فصلنامه علمی- پژوهشی
فنّاوری اطلاعات و ارتباطات ایران

سال دوم، شماره‌های۳و٤، بهار و تابستان ۱۳۸۹
صص: ۵۵- ٦٧

طراحی سیستم مخابراتی امن با استفاده از سنکرون‌کردن سیستم‌های آشوبی

محمد نیکخو*▪ مسعود شفیعی کوروش کیانی*****

* دانشجوی کارشناسی ارشد، دانشکده مهندسی برق، دانشگاه صنعتی امیرکبیر
** استاد، دانشکده مهندسی برق، دانشگاه صنعتی امیرکبیر
*** دانشجوی کارشناسی ارشد، دانشکده مهندسی برق، دانشگاه سمنان

چکیده

در این مقاله ابتدا مفهوم سنکرون‌کردن امن سیستم‌های آشوبی با استفاده از تکنیک‌های کنترل تطبیقی و مقاوم مورد بحث قرار گرفته است. در ادامه یک طرح مخابراتی امن جدید بر مبنای سنکرون‌کردن امن یک کلاس عمومی از سیستم‌های آشوبی به نام سیستم لورنز تعمیم یافته ارائه گردیده است. این طرح مخابراتی ترکیبی از روش‌های رمزنگاری مرسوم و روش مدولاسیون آشوبی است. نتایج تحلیل‌های تئوریک و شبیه‌سازی با استفاده از سیگنال سینوسی و سیگنال صوتی و با وجود تاخیر انتشار ثابت نامشخص بین فرستنده و گیرنده بررسی شده است. همچنین مقاومت این طرح در برابر نویز گوسی کانال با واریانس 10^{-3} نیز بررسی شده و آنالیز امنیت این سیستم مخابراتی از نقطه نظر جستجوی بروت- فورس مورد ارزیابی قرار گرفته است. با استفاده از این طرح مخابراتی طول کلید بسیار مناسبی حاصل شده است.

کلیدواژگان: آشوب، سیستم‌های غیرخطی، سنکرون‌کردن، مشاهده‌گر، مخابرات امن

۱- مقدمه

یکی از این پدیده‌های بسیار جالب در مبحث سیستم‌های غیرخطی، "آشوب" است. کشف آشوب این اصل اساسی دانش را که "سیستم‌های یقینی دارای رفتاری قابل پیش‌بینی هستند" ، زیر سوال برد. سیستم‌های آشوبی دارای چندین خاصیت قابل توجه نظیر: ارگادیک بودن[1]، تصادفی بودن، غیر تناوبی بودن، حساسیت به شرایط اولیه و غیر قابل پیش بینی بودن، هستند[۱و۲] ، که آنها را برای کاربرد رمزنگاری مساعد می-سازد. محققین براین عقیده‌اند که این خاصیت‌ها می‌توانند چندین ویژگی اولیه نظیر پخش‌شدگی[2] و درهم‌ریختگی[3] که در رمزنگاری مدرن مورد نیاز است را برآورده سازند[۳ تا ۵].

در چنددهه اخیر، ساخت سیستم‌های رمزنگار بر مبنای تئوری آشوب توجه بسیاری را به خود جلب کرده است. این سیستم‌ها را به دو دسته کلی،سیستم‌های رمزنگاری آشوبی زمان گسسته و سیستم‌های رمزنگاری آشوبی زمان پیوسته تقسیم‌بندی می‌کنند. سیستم‌های رمزنگاری آشوبی زمان گسسته برای رمزنگاری اطلاعات دیجیتال از سیستم‌های آشوبی زمان گسسته، معمولاً به عنوان منبع تولید کننده بیت شبه رندم، استفاده می‌کنند. استفاده از سیستم‌های آشوبی زمان گسسته برای هدف رمزکردن نخستین بار توسط آقای ماتئوس[4] در[٦] انجام گرفت. در این روش، یک نگاشت آشوبی تک بعدی، که برای یک محدوده از شرایط اولیه و

1. ergodicity
2. Diffusion
3. Confusion
4. Matthews

▪ نویسنده عهده‌دار مکاتبات (Nickhoo_m@yahoo.com)

پارامترهای کنترلی دارای رفتار آشوبی است، برای تولید یک دنباله‌ای از اعداد شبه رندم برای رمزنگاری و رمزگشایی پیام مورد استفاده قرار می‌گیرد. اندکی بعد از آن، در سال ۱۹۹۰، یک سیستم رمزنگار بر مبنای نگاشت تنت[1] آشوبی تکه‌ای خطی که توسط آقای هابوتسو[2] و همکارانش توسعه یافت ایجاد گردید [۷]، در این مقاله پارامتر نگاشت تنت به عنوان یک کلید محرمانه مورد استفاده قرار گرفت و رمزنگاری ورمزگشایی به ترتیب توسط تکرار معکوس و مستقیم نگاشت تنت آشوبی حاصل می‌گشت. تعداد بسیار زیاد دیگری از الگوریتم‌های رمزنگاری آشوبی گسسته در چند سال اخیر پیشنهاد شده‌اند، که برای نمونه می‌توان به مراجع [۸و۹] مراجعه کرد.

سیستم رمزنگار آشوبی زمان پیوسته، اساساً جهت تولید سیگنال آشوبی شبه نویز، غیر متناوب، باند وسیع برای مخابرات امن مورد استفاده قرار می‌گیرد، در حالیکه سیگنال‌های پیام معمولاً سیگنال-های پیوسته بوده که درون سیگنال آشوبی در سمت فرستنده مخفی می‌گردند، و در سمت گیرنده این سیگنال‌های پیام توسط فرایند سنکرون‌کردن بازیابی می‌شوند.

ایده استفاده از سیستم‌های آشوبی سنکرون برای مخابرات امن ابتدا توسط پکورا و کارول ارائه گردید[۱۰]. این دو گزارش کردند که سیستم‌های آشوبی خاصی می‌توانند به دو زیر سیستم درایو و زیر سیستم پاسخ پایدار تجزیه گردند. این دو زیر سیستم با استفاده از یک سیگنال درایومشترک با یکدیگر کوپل شده‌اند. بر طبق مفهوم درایو–پاسخ پکورا و کارول، چندین سیستم مخابراتی امن با موفقیت طراحی گردید[۱۱تا۱۳]. به علاوه بر اساس تئوری پایداری لیاپانوف، روش فیدبک حالت خطی یا غیر خطی، روش مفید دیگری برای سنکرون‌کردن دو سیستم آشوبی ایزوله شده برای کاربرد مخابرات امن در مقاله [۱٤] پیشنهاد شد. روش طراحی مشاهده‌گر حالت غیرخطی برای مسئله سنکرون کردن آشوبی یک کلاس از سیستم‌های آشوبی در [۱۵ و۱٦] ارائه شده است.

بر طبق این رهیافت‌ها، روش‌های مخابرات امن آشوبی را می‌توان به انواع ماسک زدن آشوبی[3]، مدولاسیون آشوبی[4] و سوییچینگ آشوبی[5] تقسیم بندی نمود. در روش اول، سیگنال پیام محرمانه فقط با سیگنال کریر آشوبی جمع می‌گردد [۱۷و۱۸]. درروش دوم، نه تنها سیگنال پیام با سیگنال کریر آشوبی جمع می‌گردد، بلکه حالت‌های سیستم آشوبی توسط سیگنال پیام از طریق یک روند معکوس پذیر مدوله می‌گردند به نحوی که سیگنال آشوبی تولید شده ذاتاً شامل اطلاعات سیگنال پیام است [۱۳و۱٦]. در روش سوم، که به نام سوییچینگ آشوبی است نیازمند دو سیستم آشوبی برای بیت‌های صفر و یک هستیم. سیگنال ارسالی توسط سوییچ بین این دو سیستم آشوبی بر اساس اینکه صفر یا یک سیگنال پیام منتقل می‌گردد انتخاب می‌گردد [۱۹و۲۰].

