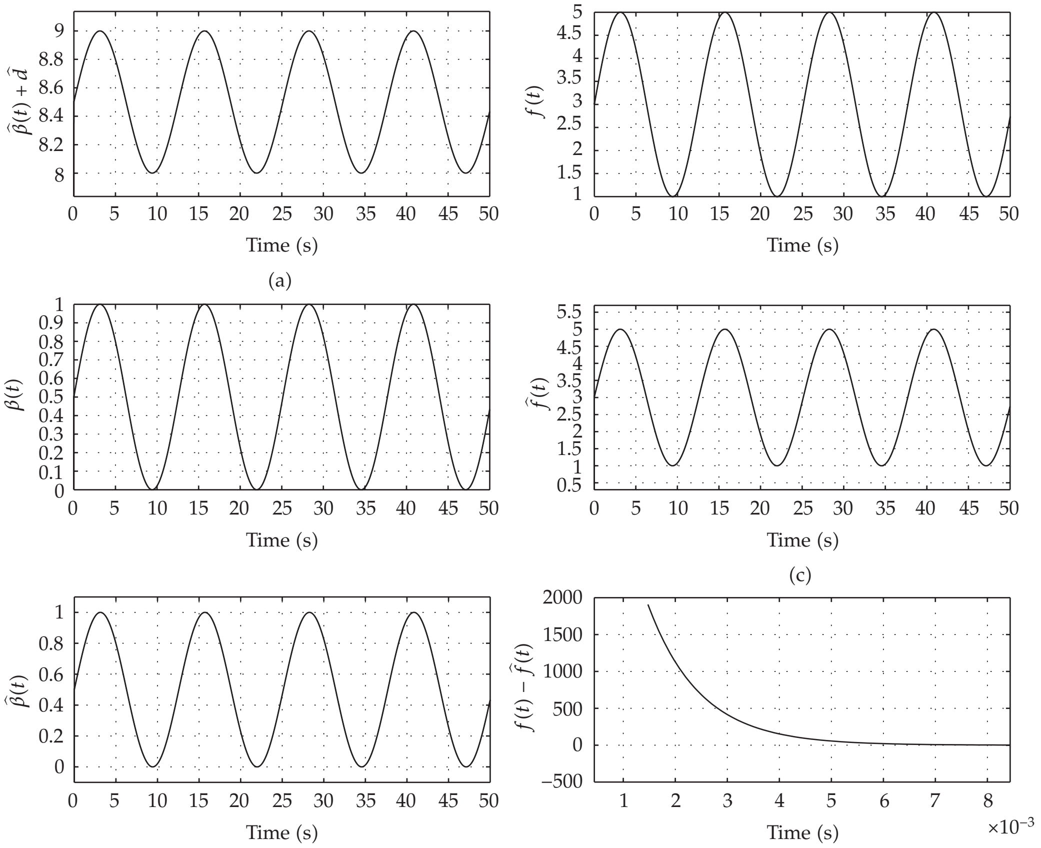
$$\begin{gathered} \dot{\delta} = \dot{g}(t) - z_m l(z_m)\delta + l(z_m)\left(z_m p(z_m) + x_m y_m\right), \\ \widehat{g}(t) = \delta - p(z_m). \end{gathered} \tag{2.11}$$

Obviously, choose function $p(z_m)$ such that

$$\dot{e}_g(t) + \frac{dp(z_m)}{dz_m} e_g z_m = 0 \tag{2.12}$$

is exponentially stable, then $\widehat{g}(t)$ will exponentially converge to $g(t)$.

Summing up the above analysis, we have the following parameter observer.



(a)

(c)

(b)

(d)

Figure 1: Simulation results with Case 1 of Section 2: $f(t) = 3 + 2\sin(0.5t)$.

Result 1. With known $\dot{\beta}(t)$, we can obtain $\dot{g}(t) = \dot{\beta}(t)/3$. The parameter observer of $g(t)$ is designed as follows:

$$\begin{gathered}\dot{\delta} = \dot{g}(t) - z_m l(z_m)\delta + l(z_m)\left(z_m p(z_m) + x_m y_m\right), \\ \widehat{g}(t) = \delta - p(z_m),\end{gathered} \tag{2.13}$$

where $p(z_m)$ is a designed function verifying $dp(z_m)/dz_m = l(z_m)$ and $l(z_m)$ determines the converging speed.

Based on (1.2) and (2.1), we get

$$\widehat{\beta}(t) = 3\widehat{g}(t) - \widehat{d}, \tag{2.14}$$

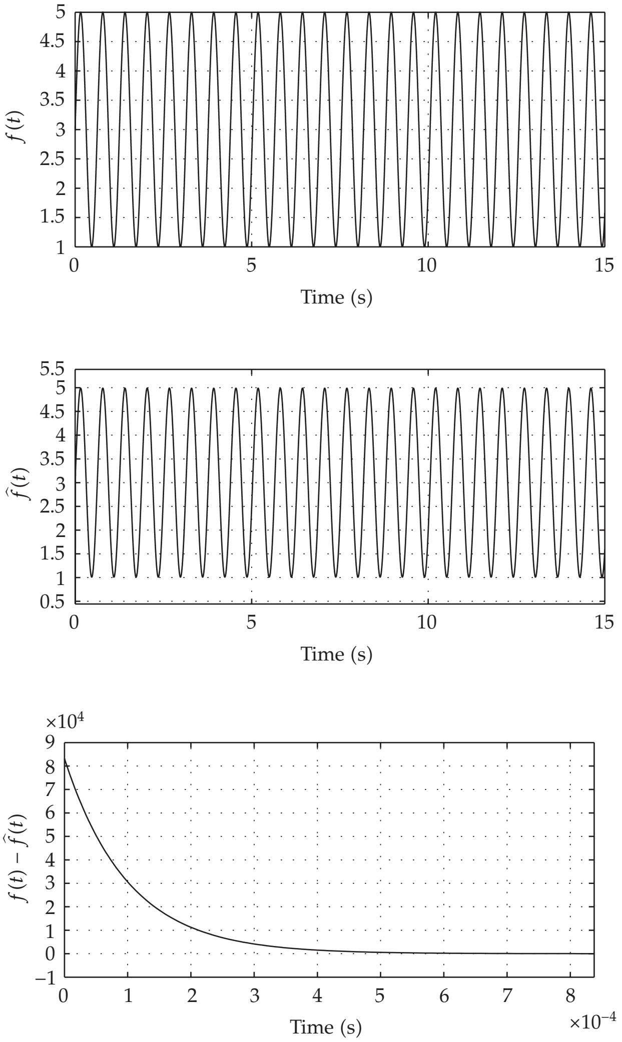


Figure 2: Simulation results with Case 2 of Section 2: $f(t) = 3 + 2\sin(10t)$.

