بهبود عملکرد سامانه‌های کنترل از طریق شبکه با استفاده از یک روش رمزنگاری جدید

سیدعلی مصباحی‌فرد[(۱)] - بنیامین حق‌نیاز جهرمی[(۱)] - پویا حاجبی[(۲)] - سید محمدتقی المدرسی[(۳)]

(۱) کارشناس ارشد- دانشکده مهندسی برق و کامپیوتر، دانشگاه یزد

(۲) دانشجوی دکتری- دانشکده مهندسی برق و کامپیوتر، دانشگاه یزد

(۳) استادیار- دانشکده مهندسی برق و کامپیوتر، دانشگاه یزد

تاریخ دریافت: تابستان ۱۳۹۲ تاریخ پذیرش: زمستان ۱۳۹۳

خلاصه: سامانه‌های کنترل از طریق شبکه شامل آن دسته از سامانه‌های کنترلی می‌باشد که در آن‌ها ارتباط میان کنترل‌گر و دستگاه از طریق شبکه‌های مخابراتی برقرار است. اولین و بزرگترین چالش در سامانه‌های کنترل از طریق شبکه، مسأله تأخیر زمانی می‌باشد که افزایش مقدار آن، به شدت عملکرد سامانه کنترلی را تحت تأثیر قرار می‌دهد. از جمله مسائل مهم دیگر در سامانه‌های کنترل از طریق شبکه مسائل امنیتی است، زیرا امکان دسترسی افراد مختلف به شبکه مخابراتی بخصوص اینترنت، زمینه حملات خطرناکی مانند حمله تقلب را به این سامانه‌ها فراهم می‌آورد. از این رو ارائه روش‌هایی که بتواند مقدار تأخیر زمانی را کاهش داده و امنیت سامانه را افزایش دهد، همواره در این زمینه مورد توجه بوده است. آنچه در این مقاله ارائه می‌شود یک روش رمزنگاری متقارن و متناسب با حجم کم داده برعلیه حملات تقلب است که ضمن برآورده کردن توأم یکپارچگی و محرمانگی داده، تأخیر زمانی کمتری را نسبت به سایر روش‌های رمزنگاری دارد و می‌تواند در مقابل حملات تقلب، عملکرد سامانه کنترلی را بهبود بخشد.

کلمات کلیدی: امنیت، تأخیر زمانی، حمله تقلب، رمزنگاری، سامانه‌های کنترل از طریق شبکه.

۱- مقدمه

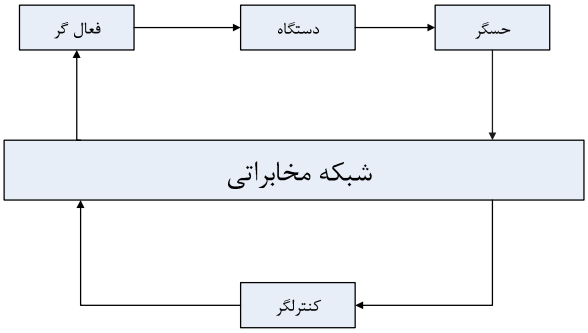
سامانه‌های کنترل از طریق شبکه[1]، به منظور کنترل دستگاه‌ها از طریق شبکه‌های مخابراتی مانند اترنت[2]، به کار می‌روند. در این‌گونه سامانه‌های کنترلی، ارتباط بین کنترل‌گر و دستگاه از طریق شبکه های مخابراتی صورت می‌گیرد. شمای کلی یک سامانه‌ی کنترل از طریق شبکه در شکل (۱) نشان داده شده است. سامانه‌های کنترل از طریق شبکه به دلیل گستردگی شبکه‌های مخابراتی نظیر اینترنت در سراسر جهان، مزایایی از قبیل کاهش هزینه نصب و نگهداری، کنترل همزمان چند دستگاه از یک مکان، سهولت در گسترش‌پذیری سامانه را به همراه داشته است.

سامانه‌های کنترل از طریق شبکه، کاربردهای فراوانی در حوزه‌های پزشکی، صنعتی و علوم فضایی پیدا کرده است. از جمله کاربردهای این‌گونه سامانه‌های کنترلی، شبکه‌های حس‌گر متحرک، سامانه کنترل خودکار بزرگراه‌ها، کنترل وسایل نقلیه بدون سرنشین، انجام عمل جراحی از راه دور و سامانه‌های "کنترل نظارتی و اکتساب داده‌ها[3]" را می‌توان نام برد [۱].