اگرچه بکارگیری سیستم‌های آشوبی به صورت شبیه‌سازی وسخت‌افزاری با موفقیت انجام شد، ولی کاربردهای اولیه سیستم-های آشوبی برای مخابرات امن دارای سطح پایینی از امنیت بودند از آنجایی که فرد مهاجم می‌توانست با بکارگیری تکنیک‌های مختلف برداشتن ماسک از سیگنال ارسالی سیگنال پیام را بازسازی نماید [۲۱]. برای چیره‌شدن بر این مسئله، روش‌های مختلفی برای بهبود امنیت سیستم‌های رمزنگارارائه شده است. برای مثال، یک طرح رمزنگاری پیشرفته با استفاده از سیگنال‌های آشوبی چندگانه در [۲۲] ارائه شده است و در[۲۰و۲۳] نویسندگان به یک ایده برای انتقال امن سیگنال پیام با در نظرگرفتن این نکته که رمزنگاری سیگنال آشوبی به اندازه رمزنگاری سیگنال پیام اهمیت دارد دست یافتند. برای این منظور روش رمزنگاری مرسوم و سنکرون‌کردن آشوب با یکدیگر برای طراحی سیستم رمزنگار آشوبی ترکیب شدند.

با این وجود، از آنجایی که همه سیستم‌های مخابراتی امن آشوبی، که در بالا اشاره گردید، بر مبنای ویژگی سنکرون‌کردن سیستم‌های آشوبی ساده هستند، نکته کلیدی برای این روش‌ها امنیت سنکرون‌کردن است. متاسفانه این مسئله در گذشته برای طرح‌های سنکرون‌کردن مورد توجه قرار نمی‌گرفت. برای مثال، در [۲٤]، محققین تئوری سنکرون‌کردن مقاوم و سنکرون‌کردن تطبیقی را برای رفتارکردن با مسائل مربوط به پارامترهای ناشناخته یا عدم تطبیق پارامترها در نظر گرفته‌اند. از آنجایی که مقدار پارامترهای سیستم آشوبی معمولاً به عنوان "کلید" محرمانه برای سنکرون-کردن بین فرستنده و گیرنده در نظر گرفته می‌شوند، این روش‌های مقاوم و تطبیقی امکانی را برای اندازه‌گیری کلید به ما می‌دهند. به این معناکه با استفاده از تکنیک‌های تطبیقی و مقاوم، مهاجم قادر است بدون دانش دقیق از "کلید" یک سیستم گیرنده طراحی کند، و با فرستنده سنکرون کند. در این زمینه، مفهوم سنکرون‌کردن امن با توجه به روش‌های کنترل مقاوم و تطبیقی در [۲۵] توضیح داده شده است.

1. Tent Map
2. Habutsu
3. Chaotic Masking
4. Chaotic Modulation
5. Chaotic Switching

در ادامه این مقاله در بخش ۲ طرح سنکرون کردن امن مورد استفاده درسیستم مخابراتی امن پیشنهادی فرموله می‌گردد. در بخش ۳ طرح مخابراتی امن پیشنهادی ارائه گردیده و در بخش ٤ نتایج شبیه سازی با سیگنال‌های مختلف آمده است . در بخش۵ آنالیز امنیت با روش جستجوی بروت-فورس و در بخش ٦ نتیجه‌گیری آورده شده است.

۲- طرح سنکرون‌کردن امن مورد استفاده در سیستم مخابراتی امن پیشنهادی

واضح است که اگر یک طرح سنکرون‌کردن که برای مخابرات امن استفاده می‌شود به راحتی آسیب‌پذیر باشد نامطلوب است. برای فهم این موضوع، مفهوم سنکرون‌کردن امن را، با توجه به طرح-های کنترل مقاوم وکنترل تطبیقی ارئه می‌دهیم [۲۵]. برای شروع تعریف سنکرون‌کردن سیستم‌های آشوبی را در تئوری کنترل ارائه می‌نماییم.

سیستم آشوبی غیرخطی را با بردار پارامتر μ در نظر بگیرید:

$$\dot{x} = f(x,t,\mu) \qquad (۱)$$

در حالیکه $x \in \Re^n$ و $\mu \in \Re^m$ است.

تعریف۱: گوییم سیستم (۱) به سنکرون‌شدن با حل $x(t), t \geq t_0$ دست پیدا کرده است، اگر یک خروجی کمکی $y = y(x) \in \Re^p$ و $p < n$ وجود داشته باشد، به نحوی که با این خروجی، سیستم (۱) دارای مشاهده‌گر مجانبی فرم ذیل برای حل $x(t), t \geq t_0$:

$$\dot{\hat{x}} = f(\hat{x},t,\mu) + \phi(y(x), y(\hat{x}), \hat{x}, \mu) \qquad (۲)$$

باشد در حالیکه $x, \hat{x} \in \Re^n$ و $\mu \in \Re^m$ است.

تعریف۲:گوییم سنکرون‌کردن به صورت **امن ضد تطبیقی**[1] نسبت به پارامتر μ است اگر هیچ مشاهده‌گر تطبیقی به شکل (۲) با $\mu = \hat{\mu}$, $\hat{\mu} \in \Re^m$ وجود نداشته باشد به نحوی که بتواند از الگوریتم تطبیقی ذیل حاصل شود.

$$\dot{\hat{\mu}} = \psi(\hat{\mu}, y(x), y(\hat{x}), \hat{x}, t) \qquad (۳)$$

تعریف۳: گوییم سنکرون‌کردن به صورت **امن ضد مقاوم**[2] نسبت به پارامتر μاست، هر گاه یک ثابت مثبت K وجود داشته باشد به‌نحوی که برای هر $\bar{\mu}$ و $\tilde{\mu}$ از یک مجموعه بسته داده شده و برای هر حل سیستم(۱) با $\mu = \bar{\mu}$ و مشاهده‌گر (۲) با $\mu = \tilde{\mu}$ داشته باشیم:

$$\lim_{t\to\infty} \|x(t) - \hat{x}(t)\| \geq K(\bar{\mu} - \tilde{\mu}) \qquad (٤)$$

سپس **سنکرون کردن امن** به این صورت تعریف می‌گردد که، هم امن ضد تطبیقی و هم امن ضد مقاوم باشد. روشن است که، برای هر طرح سنکرون‌کردن، امن ضد تطبیقی نشان‌دهندهٔ این است که، اگر پارامتر μ به عنوان کلید محرمانه در نظر گرفته شود، نبایستی هیچ راهی وجود داشته باشد که یک مهاجم بتواند با استفاده از تکنیک طراحی مشاهده‌گر تطبیقی به آن دست یابد. به علاوه، امن ضد مقاوم به این معناست که برای هر روش سنکرون‌کردن با استفاده از یک پارامترکلید تخمین‌زده شده، یک عدم دقت به اندازه کافی بزرگ از پارامترهای تخمین بایستی منجر به خطای سنکرون‌کردن به اندازه کافی بزرگ گردد. بنابراین هر دو ویژگی امنیتی ضد مقاوم و ضد تطبیقی از طرح سنکرون‌کردن، برای مقاومت در برابر هجوم قاطع هستند. برای اینکه این دو ویژگی تضمین می‌کنند که فقط یک شخص که دقیقاً کلید محرمانه را می-شناسد قادر باشد یک مشاهده‌گر برای ساختن سیستم سنکرون - ساز طراحی نماید.