where the minimum and maximum values of $\hat{\beta}(t)$ are 0 and 1, respectively. Note that $\hat{g}(t)$ can be obtained by the observer mentioned before and d is the constant, it is possible to determine $\hat{d}$ by the minimum and maximum values of $\hat{\beta}(t)$. Consequently, $\hat{\beta}(t)$ can be obtained. Then, the information $f(t)$ can be retrieved as follows:

$$\hat{f}(t) = (M - m)\hat{\beta}(t) + m. \tag{2.15}$$

As the result, the scheme proposed in [7] is considered to be insecure.

The parameter observer proposed in this paper gives excellent performances in following aspects.

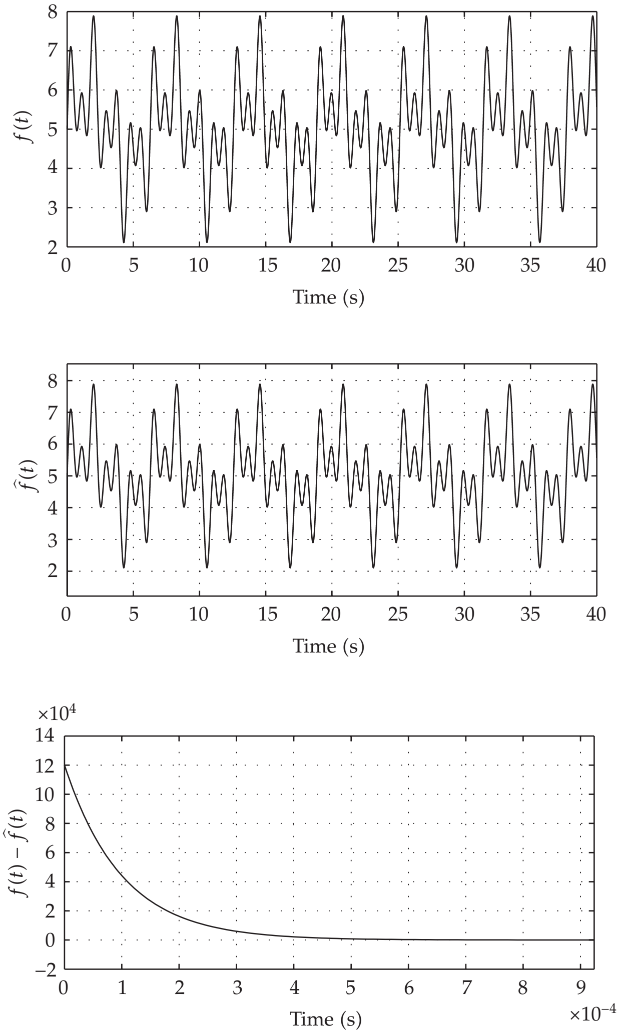


Figure 3: Simulation results with Case 3 of Section 2: $f(t) = 5 + \sin(t) + \sin(4t) + \sin(7t)$.

Firstly, the parameter observer is simple and direct. To retrieve the transmitted information, we only need to construct one observer to identify the true value of $\beta(t)$, which is directly determined by the transmitted information. And it is unnecessary to obtain the true value of the user-specific parameters a, b, c and d. The result answers on the first question in Section 1.

Secondly, the parameter observer is only related to the structure of the third equation in system (1.1), which means it is possible to construct the parameter observer, even if part of the structure information of the transmitter system is unknown. The result answers on the second question in Section 1. Furthermore, for the reason that the parameter observer is designed based on the third equation, any change of parameters or structures in the first and second equations in system (1.1) has no effect on the result of parameter identification.