قابلیت دست‌یابی به سیگنال‌های کنترلی در شبکه به ویژه زمانی که از اینترنت به عنوان شبکه ارتباطی استفاده می‌شود، معیاری حیاتی در امنیت سامانه‌های کنترل از طریق شبکه به حساب می‌آید.

امنیت در سامانه‌های کنترل از طریق شبکه به دلیل ارتباط تنگاتنگ آن با ابزارآلات و مکان‌های حیاتی، نه تنها شامل مسائلی همچون محافظت در مقابل دزدی داده و یا تغیر غیرمجاز داده‌ها می‌شود، بلکه فراتر از آن باید شامل ایجاد شبکه‌های پشتیبان مخابراتی، سامانه‌های تشخیص نفوذ، سیستم‌عامل‌های مناسب، آنتی ویروس‌های مناسب و سایر اقدامات امنیتی نرم‌افزاری و سخت‌افزاری و همچنین بازبینی مستمر و برنامه‌ریزی‌شده سامانه‌های سخت‌افزاری و نرم‌افزاری باشد.

نویسنده مسئول: سید علی مصباحی فرد - یزد، دانشگاه یزد ، sam.mesbah@stu.yazd.ac.ir



شکل (۱): شمای کلی یک سامانه‌ی کنترل از طریق شبکه
Fig. (1): Schematic of a networked control system

به‌علاوه می‌بایست قبل از مرحله اجرا تمام اثرات ناشی از خرابی شبکه مخابراتی یا حملات عمدی و غیرعمدی سایبری ممکن به سامانه کنترلی، مورد بررسی قرارگیرد [۲-۳]. Byres و دیگران به بررسی موارد مختلف اثرگذار بر امنیت این شبکه‌ها پرداخته‌اند و روند ارزیابی امنیتی را به صورت ارزیابی ابزارهای انسانی، ارزیابی شبکه، ارزیابی دستگاه‌ها بررسی کرده‌اند [۴].

Amin و دیگران با استفاده از نظریه بازی به بررسی اثرات حمله به شبکه پرداخته‌اند و برخی از راهبُردهایی را که منجر به تعادل سامانه می‌شود، ذکر کرده‌اند [۵]. Ke-Ya Yuan و دیگران با اجرای روش رمزنگاری DES بر روی سخت‌افزار FPGA به بررسی اثر آن بر خروجی یک موتور DC که از طریق شبکه کنترل می‌شود، پرداخته‌اند [۶]. آن‌ها نشان داده‌اند که سامانه سخت‌افزاری DES[4] بر پایه FPGA، تقریباً هیچ اثری بر خصوصیات بلادرنگ سامانه کنترل از طریق شبکه ندارد. Pang و دیگران در [۷-۸] به بررسی اثر حملات تقلب بر عملکرد یک موتور DC پرداخته‌اند و روشی را برای مقابله با آن پیشنهاد نموده‌اند. روش آن‌ها مبتنی بر استفاده از روش درهم‌ریز MD5 و رمزنگاری DES داده برای تشخیص تغییر داده و تشخیص تقلب در هویت فرستنده است. علاوه بر آن در پژوهش مذکور، قبل از رمزنگاری و درهم‌ریزی، برای تشخیص بازتکرار داده یک برچسب زمانی (که نمایانگر زمان ارسال پیام توسط فرستنده است) به بسته‌ی داده، اضافه می‌شود. در [۹] ضمن بررسی اثر تأخیر ناشی از سه روش رمزنگاری DES و DES3 و AES[5] بر سامانه کنترل از طریق شبکه، با استفاده از تغییر دادن بهره حلقه بسته سامانه کنترلی، اثرات مخرب ناشی از آن بر روی برخی شاخص‌های عملکرد کنترلی مانند میزان فراجهش و زمان نشست سامانه، بهبود داده شده و حتی سامانه از حالت ناپایدار به حالت پایدار درآمده است. در [۱۰-۱۱] به بررسی تحلیلی و آماری میزان کاهش شاخص عملکرد کنترلی در مقابل افزایش امنیت ناشی از روش‌های رمزنگاری پرداخته شده است. در این پژوهش با افزایش امنیت روش رمزنگاری، کلید رمز پیچیده‌تر شده و در نتیجه تأخیر زمانی بیشتری به سامانه کنترل از طریق شبکه اعمال می‌کند. این امر باعث کاهش شدید شاخص عملکرد کنترلی ناشی از تأخیر رمزنگاری می‌شود. بنابراین ارائه راهکاری که بتواند ضمن حفظ شاخص عملکرد کنترلی، امنیت آن را نیز تا حد زیادی بالا ببرد از مسائل چالش‌برانگیز حوزه امنیتی در سامانه‌های کنترل از طریق شبکه می‌باشد. در این مقاله یک روش جدید رمزنگاری ارائه شده که در مقایسه با سایر روش‌های رمزنگاری به‌کار رفته در سامانه‌های کنترل از طریق شبکه، دارای تأخیر زمانی کمتر و همچنین امنیت بالاتر می‌باشد. شاخص عملکرد این مقاله در روش پیشنهادی تا ۳۸٪ نسبت به روش‌های پیشین بهبود یافته است.