سیستم لورنز تعمیم یافته[3] وشکل تبدیل شده آن، که به نام فرم کانونیکال مشاهده‌گر نامیده می‌شود را در نظر بگیرید[۲۵]:

$$\dot{\eta} = A\eta + F(\eta, y) \qquad (۵)$$

که $\eta = [\eta_1 \quad \eta_2 \quad \eta_3]^T$ حالت سیستم و

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}$$

$$F(\eta, y) = \begin{bmatrix} (\lambda_1 + \lambda_2)\eta_1 \\ -\lambda_1\lambda_2\eta_1 - (\lambda_1 - \lambda_2)\eta_1\eta_3 - 0.5(k+1)(\eta_1)^3 \\ K(k)(\eta_1)^2 \end{bmatrix}$$

$K(k) = \dfrac{\lambda_3(k+1) - 2k\lambda_2 - 2\lambda_2}{2(\lambda_1 - \lambda_2)}$ ، $k \in (-1, \infty)$ است.

از آنجایی که نشان‌دهنده یک کلاس خیلی عمومی از سیستم‌های آشوبی با فقط یک پارامتر است، می‌خواهیم از آن برای طراحی سیستم مخابراتی بر مبنای سنکرون‌کردن امن استفاده کنیم.

اکنون سیستم (۵) با نمودار محدود شده آن $\eta(t)$ و $t \geq t_0$ را به عنوان سیستم درایو و حالت اول η_1 که به عنوان سیگنال درایو برای درایوکردن سیستم پاسخ انتخاب می‌شود را در نظر بگیرید. سیستم درایو به صورت ذیل قابل نمایش است:

$$\dot{\eta} = A\eta + F(\eta, y)$$
$$y = C^T\eta \qquad (٦)$$

در حالیکه $C^T = [1 \quad 0 \quad 0]$. توجه کنید که، برای سیستم درایو (٦)، جفت (C^T, A) مشاهده‌پذیر نیست اما آشکارپذیر است، که

1. Antiadaptive Secure
2. Antirobust Secure
3. Generalized Lorenz System(GLS)

نشان می‌دهد امکان طراحی سیستم پاسخ به صورت مشاهده‌گر برای سنکرون‌کردن سیستم (٦) وجود دارد. اکنون سیستم ذیل را به عنوان یک پاسخ در نظر بگیرید:

$$\dot{\hat{\eta}} = A\hat{\eta} + F(\hat{\eta}, y) + L(\hat{\eta}_1 - \eta_1')$$
$$= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \hat{\eta} + \begin{bmatrix} (\lambda_1+\lambda_2)\eta_1' \\ -\lambda_1\lambda_2\eta_1' - (\lambda_1-\lambda_2)\eta_1'\hat{\eta}_3 - 0.5(k+1)(\eta_1')^3 \\ K(k)(\eta_1')^2 \end{bmatrix} + \begin{bmatrix} l_1 \\ l_2 \\ 0 \end{bmatrix} (\hat{\eta}_1 - \eta_1') \quad (٧)$$

در حالیکه $L = [l_1 \quad l_2 \quad 0]^T$ و $\hat{\eta} = [\hat{\eta}_1 \quad \hat{\eta}_2 \quad \hat{\eta}_3]^T$ با $l_{1,2} < 0$ است. به علاوه، η_1' سیگنال درایو ورودی است، که ممکن است توسط نویز در طول فرایند ارسال بایاس شود.با فرض $\|\eta_1(t) - \eta_1'(t)\| < \varepsilon$ که ε یک ثابت مثبت کوچک است، تئوری ذیل به دست می‌آید:

تئوری۱ [۲۵]: یک سیستم درایو داده شده توسط (٦) و یک سیستم پاسخ بر مبنای مشاهده‌گر توسط (٧) را در نظر بگیرید. رابطه زیر به صورت نمایی در زمان برقرار است:

$$\lim_{t\to\infty} \| \eta(t) - \hat{\eta}(t) \| \le D\varepsilon \quad (٨)$$

در حالیکه D برخی ثابت‌های مثبت است. مخصوصاً، اگر $\eta_1 = \eta_1'$ باشد، سیستم پاسخ (٧) به صورت مجانبی سرتاسری سیستم درایو (٦)را سنکرون می‌سازد ، به این معنی که :

$$\lim_{t\to\infty} \| \eta(t) - \hat{\eta}(t) \| = 0 \quad (٩)$$

به علاوه در[۲۵] اثبات شده که سیستم لورنز تعمیم یافته هم خاصیت امن ضدمقاوم و هم امن تطبیقی را برآورده می سازد، لذا برای کاربرد مخابرات امن مناسب به نظر می‌رسد.

۳- طرح مخابراتی امن پیشنهادی

در طرح مخابراتی پیشنهادی از تکنیک رمزنگاری مرسوم همراه با مدولاسیون آشوبی برای رمزنگاری بیشتر استفاده شده است. شکل (١) بلوک دیاگرام سیستم رمزکننده پیشنهاد شده را نشان می‌دهد، که شامل یک ماژول رمزکننده (فرستنده)، یک کانال مخابراتی عمومی و یک ماژول رمزگشا (گیرنده) است. همانطوری که شکل نشان می‌دهد، فرستنده شامل یک سیستم آشوبی و طرح رمزنگاری است. "کلید" محرمانه $Key \equiv \{k, \lambda_1, \lambda_2, \lambda_3\}$، که در شکل (١) نشان داده شده است، برای تنظیم مقادیر پارامترهای سیستم آشوبی استفاده شده است. سیستم آشوبی برای تولیدکردن دو سیگنال کلید $k_1(t)$ و $k_2(t)$ استفاده شده است. سیگنال کلید اول، $k_1(t)$، یک متغیر حالت سیستم آشوبی است، که بایستی توسط طرح رمزکننده به سیگنال پیام پیش‌رمزکننده، $P(t)$،مورد استفاده قرار گیرد.سپس، سیگنال پیش‌رمزکننده، $E(t)$، با سیگنال کلید دوم $k_2(t)$، که متغیرحالت دیگر سیستم آشوبی است، برای رمزکردن بیشتر جمع می‌شود. این مجموع به سیستم گیرنده از طریق کانال عمومی انتقال داده می‌شود، در حالیکه دوباره به سیستم آشوبی فرستنده فیدبک می‌گردد. سیستم گیرنده، مشابه قسمت فرستنده، شامل یک سیستم آشوبی و طرح رمزگشایی است. با استفاده از"کلید" کاملاً مشابه برای پارامترهای سیستم آشوبی، سنکرون‌کردن بین فرستنده و گیرنده قابل دستیابی است. دو سیگنال کلید، $k_1(t)$ و $k_2(t)$، دقیقاً مشابه آنچه که توسط سیستم فرستنده استفاده می‌شود، دوباره توسط طرح سنکرون‌کردن بازسازی می‌گردد. طرح رمزگشا نهایتاً با استفاده از این کلیدها سیگنال پیام $P(t)$ را بازیابی می‌کند.