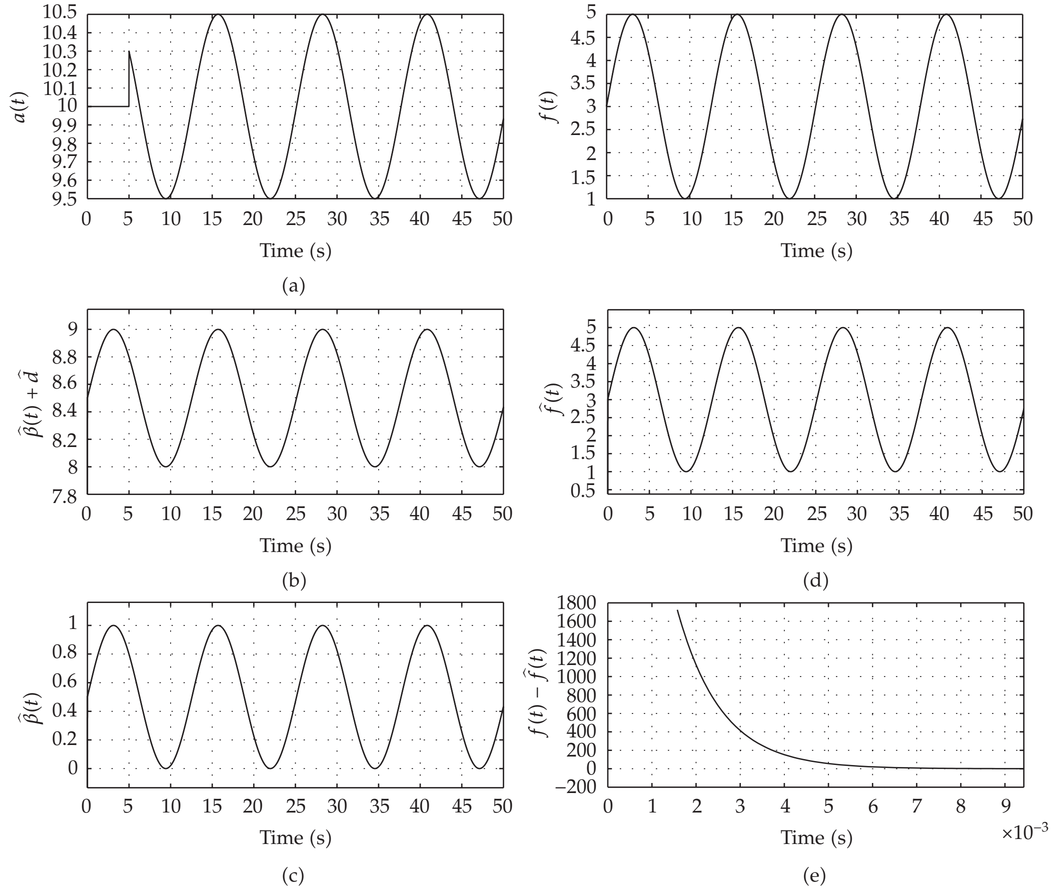


Figure 4: Simulation results with Case 4 of Section 2: $f(t) = 3 + 2\sin(0.5t)$. The parameter a changes during parameter identification.

Thirdly, our cryptanalysis with parameter observer imposes less assumptions than the cryptanalysis proposed in [6], where, in order to obtain the true value of the parameters, persistently excitation or linearly independent condition are need.

As mentioned in the first and second aspects, the questions proposed in Section 1 have been resolved. Moreover, it can be concluded that the parameter observer has stronger practicality and robustness.

2.2. Numerical Simulations with Available $\dot{\beta}(t)$

In the following, several functions of $f(t)$ are tested. At the meantime, a possible case, for which the parameter a changes during the parameter identification process, is also simulated. Furthermore, we also take the influence of the noise on the identification performance into consideration. The parameters and initial states of system (1.1) are set the same as [6]: $a = 10$, $b = 28$, $c = 1$, $d = 8$, $x_m = 1$, $y_m = 1$, $z_m = 2$. For the parameter observer, the initial state is set as: $\delta(0) = 0$. It was shown above that $l(z_m)$ is a designed gain function, which determines the

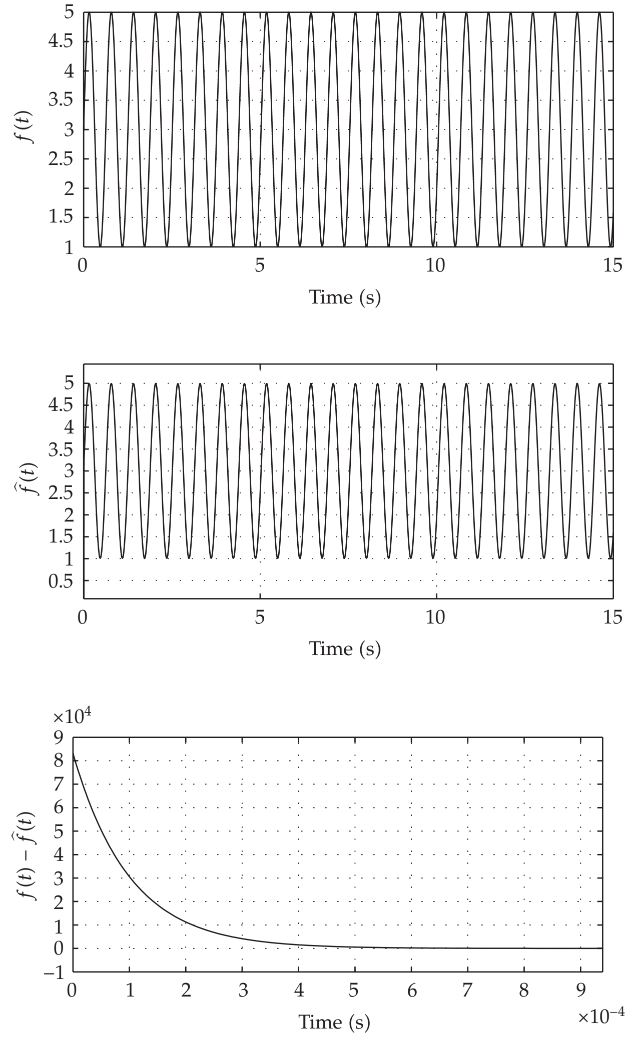


Figure 5: Simulation results with Case 4 of Section 2: $f(t) = 3 + 2\sin(10t)$. The parameter a changes during parameter identification.

converging speed. $l(z_m)$ is set as: $l(z_m) = k/z_m$, where different k is chosen in different cases, according to the frequency of the information signal.

Case 1 ($f(t) = 3 + 2\sin(0.5t)$). For the first case, $M = 5$ and $m = 1$. According to (1.2), $\beta(t) = [1 + \sin(0.5t)]/2$. The simulation results are given in Figure 1 with $k = 1000$. It is shown in Figure 1(a) that $3\hat{g}(t) = \hat{\beta}(t) + \hat{d}$ is obtained and found to be varied in the range of $[8, 9]$. Considering that the minimum and maximum values of $\beta(t)$ are 0 and 1, respectively, it is estimated that $\hat{d} = 8.00$ and $\hat{\beta}(t)$ is shown in Figure 1(b). Figure 1(d) shows the estimation of the absolute error. After the initial transient time of about 7×10^{-3} s, information signal can be recovered with a fluctuation of $|f(t) - \hat{f}(t)| \leq 0.5 \times 10^{-3}$. A faster convergence rate is achieved, compared with the result given in [6].