در بخش (۲) این مقاله مفهوم سامانه‌های کنترل از طریق شبکه توضیح داده خواهد شد. روش رمزنگاری پیشنهادی در بخش (۳) توضیح داده می‌شود. در بخش (۴) روش رمزنگاری پیشنهادی بر روی یک موتور DC پیاده‌سازی می‌شود و با سایر روش‌های رمزنگاری به کار رفته در سامانه‌های کنترل از طریق شبکه مقایسه می‌شود. بخش (۵)، نتایج و زمینه‌های پژوهشی آینده را بیان خواهد کرد.

۲- سامانه‌های کنترل از طریق شبکه

به طور کلی همان‌طور که در شکل (۱) نشان داده شده، سامانه‌های کنترل از طریق شبکه یک نمونه از "سامانه‌های کنترلی توزیع‌شده[6]" می‌باشد که در آن حس‌گر، فعال‌گر و کنترل‌گر توسط شبکه‌های مخابراتی دیجیتال[7] باندمحدود[8] به هم متصل می‌شوند[۱۲]. ابتدا سیگنال کنترلی به دست‌آمده از کنترل‌گر، قبل از ارسال رمزنگاری می‌شود. سیگنال مورد نظر پس از انتقال از طریق شبکه، به فعال‌گر می‌رسد که ابتدا رمزگشایی شده و سپس از طریق یک مبدل، داده‌های دیجیتال به آنالوگ تبدیل می‌شود و به دستگاه اعمال می‌گردد. پس از آن خروجی آنالوگ دستگاه توسط حس‌گر اندازه‌گیری شده و به سیگنال دیجیتال تبدیل می‌شود. این سیگنال قبل از ارسال، رمزنگاری شده و از طریق شبکه ارسال می‌شود، سپس سیگنال‌های دریافتی توسط کنترل‌گر رمزگشایی می‌شود و با سیگنال مرجع مقایسه شده و سیگنال خطا را می‌سازد. در یک چرخه سیگنال کنترلی، با توجه به مطالب گفته شده، هر کدام از فرایندهای رمزنگاری و رمزگشایی، دو بار اجرا می‌شود که باعث تحمیل چهار تأخیر زمانی اضافی علاوه بر تأخیر شبکه در کل سامانه می‌شود، این چهار تأخیر ایجادشده در اثر رمزنگاری را تأخیر رمزنگاری در سامانه‌های کنترل از طریق شبکه می‌نامند. به علت وجود شبکه مخابراتی برای ارتباط بین اجزای سامانه کنترل از طریق شبکه، تحلیل و طراحی این سامانه‌ها دچار مشکلاتی می‌شود. دو چالش مهم در این سامانه‌ها، تأخیر زمانی تصادفی[9] و از دست‌رفتن بسته‌های[10] داده در شبکه می‌باشد[۱۳]. از زمان نمونه-برداری خروجی دستگاه توسط حس‌گر تا زمان اعمال سیگنال کنترلی توسط فعال‌گر، تأخیرهای گوناگونی رخ می‌دهد. در سامانه‌های کنترل از طریق شبکه، تأخیر زمانی از دو بخش ثابت و متغیر تشکیل شده-است. این تأخیرها شامل تأخیر شبکه، تأخیر رمزنگاری و تأخیر