سیستم آشوبی استفاده شده توسط معادله (٦) با اندکی تغییرات به صورت معادله (١٠) داده شده است:

(١٠)

$$\dot{\eta} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \eta + \begin{bmatrix} (\lambda_1+\lambda_2)y(t) \\ -\lambda_1\lambda_2 y(t) - (\lambda_1-\lambda_2)\eta_3 y(t) - 0.5(k+1)(y(t))^3 \\ K(k)(y(t))^2 \end{bmatrix} + LE(t)$$
$$y = \eta_1 + E(t)$$

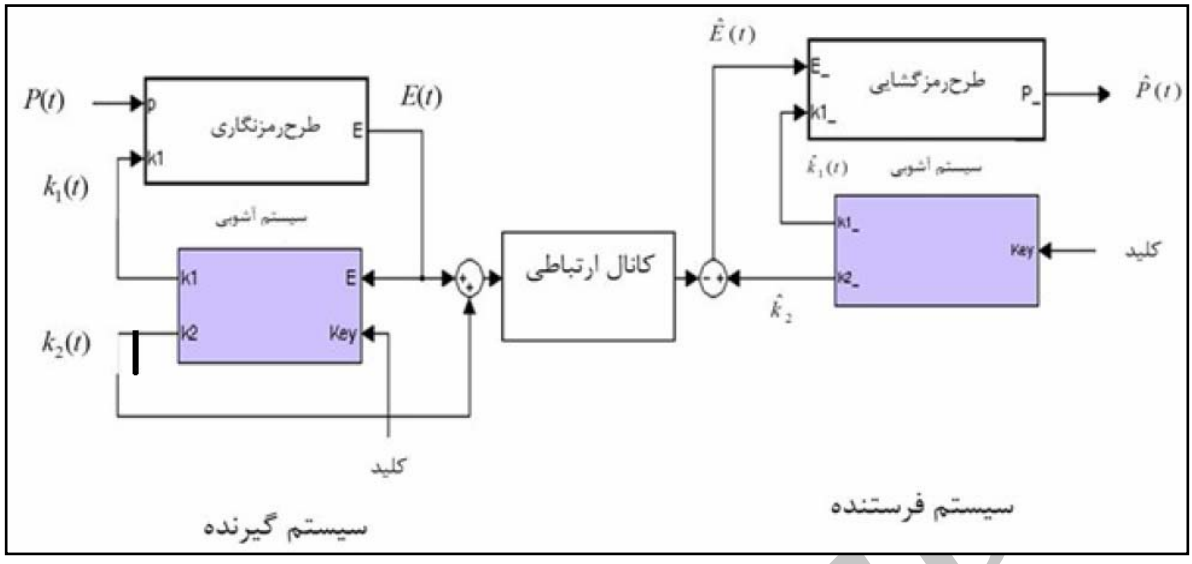
$E(t) \in \Re$ سیگنال پیش‌رمز شده است که از طرح رمزنگاری خارج می‌شود. $L = [L_1 \quad L_2 \quad 0]^T$ یک بردار بهره است. $\eta_1(t)$ را به عنوان سیگنال کلید $k_2(t)$ در نظر می‌گیریم، سپس جمع $k_2(t)$ و سیگنال پیش‌رمزکننده $E(t)$ را به نام $y(t) \in \Re$ می‌نامیم که به عنوان سیگنال انتقال آشوبی، برای درایو کردن گیرنده به کار می‌رود. برای طرح رمزنگاری، از آنجایی که جزء سوم متغیرهای حالت سیستم آشوبی، η_3، فقط آشکارپذیر است و مشاهده پذیر نمی باشد، از آن به عنوان سیگنال کلید دیگر $k_1(t)$ کمک گرفته‌ایم. این کار سطح امنیت سیستم رمز کننده پیشنهاد شده را افزایش می‌دهد. سیگنال پیام با استفاده از رمز شیفت‌دهنده n تایی[1] توصیف شده در [۲۲]پیش‌رمز می‌گردد. رمز شیفت‌دهنده n تایی به صورت رابطه (١١) نشان داده می‌شود:

$$E(t) = \underbrace{f(...f(}_{n} f(p(t), \underbrace{k_1(t)), k_1(t)), ..., k_1(t))}_{n} \quad (١١)$$

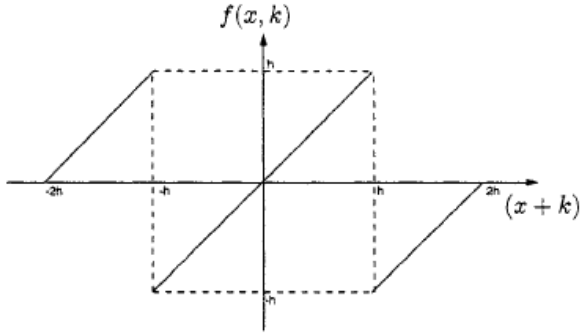
که f یک تابع غیرخطی داده شده توسط رابطه

$$f(x,k) = \begin{cases} (x+k) + 2h, & -2 \le (x+k) \le -h \\ (x+k), & -h \le (x+k) \le h \\ (x+k) - 2h, & h \le (x+k) \le 2h \end{cases} \quad (١٢)$$

1. n-shift cipher



شکل ۱ بلوک دیاگرام سیستم مخابراتی امن جدید



شکل ۲ تابع مورد استفاده در پیش رمز کننده

است. جائیکه h پارامتر ثابت انتخاب شده به نحوی است که $x(t)$ و $k(t)$ بین $(-h,h)$ قرار بگیرند. این تابع در شکل (۲) نشان داده شده است.

در رمز شیفت‌دهنده n تایی، سیگنال کلید $k_1(t)$، n بار برای رمزکردن سیگنال پیام استفاده شده است. از آنجایی که سیگنال پیش‌رمزکننده یک تابعی از $P(t)$ و $k_1(t)$ است، و علاوه برآن سیگنال پیش‌رمزکننده دوباره برای رمزنگاری بیشتر توسط سیگنال کلید دوم که $k_2(t)$ است مدوله می‌گردد، لذا مشخصات استاتیک و دینامیک $P(t)$ و $k_1(t)$ هردو مخفی می‌گردند. به صورت مشابه، سیستم سنکرون آشوبی در قسمت گیرنده به صورت رابطه (۱۳) قابل بازسازی است:

$$\dot{\hat{\eta}}=\begin{bmatrix}0&1&0\\0&0&0\\0&0&\lambda_3\end{bmatrix}\hat{\eta} + \begin{bmatrix}(\lambda_1+\lambda_2)y(t)\\ -\lambda_1\lambda_2 y(t)-(\lambda_1-\lambda_2)\hat{\eta}_3 y(t)-0.5(k+1)(y(t))^3\\ K(k)(y(t))^2\end{bmatrix}+L(y(t)-\hat{\eta}_1) \quad (۱۳)$$

که y سیگنال دریافت‌شده و L بردار بهره مشابه با آن بهره‌ای است که در سیستم فرستنده استفاده شد. بر این عقیده‌ایم که سنکرون‌شدن فقط زمانی قابل دستیابی است که "کلید" مشابهی در هر دو قسمت فرستنده و گیرنده مورد استفاده قرار گیرد. بنابراین سیگنال‌های کلید که به نام $\hat{k}_1(t)\to k_1(t)$ و $\hat{k}_2(t)\to k_2(t)$ هستند زمانی که t به سمت بی نهایت می رود می‌توانند دوباره تولید گردند. سرانجام، طرح رمزگشایی متناظر به صورت رابطه(۱٤) قابل نمایش است:

$$\hat{p}(t)=\underbrace{f(\ldots f}_{n}(f(\hat{E}(t),\underbrace{-\hat{k}_1(t)),-\hat{k}_1(t)),\ldots,}_{n}-\hat{k}_1(t)) \quad (۱٤)$$

که $\hat{E}(t)=y(t)-\hat{k}_1(t)$ است. تئوری(۲) را دراین مورد بیان می‌کنیم:

تئوری۲: فرض کنید که سیگنال پیام، $P(t)$، از طریق سیستم مخابراتی شامل فرستنده با سیستم آشوبی (۱۰) و طرح رمزنگاری (۱۱)، وگیرنده با سیستم آشوبی (۱۳) و طرح رمزنگاری (۱٤) منتقل شده باشد. با استفاده از "کلید" مشابه هم در سیستم فرستنده و هم در گیرنده یک سنکرون‌کردن عمومی بین سیستم فرستنده و گیرنده قابل دستیابی است و سیگنال پیام، $P(t)$، به صورت کامل در سمت گیرنده قابل بازسازی است.