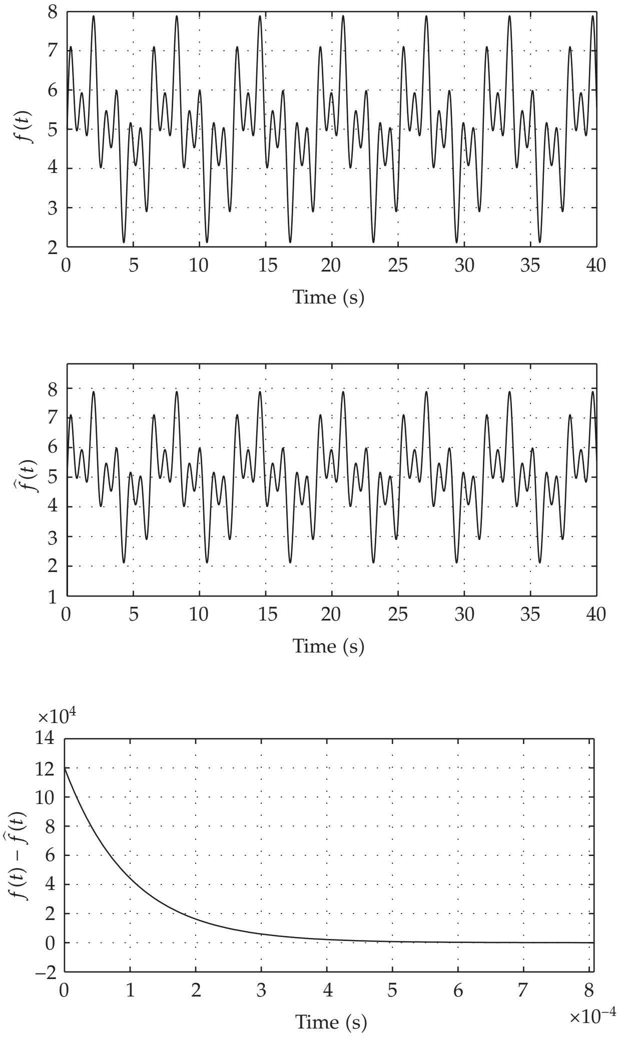


Figure 6: Simulation results with Case 4 of Section 2: $f(t) = 5 + \sin(t) + \sin(4t) + \sin(7t)$. The parameter a changes during parameter identification.

Case 2 ($f(t) = 3 + 2\sin(10t)$). In this case, information signal with higher frequency is simulated and a large value is set for k as: $k = 10000$. As it is shown in Figure 2, $\widehat{f}(t)$ still closely follows $f(t)$ with a small mismatch $|f(t) - \widehat{f}(t)| \leq 1.65 \times 10^{-3}$ after a transient time of 6×10^{-4} s.

Case 3 ($f(t) = 5 + \sin(t) + \sin(4t) + \sin(7t)$). In this case, a composite signal is chosen as the information signal. It is assumed that $f(t) = 5 + \sin(t) + \sin(4t) + \sin(7t)$. As it is indicated in Figure 3 with $k = 8000$, information signal is identified with a small mismatch of $|f(t) - \widehat{f}(t)| \leq 1.1 \times 10^{-3}$ after a transient time of 9×10^{-4} s.

Case 4 (The parameter a changes during parameter identification process). In the above three cases, the success of the proposed algorithm is clearly indicated. In the following two cases, we are going to demonstrate that the parameter observer has strong robustness.

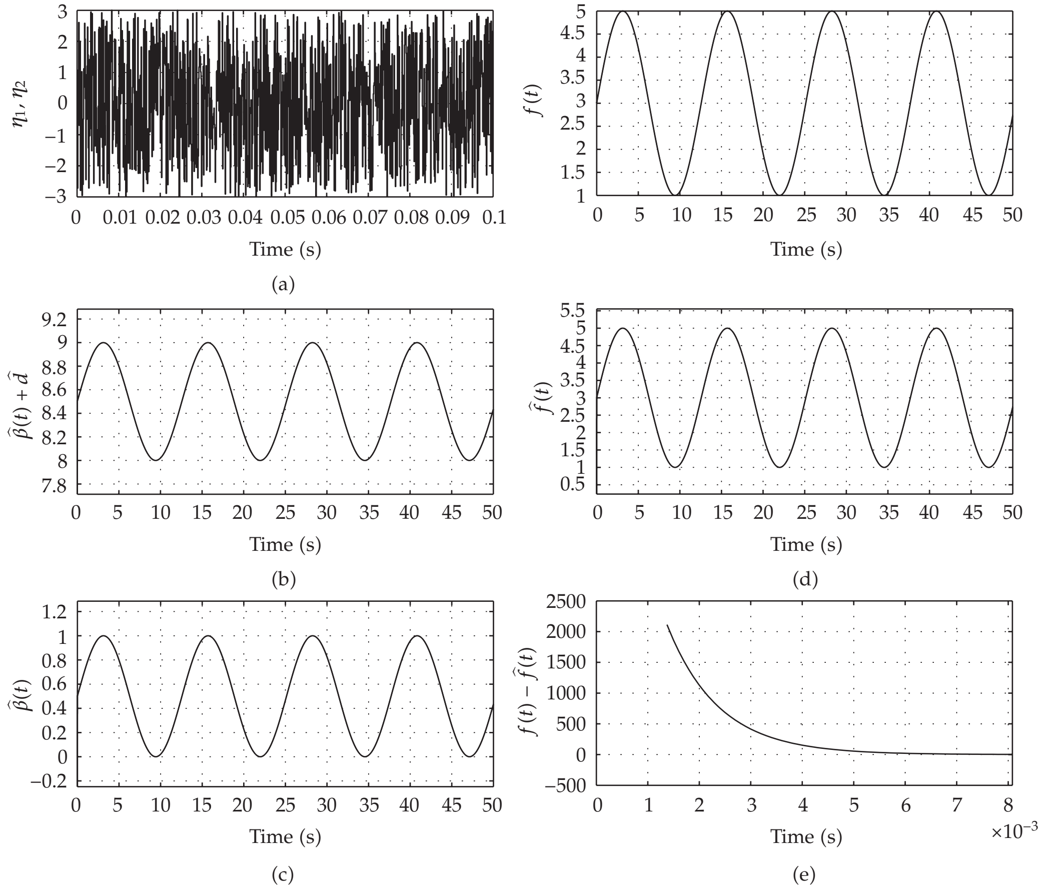


Figure 7: Simulation results in presence of noise with Case 5 of Section 2: $f(t) = 3 + 2\sin(0.5t)$.