پردازش می‌باشد. تأخیر شبکه شامل تأخیر دستیابی به شبکه (مدت زمانی که طول می‌کشد تا اجازه دستیابی به شبکه حاصل شود) و تأخیر انتشار سیگنال در شبکه (مدت زمانی که طول می‌کشد تا سیگنال از کانال مخابراتی عبور کند) می‌باشد که به ویژگی‌های تصادفی شبکه مانند پروتکل شبکه، ترافیک شبکه، تعداد گره‌های شبکه و سیاست مسیریابی شبکه در روترها بستگی دارد و از دسته تأخیرهای تصادفی است. تأخیر پردازش نیز به علت عملیات پردازشی در کنترل‌گر به وجود می‌آید. تأخیر رمزنگاری و پردازش از دسته تأخیرهای ثابت می‌باشد. این تأخیرها در عملکرد سامانه کنترلی تأثیر بسزایی دارد و می‌تواند باعث ناپایداری سامانه کنترل از طریق شبکه شود. یکی از راه‌های بهبود عملکرد سامانه‌های کنترل از طریق شبکه، استفاده از روش رمزنگاری مناسب می‌باشد به‌گونه‌ای که تأخیر زمانی کمتری به سامانه تحمیل کند و باعث بهبود عملکرد سامانه کنترل از طریق شبکه شود. روش رمزنگاری پیشنهادی در این مقاله با تحمیل تأخیر زمانی کمتر به سامانه، باعث بهبود عملکرد سامانه کنترلی شده است.

۳- روش رمزنگاری پیشنهادی

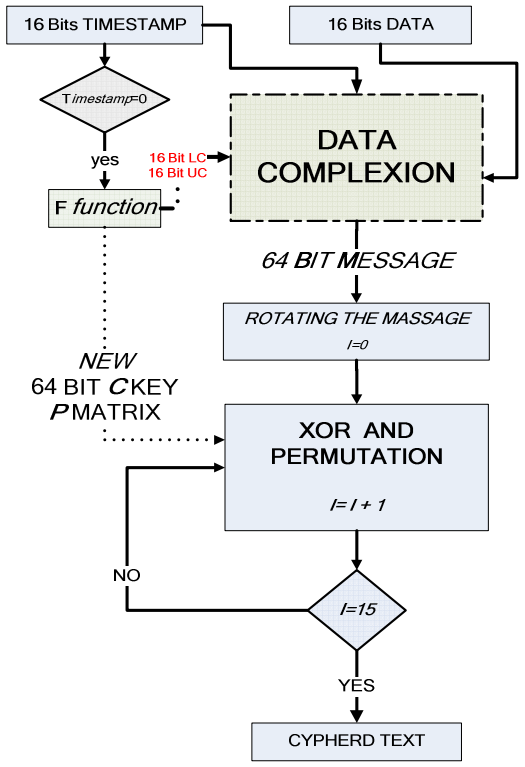
چون اکثر داده‌های کنترلی دارای حجم کمی می‌باشند، معمولاً ۱۶ بیت داده برای آن در نظر گرفته می‌شود که معادل عددی بین ۰ تا ۶۵۵۳۵ و یا بین ۳۲۷۶۸- تا ۳۲۷۶۷ است. این حجم داده، برای بسیاری از کاربردهای کنترلی کافی است. همچنین فرض شده است که گیرنده و فرستنده دارای فرکانس ساعت یکسان باشد.

ابتدا از یک دنباله کلید اولیه ۹۶ بیتی IK0، کلید ۹۶ بیتی جدید IK[11] ساخته می‌شود. سپس از این کلید در هر بار صفر شدن شمارنده برچسب زمانی[12]، کلید ۹۶ بیتی رمزنگاری با نام SK[13] تولید می‌شود.

روش پیشنهادی یک رمزنگاری متقارن با کلید SK است که این کلید در طول زمان تغییر می‌کند و تغییر آن منجر به تغییر برخی پارامترهای دیگر مانند تغییر اندازه چرخش‌ها و تغییر ماتریس جایگشت P می‌گردد.

همانطور که در شکل (۲) نشان داده شده است، ورودی‌های قسمت رمزکننده، یک داده ۱۶ بیتی و یک برچسب زمانی۱۶ بیتی هستند و خروجی نهایی، یک دنباله ۶۴ بیتی است که به معنای ۳۲ بیت افزونگی داده می‌باشد.