اثبات: خطای سنکرون‌کردن $\tilde{\eta}(t)=\eta(t)-\hat{\eta}(t)$ را تعریف می‌کنیم در حالیکه $\tilde{\eta}=[\tilde{\eta}_1\ \ \tilde{\eta}_2\ \ \tilde{\eta}_3]^T$ و داریم:

$$\dot{\tilde{\eta}}_1(t) = \dot{\eta}_1(t) - \dot{\hat{\eta}}_1(t)$$
$$= \eta_2(t) + (\lambda_1+\lambda_2)(\eta_1(t)+E(t)) + L_1E(t)$$
$$- \hat{\eta}_2(t) - (\lambda_1+\lambda_2)(\eta_1(t)+E(t)) - L_1(\eta_1(t)+E(t)-\hat{\eta}_1(t))$$
$$= -L_1(\eta_1(t)-\hat{\eta}_1(t)) + \eta_2(t) - \hat{\eta}_2(t)$$
$$= -L_1\tilde{\eta}_1(t) + \tilde{\eta}_2(t)$$

(۱۵)

$$\dot{\tilde{\eta}}_2(t) = \dot{\eta}_2(t) - \dot{\hat{\eta}}_2(t)$$
$$= (-\lambda_1\lambda_2 - (\lambda_1-\lambda_2)\eta_3(t))(\eta_1(t)+E(t))$$
$$- 0.5(k+1)(\eta_1(t)+E(t))^3 + L_2E(t)$$
$$- (-\lambda_1\lambda_2 + (\lambda_1-\lambda_2)\hat{\eta}_3(t))(\eta_1(t)+E(t))$$
$$+ 0.5(k+1)(\eta_1(t)+E(t))^3 - L_2(\eta_1(t)+E(t)-\hat{\eta}_1(t))$$
$$= -(\lambda_1-\lambda_2)(\eta_1(t)+E(t))\tilde{\eta}_3(t) - L_2\tilde{\eta}_1(t)$$
$$= -L_2\eta_1(t) + (\lambda_1-\lambda_2)(\eta_1(t)+E(t))\tilde{\eta}_3(t)$$

(۱۶)

$$\dot{\tilde{\eta}}_3(t) = \dot{\eta}_3(t) - \dot{\hat{\eta}}_3(t)$$
$$= \lambda_3\eta_3(t) + K(k)(\eta_1(t)+E(t))^2 - \lambda_3\hat{\eta}_3(t) - K(k)(\eta_1(t)+E(t))^2$$
$$= \lambda_3\tilde{\eta}_3(t)$$

(۱۷)

با توجه به نامساوی $-\lambda_2 > \lambda_1 > -\lambda_3 > 0$ [25] که شرط وجود آشوب در سیستم لورنز تعمیم یافته است معادله (۱۸) برآورده می‌گردد:

$$\lim_{t\to\infty} \|\tilde{\eta}_3(t)\| = 0 \qquad (۱۸)$$

باتعریف $\overline{\eta}(t) = [\tilde{\eta}_1(t) \quad \tilde{\eta}_2(t)]^T$، داریم:

$$\dot{\overline{\eta}}(t) = \begin{bmatrix} \dot{\tilde{\eta}}_1(t) \\ \dot{\tilde{\eta}}_2(t) \end{bmatrix}$$
$$= \begin{bmatrix} -L_1 & 1 \\ -L_2 & 0 \end{bmatrix}\overline{\eta}(t) + \begin{bmatrix} 0 \\ (\lambda_1-\lambda_2)(\eta_1(t)+E(t)) \end{bmatrix}\tilde{\eta}_3(t)$$
$$= S\overline{\eta}(t) + \phi(t)\tilde{\eta}_3(t)$$

(۱۹)

که $S = \begin{bmatrix} -L_1 & 1 \\ -L_2 & 0 \end{bmatrix}$ و $\phi(t) = \begin{bmatrix} 0 \\ (\lambda_1-\lambda_2)(\eta_1(t)+E(t)) \end{bmatrix}$ یک تابع محدود شده هستند. از آنجایی که $\phi(t)$ و $\tilde{\eta}(t)$ محدود شده هستند، پس اگر $L_{1,2}$ را بتوانیم به نحوی انتخاب کنیم که S یک ماتریس هرویتز باشد، خطای سنکرون‌کردن به صورت نمایی به سمت صفر میل خواهد کرد. به محض اینکه سنکرون‌شدن بین فرستنده و گیرنده بدست آید، سیستم آشوبی در سمت گیرنده قادر است سیگنال‌های کلید را مشابه با سیگنال‌های استفاده شده در سمت فرستنده تولید کند یعنی اینکه $\lim_{t\to\infty}\hat{k}_1(t) \to k_1(t)$ و $\lim_{t\to\infty}\hat{k}_2(t) \to k_2(t)$. این بدان معناست که

$$\lim_{t\to\infty}\hat{\tilde{E}}(t) = y(t) - \hat{k}_2(t) = E(t) + k_2(t) - \hat{k}_2(t) \to E(t)$$

و طرح رمزگشایی (۱۴) را می‌توان به صورت ذیل نوشت:

$$\hat{p}(t) = \underbrace{f(...f(f}_{n}(E(t), \underbrace{-K_1(t)), -K_1(t)),...,-K_1(t))}_{n} \qquad (۲۰)$$

سیستم (۲۰)روش معکوس طرح رمزنگاری (۱۱) است، این امر نشان می‌دهد که سیگنال اطلاعات نهایتاً می‌تواند بازیابی شود.

در هر سیستم مخابراتی واقعی، همیشه یک تاخیر زمانی انتشار در طول فرایند انتقال سیگنال‌های پیام از فرستنده به گیرنده وجود دارد. از نقطه نظر تئوری کنترل، تاخیر زمانی ممکن است باعث ناپایداری سیستم مخابراتی گردد[۲۶]. همانطور که درکار [۲۷] می‌بینیم که وجود تاخیر زمانی در سیستم سنکرون‌شده ممکن است منجر به از بین رفتن فرایند سنکرون‌شدن شود. حال سنکرون‌کردن فرستنده و گیرنده برای سیستم مخابراتی با یک زمان تاخیر ثابت نامشخص را تعریف می‌کنیم:

تعریف ٤[۲۸]: حالت سیستم گیرنده در زمان t به صورت مجانبی با سیستم فرستنده در زمان $t-\tau_d$ سنکرون می‌گردد، اگر

$$\lim_{t\to\infty}\|x(t-\tau_d) - \hat{x}(t)\| = 0$$

درحالیکه τ_d یک تاخیر زمانی ثابت نامشخص است و $x(t)$ و $\hat{x}(t)$ به ترتیب حالت سیستم گیرنده و فرستنده هستند.