In Case 4, it is assumed that the parameter a in system (1.1) is not a constant anymore. Instead, a is varied in the range of $[9.5, 10.5]$. Figure 4(a) shows that during the initial five seconds, $a = 5$ and then $a = 10 + 0.5\sin(0.5t)$. It is demonstrated in Figure 4 with $k = 1000$ that the information $f(t) = 3 + 2\sin(0.5t)$ can still be recovered with the same mismatch as that in Case 1. Furthermore, information signal with higher frequency and composite signal are also considered. The results with $f(t) = 3 + 2\sin(10t)$, $k = 10000$ and $f(t) = 5 + \sin(t) + \sin(4t) + \sin(7t)$, $k = 8000$ are shown in Figures 5 and 6, respectively. It is clearly demonstrated that the information signal can be recovered successfully, even if the parameter a changes during the identification process. Based on much simulations, we find that any change of parameters in the first and second equations of system (1.1) has nothing to do with the identification results.

Case 5 (Simulation results in presence of noise). In this part, we are going to consider the influence of the noise on the identification performance of the proposed parameter observer in practical applications. We keep the third equation of system (1.1) invariant and add the noise into the other two equations, then the transmitter system can be written as

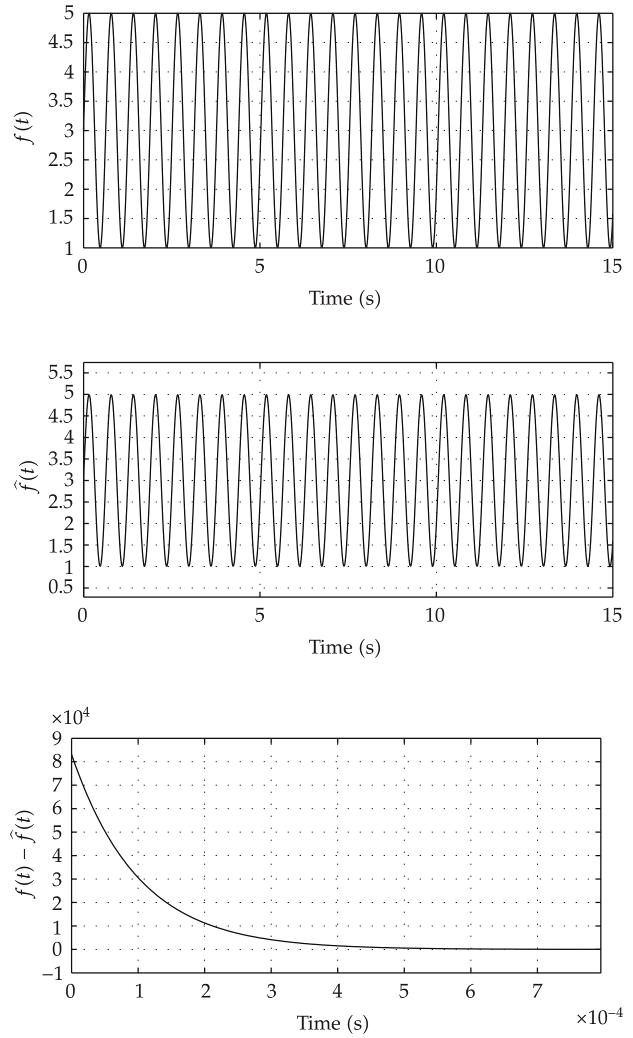


Figure 8: Simulation results in presence of noise with Case 5 of Section 2: $f(t) = 3 + 2\sin(10t)$.

follows:

$$\begin{gathered}\dot{x}_s = \left(25\beta_1(t) + a\right)\left(y_s - x_s\right) + \eta_1, \\ \dot{y}_s = \left(b - 35\beta_1(t)\right)x_s - x_s z_s + \left(29\beta_1(t) - c\right)y_s + \eta_2, \\ \dot{z}_s = x_s y_s - \frac{\beta_1(t) + d}{3} z_s.\end{gathered} \tag{2.16}$$

As it is shown in Figure 7(a), the mean of the random noise η_i $(i = 1, 2)$ is zero mean and the sample time is 0.001. In the simulations, we set the amplitudes of the noise as 3 and the information signal as $f(t) = 3 + 2\sin(0.5t)$, $f(t) = 3 + 2\sin(10t)$, $f(t) = 5 + \sin(t) + \sin(4t) + \sin(7t)$, respectively. We utilize the proposed parameter observer to

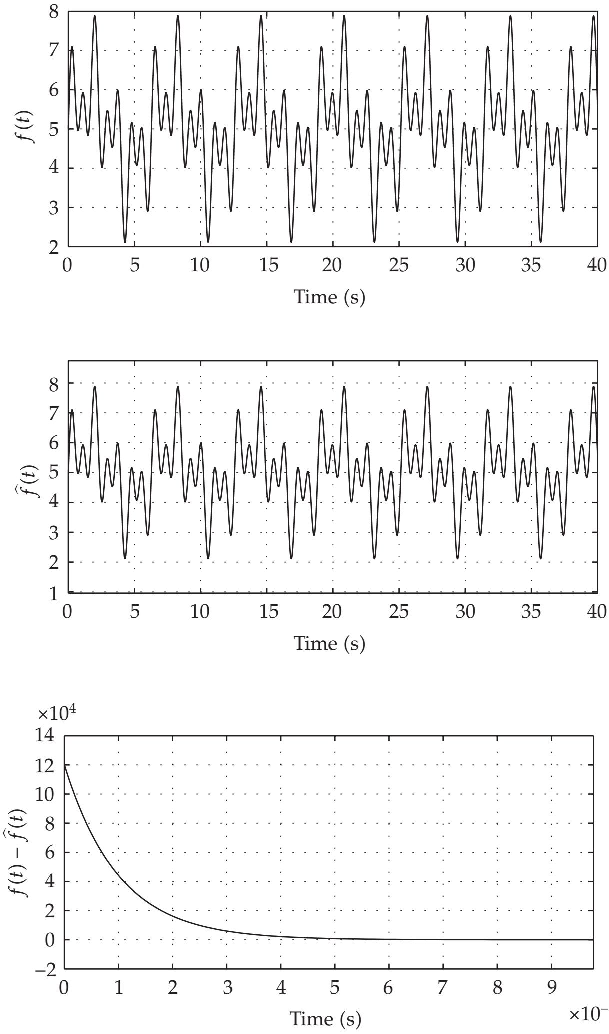


Figure 9: Simulation results in presence of noise with Case 5 of Section 2: $f(t) = 5 + \sin(t) + \sin(4t) + \sin(7t)$.

recover the information signal. Figures 7, 8, and 9 show the identification results when the information signals are $f(t) = 3 + 2\sin(0.5t)$, $f(t) = 3 + 2\sin(10t)$, $f(t) = 5 + \sin(t) + \sin(4t) + \sin(7t)$, respectively. It is indicated that for the transmitter system in presence of noise, the information signal can still be retrieved with the same mismatch as Cases 1, 2, and 3. Based on the simulations, we can conclude that the proposed observer in this paper is robust to noise.