فرض کنیم که یک زمان تاخیر انتشار ثابت نامشخص، τ_d، برای انتقال سیگنال پیام از فرستنده به گیرنده وجوددارد. این بدان معناست که، در زمان $t-\tau_d$، سیگنال انتقال از فرستنده منتقل شده است. سیگنال انتقال تاخیردار توسط گیرنده درزمان t دریافت خواهد شد. سپس سیستم آشوبی (۱۰) در سمت فرستنده به صورت زیر بازنویسی می‌گردد:

$$\dot{\eta}(t-\tau_d) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}\eta(t-\tau_d) + LE(t-\tau_d)$$
$$+ \begin{bmatrix} (\lambda_1+\lambda_2)y(t-\tau_d) \\ -\lambda_1\lambda_2 y(t-\tau_d) - (\lambda_1-\lambda_2)\eta_3 y(t-\tau_d) - 0.5(k+1)(y(t-\tau_d))^3 \\ K(k)(y(t-\tau_d))^2 \end{bmatrix}$$
$$y(t-\tau_d) = \eta_1(t-\tau_d) + E(t-\tau_d)$$

(۲۱)

جاییکه L بردار بهره مشاهده‌گر و $E(t-\tau_d)$ خروجی طرح رمزنگاری است. دراینجا نیز از همان طرح رمزنگاری (۱۱) استفاده می شود. سیستم آشوبی در سمت گیرنده، توسط سیگنال تاخیردار $y(t-\tau_d)$ برای هدف سنکرون کردن درایو

خواهد شد، به نحوی که سیستم (۱۳) به صورت رابطه (۲۲) قابل بازنویسی است:

$$\dot{\hat{\eta}}(t)=\begin{bmatrix}0&1&0\\0&0&0\\0&0&\lambda_3\end{bmatrix}\hat{\eta}(t)+L(y(t-\tau_d)-\hat{y}(t))+\begin{bmatrix}(\lambda_1+\lambda_2)y(t-\tau_d)\\-(\lambda_1\lambda_2+(\lambda_1-\lambda_2)\hat{\eta}_3(t))y(t-\tau_d)-0.5(k+1)(y(t-\tau_d))^3\\K(k)(y(t-\tau_d))^2\end{bmatrix}$$
$$\hat{y}(t)=\hat{\eta}_1(t)$$

(۲۲)

جاییکه $y(t-\tau_d)$ سیگنال دریافت شده و L بردار بهره مشابه با چیزی است که در سیستم فرستنده استفاده شده بود.

اگر سیستم (۲۱) با سیستم (۲۲) سنکرون گردد، $\lim_{t\to\infty}\|x(t-\tau_d)-\hat{x}(t)\|=0$ و داریم: $\hat{\eta}_1(t)\to\eta_1(t-\tau_d)$ و $\hat{\eta}_3(t)\to\eta_3(t-\tau_d)$، پس طرح رمزگشایی متناظر به صورت زیر قابل بازنویسی است:

$$\hat{p}(t)=\underbrace{f(\ldots f(}_{n}f(\hat{E}(t),\underbrace{-\hat{\eta}_3(t)),-\hat{\eta}_3(t)),\ldots,-\hat{\eta}_3(t))}_{n}$$

(۲۳)

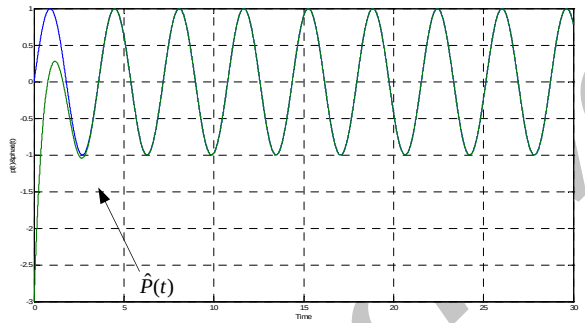
درحالیکه $\hat{p}(t)$ سیگنال پیام بازیابی شده است ، که مشابه با سیگنال پیام اصلی ولی با تاخیر τ_d است. حال ثابت می‌کنیم که، با انتخاب مناسب بردار بهره مشاهده‌گر L، سیستم (۲۲) می‌تواند با (۲۱) همانطوری که در نتیجه ذیل توضیح داده شده است سنکرون گردد.

نتیجه تئوری۲: فرض کنید که سیگنال پیام، $p(t)$ ، از طریق یک سیستم مخابراتی امن شامل یک سیستم فرستنده با سیستم آشوبی (۲۱) و طرح رمزنگاری (۱۱)، و سیستم گیرنده با سیستم آشوبی (۲۲) و طرح رمزگشایی (۲۳) باشد. همچنین یک تاخیر زمانی انتشار نامشخص اما ثابت، τ_d، در طول فرایند انتقال درگیر است. با استفاده از "کلید" مشابه در سیستم فرستنده و گیرنده، سنکرون‌کردن فرستنده و گیرنده قابل دستیابی است، و سیگنال پیام، $p(t)$ ، در سمت گیرنده، با زمان تاخیر τ_d دوباره به صورت کامل بازیابی می‌گردد.

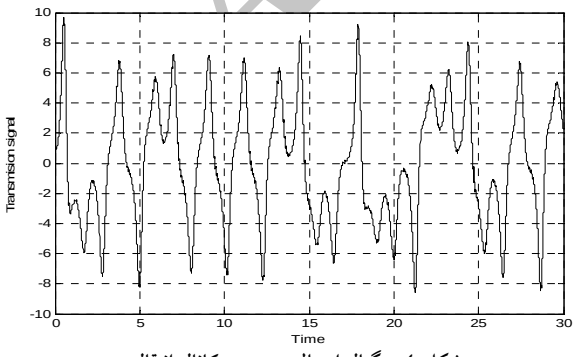
اثبات: کافیست خطای سنکرون کردن را به صورت $\tilde{\eta}(t)=\eta(t-\tau_d)-\hat{\eta}(t)$ تعریف کنیم و بقیه مراحل اثبات مشابه تئوری۲ قابل انجام است.

۴- نتایج شبیه‌سازی

برای بررسی عملکرد سیستم مخابراتی امن پیشنهادی دو نوع پیام که یکی سیگنال سینوسی و دیگری سیگنال صوت است برای شبیه سازی انتخاب شده است. پارامترهای سیستم آشوبی به صورت $\lambda_1=8$ ، $\lambda_2=-16$ ، $\lambda_3=-2$ و $k=0$ تنظیم شده‌اند. سیگنال پیام به عنوان یک تابع سینوسی $P(t)=\sin(0.5\pi t)$، و بردار بهره به صورت $L=[5\ \ 8\ \ 0]^T$ انتخاب می‌شود، با بکار بردن این بهره‌ها ماتریس S در (۱۹) هرویتز است. برای هدف رمزنگاری و رمزگشایی، $h=10$ و $n=30$ برای رمز شیفت‌دهنده nتایی (۱۱)و (۱٤) انتخاب شده‌اند. شکل (۳) سیگنال رمزنشده اصلی $P(t)$ و سیگنال دریافت شده $\hat{P}(t)$ را با استفاده از کلید مشابه در گیرنده و فرستنده نشان می‌دهد. شکل (٤) سیگنال انتقال داده شده آشوبی را نشان می‌دهد. در مرحله بعد بخشی از یک سیگنال صدا را با پسوند(Wave.) به عنوان سیگنال پیام انتخاب کرده‌ایم .در این شبیه‌سازی از "کلید" مشابه برای فرستنده و گیرنده استفاده کرده‌ایم . شکل (۵) سیگنال صدای اصلی و صدای بازیابی شده را نشان می‌دهد.

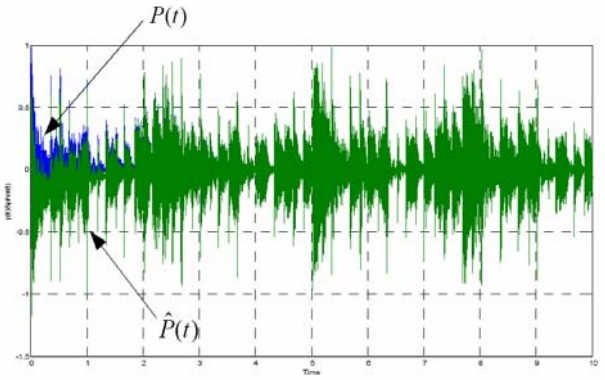


شکل ۳ سیگنال پیام ارسالی و سیگنال پیام بازیابی شده با کلید مشابه

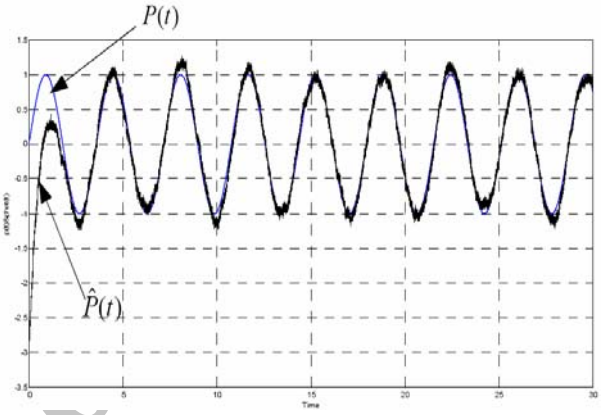


شکل ٤ سیگنال ارسالی بر روی کانال انتقال

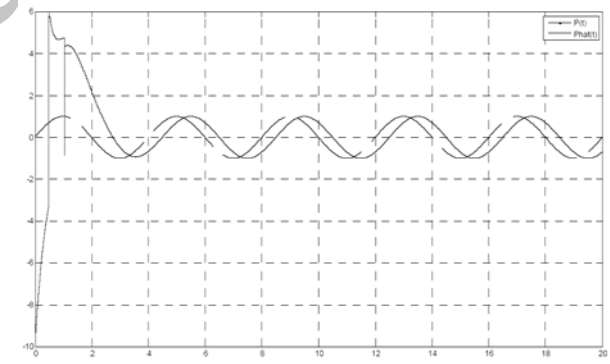
در شبیه سازی بعدی تاثیر نویز کانال انتقال بر روی بازسازی سیگنال پیام مورد بررسی قرار گرفته است. در این راستا با استفاده از پیام سینوسی مورد استفاده در شبیه سازی اول و پارامترهای مشابه با آن و نویز کانال به صورت گوسی با



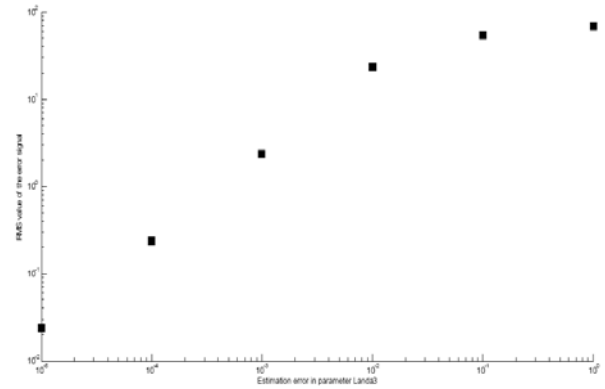
شکل ۵ سیگنال صوت ارسالی و سیگنال بازیابی شده



شکل٦ سیگنال ارسالی و بازیابی شده در حضور نویز کانال



شکل ۷ سیگنال ارسالی و بازیابی شده در سیستم مخابراتی با تاخیر زمانی



شکل ۸ خطای تخمین در پارامتر λ_3

واریانس 10^{-3} شبیه‌سازی را انجام داده‌ایم. شکل(٦) سیگنال ارسالی و بازیابی شده با توجه به نویز کانال را نشان می دهد. با توجه به شکل می‌توانیم ببینیم که مقاومت طرح پیشنهادی در مقابل نویز کانال مناسب است و بازسازی به خوبی انجام می‌گیرد.برای توصیف عملکرد سیستم مخابراتی امن که با یک تاخیر زمانی نامشخص در طول فرایند انتقال درگیر است، زمان تاخیر به صورت $\tau_d = 0.5$ (sec) در نظر گرفته شده است.با استفاده از "کلید" مشابه برای هر دو سیستم فرستنده و گیرنده شبیه‌سازی انجام شده است. شکل (۷) سیگنال پیام اصلی $p(t)$ و سیگنال بازیابی شده $\hat{p}(t)$ را نشان می‌دهد.با توجه به شکل می‌توان دید که، وقتی یکبار سنکرون‌شدن بین سیستم‌های فرستنده و گیرنده حاصل شود، سیگنال پیام اصلی p(t) با موفقیت ولی با تاخیر τ_d قابل بازیابی است.

۵- آنالیز امنیت سیستم

از نقطه نظر رمزنگاری، براساس[۲۰]، امنیت سیستم رمزنگاری تابعی از دو چیز است:قدرت الگوریتم و طول کلید. در بخش ۲، مشخصات امنیت در طرح سنکرون‌کردن آشوب برای سیستم‌های مخابراتی امن از نقطه نظر تئوری کنترل، مورد بحث قرار گرفت. از آنجایی که سیستم مخابراتی امن پیشنهاد شده در طرح سنکرون کردن، هم دارای مشخصات امن ضد مقاوم و هم امن ضد تطبیقی است، بنابراین می‌تواند سیستم را از حمله مهاجمان حفظ کند. این بدان معناست که الگوریتم استفاده شده در سیستم مخابراتی امن پیشنهاد شده به اندازه کافی مناسب است. اکنون توجه خود را به آنالیز مشخصه امنیت دیگری از سیستم مخابراتی امن پیشنهاد شده که طول کلید نامیده می‌شود معطوف می‌کنیم.

مجموعه "کلید" مورد استفاده در طرح مخابراتی همان پارامترهای سیستم آشوبی به صورت $Key \equiv \{k, \lambda_1, \lambda_2, \lambda_3\}$ هستند. طرح مخابراتی امن پیشنهاد شده را با بکارگیری یک "کلید" غلط در سیستم گیرنده با خطاهای مختلف در تخمین تنظیمات پارامتر شبیه‌سازی کرده‌ایم. سیگنال پیام به صورت تابع سینوسی $P(t) = \sin(0.5\pi t)$ انتخاب شده است. با محاسبه مقدار نرم RMS خطای بازسازی سیگنال پیام و با توجه به اینکه فقط یکی از پارامترها در فرستنده و گیرنده متفاوت انتخاب شده است شبیه سازی انجام شده است.پارامترهای سیستم و بردار بهره L مانند شبیه‌سازی اول انتخاب شده است.شکل (۸) اثر خطای تخمین در پارامتر λ_3 و نرم RMS خطای ایجاد شده را

بر روی نمودار لگاریتمی نشان می‌دهد. شکل (۸) نشان می‌دهد که خطای تخمین می‌دهد که خطای تخمین پارامتر λ_3 به مقدار کم می‌دهد کهمی‌دهد که خطای تخمین پارامتر λ_3 به مقدار کم 10^{-5} باعث خطای رمزگشایی نسبتا بزرگی می‌گردد. با شبیه‌سازی‌های مشابه برای پارامترهای دیگر، این مقدار برای k برابر 10^{-6} و برای پارامترهای $\lambda_{1,2}$برابر با 10^{-5} می‌گردد. این بدان معناست که، از نقطه نظر رمزنگاری، اندازه فضای کلید سیستم مخابراتی امن پیشنهاد شده از $10^6 \times 10^5 \times 10^5 \times 10^5 = 10^{21} \approx 2^{69}$ کمترنخواهد بود [۲۹].