Compared with the performance of adaptive observer proposed in [6], it takes less time for the parameter observer to recover the transmitted information. Moreover, the proposed parameter observer is robust to any change of parameters and noise in the first and second equations in system (1.1). However, the information estimation error is larger than [6], but still tolerable. To identify the information easily and quickly, accuracy is the only sacrifice.

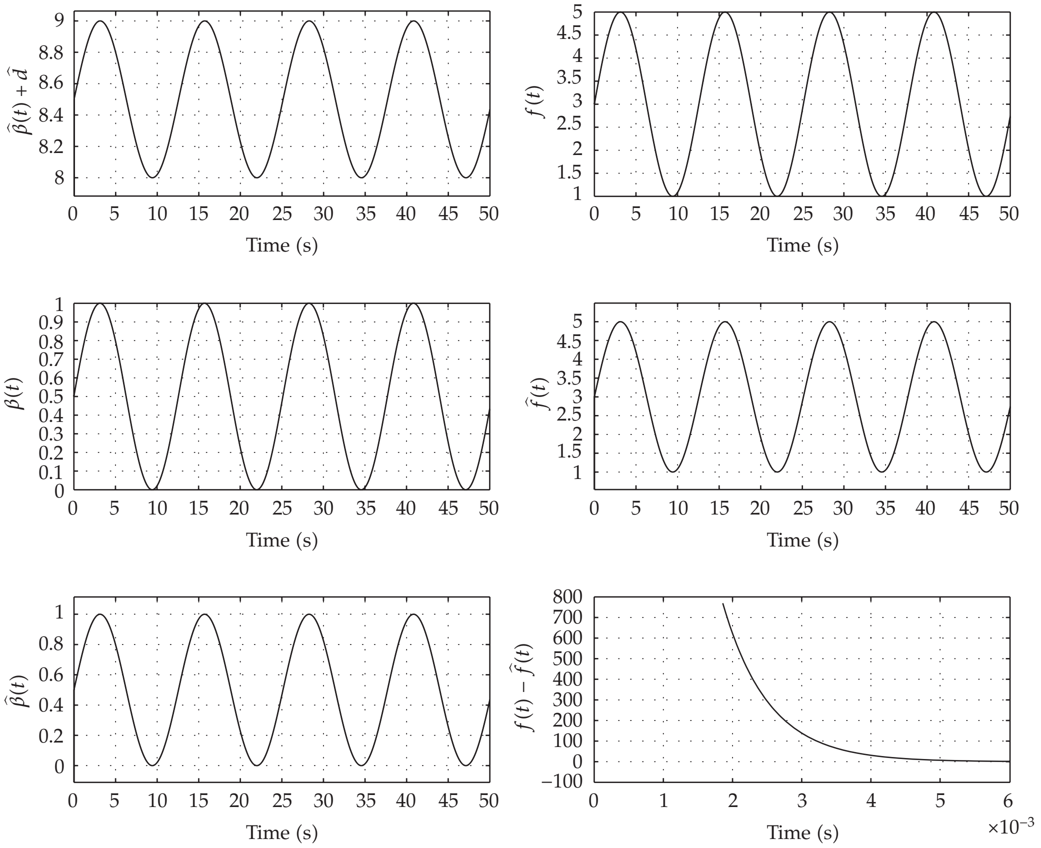


Figure 10: Simulation results with Case 1 of Section 3: $f(t) = 3 + 2\sin(0.5t)$.

3. Cryptanalysis in Case of Unavailable $\dot{\beta}(t)$

In the design process of parameter observer mentioned in Section 2, the value of $\dot{\beta}(t)$ is assumed to be available. However, from the view of real communication, it is sometimes impractical to get the information of $\dot{\beta}(t)$ [8]. Hence, in this section, we are going to consider the case with unknown $\dot{\beta}(t)$.

3.1. Design of Parameter Observer

With $\dot{\beta}(t)$ being unknown, it is impossible to get the information of $\dot{g}(t)$. The parameter observer of $g(t)$ is designed as follows:

$$\begin{gathered}
\dot{\delta} = -z_m l(z_m)\delta + l(z_m)\left(z_m p(z_m) + x_m y_m\right), \\
\widehat{g}(t) = \delta - p(z_m),
\end{gathered} \tag{3.1}$$