با درنظر گرفتن جستجوی بروت–فورس[1] هر کلید ممکن سیستم مخابراتی امن موثرترین روش در برابر شکسته شدن است. جدول (۱) زمان مورد نیاز برای اینکه سیگنال پیام با فضای کلید داده شده با استفاده از یک ماشین جستجویی که در هر ثانیه 100 میلیون کلید را تولید می‌کند بازیابی شود خلاصه کرده است. با توجه به جدول فوق طول کلید سیستم مخابراتی امن پیشنهاد شده از نظر رمزنگاری مناسب است. با توجه به این موضوع، سیستم مخابراتی امن پیشنهاد شده می‌تواند سطح نسبتا بالایی از امنیت را برای انتقال سیگنالهای پیام به ما بدهد.

۶- نتیجه گیری

در این مقاله یک طرح مخابراتی امن جدید ارائه گردید که در مقایسه با مقالات قبلی از نقطه نظر امنیت الگوریتم خواص امن ضد مقاوم و امن ضد تطبیقی را برآورده می‌سازد. از طریق تئوری (۲) امکان سنکرون شدن فرستنده و گیرنده اثبات گردید. نتایج شبیه‌سازی طرح پیشنهادی بر روی سیگنال سینوسی و سیگنال صوت با موفقیت انجام گرفت. همچنین نتایج تئوری و شبیه‌سازی با توجه به تاخیر انتشار ثابت بین فرستنده و گیرنده انجام گرفته است. پس از آن مقاومت طرح مخابراتی پیشنهادی در برابر نویز گوسی با واریانس 10^{-3} با استفاده از شبیه‌سازی بررسی گردید و نتایج بسیار خوبی در بازیابی سیگنال پیام حاصل شد. در انتها آنالیز امنیت سیستم پیشنهادی بر روی پارامتر تاثیرگذار دیگر یعنی طول "کلید" انجام گرفت و طول کلیدی برابر با 2^{69} بدست آمد. با توجه به روش جستجوی بروت–فورس که در جدول(۱) ارائه گردیده است این طول کلید برای یک سیستم رمزنگار بسیار مناسب است.

جدول ۱زمان‌های جستجوی کلید بروت–فورس
برای اندازه‌های مختلف کلید

اندازه کلید	2^{40}	2^{56}	2^{64}	2^{69}
زمان مورد نیاز	۳/۱ ساعت	۳٤/٥ روز	٥٨٤٩/٤ سال	۳۱۷۱۰۰ سال

1. Brute-force

مراجع

[1] Lasota A. and M.C.Mackey, “Chaos,Fractals, and Noise- Stochastic Aspects of Dynamics .” Springer-Verlag, Second Edition, New York, 1997

[2] Robert C.Hilborn, “Chaos and Nonlinear Dynamics”,Second Edition,Department of Physics Amherst Collage,2000

[3] Kocarev L., G.Jakimoski, T.Stojanovski, and U.Parlitz, “From Chaotic Maps to Encryption Schemes.” In Proceedings IEEE International Symposium Circuits and Systems, Vol.4, pp. 514-517, 1998

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Matthews R.A.J., “On the Derivation of a Chaotic Encryption Algorithm. ” Cryptologia XIII, Vol .1 , pp. 29-42, 1989

[7] Habutsu H.,Y.Nishio,I.Sasase and S.Mori, “A Secret Key Cryptosystem by Iterating a Chaotic Map,Advances in Cryptology ”,proceedings of EuroCrypt91,Vol .547,pp.127-140,1991

[8] Masuda N., and K.Aihara, “Cryptosystems with Discretized Chaotic Maps.” IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, Vol .49 , pp. 28-40, 2002

[9] Li S., X.Mou, and Y.Cia, “Pseudo-Random Bit Generator Based on Couple Chaotic Systems and its Application in Stream-Ciphers Cryptography. ”, Progress in Cryptology-INDDOCRYPT 2001,Lecture Notes in Computer Science, Vol .2247 , pp. 316-329, 2001

[10] Pecora L.M. and T.L.Carroll , “ Synchronization in Chaotic Systems”, Physical Review Letters , Vol.64,pp.821-824,1990

[11] Chua L.O., L.J. Kocarev, K.Eckert, and M.Itoh, “Experimental Chaos Synchronization in Chua Circuit.”, International Journal of Bifurcation and Chaos, Vol .2 , pp. 705-708, 1992

[12] Oppenheim A.V., G.W.Wornell, S.H.Isabelle, and K.M.Cuomo, “Signal Processing in the Context of ChaoticSignals.”, In Proceedings IEEE ICASSP, Vol .4 , pp. 117-120, 1992

[13] Halle K.S., C.W.Wu, M.Itoh, and L.O.Chua, “Spread Spectrum Communication Through Modulation of Chaos.”, International Journal of Bifurcation and Chaos, Vol .3 , pp. 469-477, 1993

[14] Wu C.W., and L.O.Chua, “A Unified Framework for Synchronization and Control of Dynamical Systems.”, International Journal of Bifurcation and Chaos, Vol .4 , pp.979-998, 1994

[15] Grassi G. and S.Mascolo ,“Non-Linear Observer Design to Synchronize Hyper-chaotic Systems via a Scalar Signal”, IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, Vol .44(10),pp.1011-1014,1997

[16] Liao T.L. and N.S.Huang ,“An Observer-Based Approach for Chaotic Synchronization with Application to Secure Communication”, IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, Vol .46,pp.1144-1150,1999
[17] Pecora L.M. and T.L.Carroll , “ Synchronization in Chaotic Systems”, Physical Review Letters , Vol.64,pp.821-824,1990
[18] Lian K.Y., P.Liu, T.S.Chiang, “Adaptive Synchronization Design for Chaotic Systems via a Scalar Driving Signal.”, IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, Vol .49, pp.17-27,2002
[19] Kolumban G., M.P.Kennedy, and L.O.Chua, “The Role of Synchronization in Digital CommunicationUsing Chaos—Part I:Fundamentals of Digital Communications.”, IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, Vol .44, pp.927-936, 1997
[20] Murali K., H. Yu, V.Varadan, H.Leung ,“Secure Communication Using a Chaos Based Signal Encryption Scheme.”, IEEE Transactions on Consumer Electronics, Vol .47, pp.709-714, 2001
[21] Short k., “Unmasking a modulated Chaotic Communication Scheme. ” International Journal of Bifurcation and Chaos, Vol .6 , pp. 367-375, 1996
[22] Yang T., C.W. Wu, and L.O. Chua,“Cryptography Based on Chaotic Systems”, IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, Vol .44,pp.469-472,1997
[23] Grassi G. and S.Mascolo ,“A System Theory Approach for Designing Cryptosystems Based on Hyperchaos.”, IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, Vol .46(9),pp.1135-1138,1999
[24] Suykens J.A.K., P.F. Curran, and L.O. Chua, “Robust Synthesis for Master-Slave Synchronization of Lure Systems.”, IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications, Vol .46 , pp. 841-850, 1999
[25] Celikovsky S. and G.Chen,“Secure Synchronization of a Class of Chaotic Systems From a Nonlinear Observer Approach”, IEEE Transactions on Automatic Control, Vol .50,pp.76-82,2005
[26] Kamen E.W., “Linear Systems with Commensurate Time Delays:Stability and Stabilization Independent of Delay”, IEEE Transactions on Automatic Control.,Vol. 27, pp.367-375,1982
[27] Chen H. and J.Liu, “Open-Loop Chaotic Synchronization of Injection-Locked Semiconductor Lasers with Giagahertz Range Modulation.”, IEEE Journal of Quantum Electronics,Vol. 36, pp.27-34, 2000
[28] Jiang G.P., W.X.Zheng and G.Chen, “Global Chaos Synchronization with Channel Time-Delay.”, Chaos Solution and Fractals,Vol. 20, pp.267-275, 2004
[29] Schneier B. “Applied Cryptography : Protocols , Algorithms ,and Source Code in C”, John Wiley and Sons ,Inc.,New York ,second edition,1996.