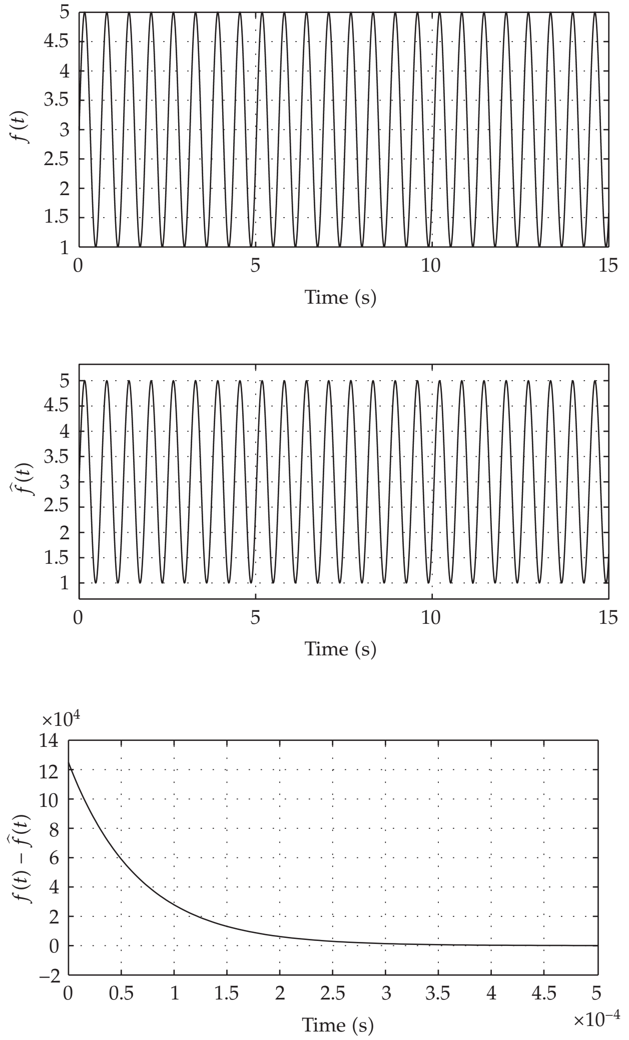


Figure 11: Simulation results with Case 2 of Section 3: $f(t) = 3 + 2\sin(10t)$.

where the designed function $l(z_m)$ determines the converging speed. The observer identifies $g(t)$ at an exponential velocity. Consequently, when the frequency of $g(t)$ is low and a large gain function $l(z_m)$ is used, $g(t)$ can be coarsely identified. Consequently, the transmitted information is coarsely achieved.

3.2. Numerical Simulation

In this part, information functions used in Section 2.2 as well as a chaotic information signal are simulated. All the parameters settings are the same as that of Section 2.2 except that a larger k is set to improve the identification performance.

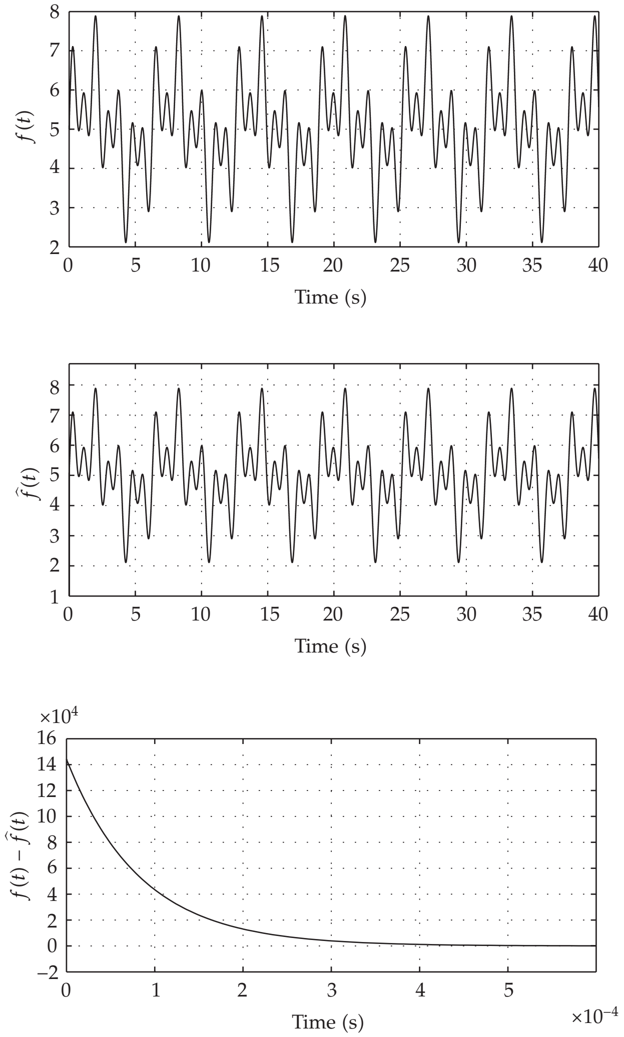
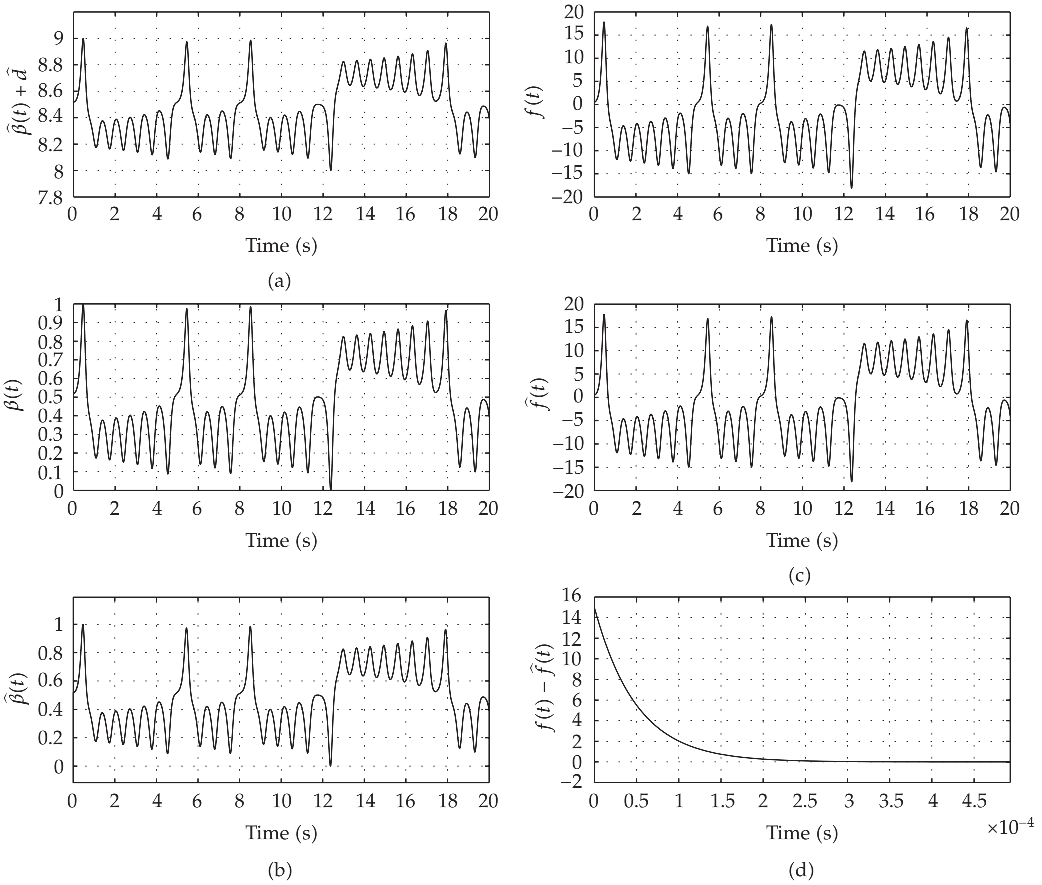


Figure 12: Simulation results with Case 3 of Section 3: $f(t) = 5 + \sin(t) + \sin(4t) + \sin(7t)$.

Case 1 ($f(t) = 3 + 2\sin(0.5t)$). The simulation results are shown in Figure 10 with $k = 1500$, which indicates the success of the information recovering. As the estimation of the absolute error shown in Figure 10, $\hat{f}(t)$ closely matches with $f(t)$, and after the initial transient time of about 0.5×10^{-3} s, information signal can be recovered with a fluctuation of $|f(t) - \hat{f}(t)| \le 0.5 \times 10^{-3}$. Although the performance is slightly worse than that shown in Case 1 of Section 2, the estimation of the absolute error is still small.

Case 2 ($f(t) = 3 + 2\sin(10t)$). The proposed parameter observer is also used to recover transmitted signal with higher frequency. A larger gain $k = 15000$ is set to achieve a small error. As shown in Figure 11, $\hat{f}(t)$ still closely follows $f(t)$ with a small mismatch of $|f(t) - \hat{f}(t)| \le 2.5 \times 10^{-3}$ after a transient time of 4×10^{-4} s. Compared with the case when $\dot{\beta}(t)$ is known, a larger fluctuation is experienced.



(a)

(b)

(c)

(d)

Figure 13: Simulation results with Case 4 of Section 3: $f(t)$ is a chaotic signal.

Case 3 ($f(t) = 5 + \sin(t) + \sin(4t) + \sin(7t)$). Figure 12 gives the simulation results when a composite signal is used and a large constant $k = 12000$ is set. Figure 12 shows the proposed parameter observer can still coarsely retrieve the transmitted information with a small mismatch of $|f(t) - \widehat{f}(t)| \leq 2 \times 10^{-3}$ after 5×10^{-4} s. The performance is inferior to that with a low frequency signal in Case 1, but superior to that with a high frequency signal in Case 2.

Case 4 ($f(t)$ is a chaotic signal). In this example, the information signal is assumed to be a chaotic signal, which is one state of a Lorenz system. We suppose that the maximum and minimum values of the signal are known, and based on (1.2), $\beta(t)$ is obtained from (1.2). Figure 13 shows the simulation results with $k = 20000$. As displayed in Figure 13, $3\widehat{g}(t) = \widehat{\beta}(t) + \widehat{d}$ is varied in the range of $[8, 9]$, so it is estimated that $\widehat{d} = 8$. It is noticed that $\widehat{f}(t)$ closely follows $f(t)$ with a small mismatch after a transient time of 3.5×10^{-4} s, implying the success of the information signal recovering.

4. Conclusions

This paper provided the cryptanalysis of a chaotic communication scheme based on parameter identification. The approach was to design a parameter observer to identify the true value of the system parameter, which was directly determined by the information signal. Supported by rigorous proof and illustrated with numerical simulation, it was clearly demonstrated that the transmitted information can be obtained with the proposed parameter observer. The results of numerical simulation showed that estimation of the absolute error was about 10^{-3} after less than 7×10^{-3} s for the presented cases with different frequencies. Furthermore, it was shown with simulations that the parameter observer was robust to parameter change and noise in the transmitter system. Therefore, the security of the analyzed communication scheme was rather weak under the observer attack, which discouraged its further applications in practical communications.

Acknowledgments

The authors would like to thank editor and all the anonymous reviewers for their helpful advices. This work is supported by the National Basic Research Program of China (973 Program) (Grant no. 2007CB310704), the Foundation for the Author of National Excellent Doctoral Dissertation of PR China (FANEDD) (Grant no. 200951), the National Natural Science Foundation of China (Grant no. 60805043, 60821001), the 111 Project (Grant no. B08004), and the National Natural Science Foundation of China (NSFC) and the Research Grants Council of Hong Kong (RGC) Joint Research Scheme (Grant no. 60731160626).

References

[1] L. M. Pecora and T. L. Carroll, “Synchronization in chaotic systems,” *Physical Review Letters*, vol. 64, no. 8, pp. 821–824, 1990.

[2] W. L. Ditto, S. N. Rauseo, and M. L. Spano, “Experimental control of chaos,” *Physical Review Letters*, vol. 65, no. 26, pp. 3211–3214, 1990.

[3] G. Hu, J. Xiao, J. Yang, F. Xie, and Z. Qu, “Synchronization of spatiotemporal chaos and its applications,” *Physical Review E*, vol. 56, no. 3, pp. 2738–2746, 1997.

[4] G. Hu and Z. Qu, “Controlling spatiotemporal chaos in coupled map lattice systems,” *Physical Review Letters*, vol. 72, no. 1, pp. 68–71, 1994.

[5] H. Lü, S. Wang, X. Li, et al., “A new spatiotemporally chaotic cryptosystem and its security and performance analyses,” *Chaos*, vol. 14, no. 3, pp. 617–629, 2004.

[6] Y. Liu and W. K. S. Tang, “Cryptanalysis of a chaotic communication scheme using adaptive observer,” *Chaos*, vol. 18, no. 4, Article ID 043110, 10 pages, 2008.

[7] X.-J. Wu, “A new chaotic communication scheme based on adaptive synchronization,” *Chaos*, vol. 16, no. 4, Article ID 043118, 12 pages, 2006.

[8] X.-P. Guan, H.-P. Peng, L.-X. Li, and Y.-Q. Wang, “Parameters identification and control of Lorenz chaotic system,” *Acta Physica Sinica*, vol. 50, no. 1, pp. 26–29, 2001.