کلید ۹۶ بیتی SK به سه کلید، شامل دو کلید ۱۶ بیتی LC و UC و یک کلید ۶۴ بیتی C تقسیم می‌شود. کلیدهای LC و UC جداگانه طبق رابطه (۱) بیت به بیت، به داده D اعمال می‌گردد و در نتیجه از کنار هم قرار دادن خروجی‌های آن‌ها، یک دنباله ۳۲ بیتی تشکیل می‌گردد. چنین عملی بر روی دنباله ۱۶ بیتی برچسب زمانی نیز انجام می‌گردد و در نتیجه پیامی با طول ۶۴ بیت حاصل می‌گردد و توسط کلید C گام نهایی رمزنگاری بر روی آن انجام می‌شود.



شکل (۲): شمای کلی روش رمزنگاری پیشنهادی

Fig. (2): Schematic of proposed encryption algorithm

این خروجی با دو معیار مختلف، به داده ورودی وابسته است، از این رو برای تشخیص یکپارچگی از آن استفاده می‌گردد. این عملیات برخلاف عملیات درهم‌ریزی، برگشت‌پذیر است و بخشی از روند رمزنگاری به حساب می‌آید.

$$\begin{cases} OUTL(i) = LC(i) \oplus D(i) \oplus OUTL(i-1) \\ OUTU(i) = LU(i) \oplus D(i) \oplus D(i-1) \end{cases} \quad (۱)$$

در رابطه(۱)، i شماره بیت در دنباله داده می‌باشد و بین ۱ تا ۱۶ تغییر می‌کند.

در مرحله بعد پیام به ۱۶دسته ۴ بیتی تقسیم می‌شود و دنباله ۶۴ بیتی پیام وارد یک چرخه رمزنگاری با ۱۶ بار تکرار می‌شود. سپس در هر بار تکرار، با C، XOR می‌شود و ماتریس جایگشت P به آن اعمال می‌گردد. در هر مرحله، C به اندازه N-i به راست می‌چرخد که I شماره حلقه است و بین صفر تا ۱۵ تغییر می‌کند.

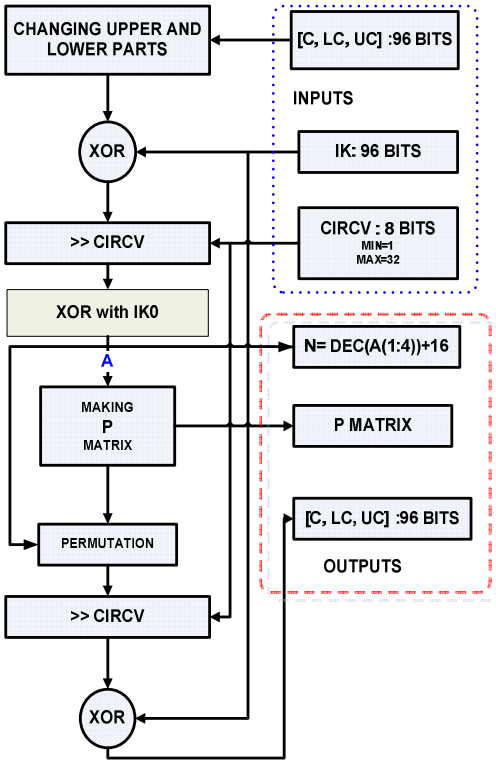
مطابق شکل (۳) تابع F مسئول ساختن کلیدهای IK و SK و ماتریس جایگشت است و دارای دو ورودی ۹۶ بیتی است. یکی از این دو کلید، کلید اولیه‌ای می‌باشد که در اولین ارتباط کنترلی بین کنترل‌گر و دستگاه ایجاد می‌شود و ورودی دوم، کلید تولید شده در مرحله قبل است. به علاوه یک ورودی ۸ بیتی CIRCV با مقدار بین ۱و ۳۲ نیز وجود دارد که مقدار آن فقط موقع ساختن کلید IK بر اساس ورودی‌ها تغییر می‌کند. خروجی تابع F شامل یک دنباله ۹۶ بیتی شامل کلید

جدید SK، یک عدد ۸ بیتی N و ماتریس جایگشت P است. مقدار N و ماتریس P به ورودی‌ها وابسته است.

در تابع F ابتدا جای ۴۸ بیت بالایی و پایینی دنباله ورودی SK عوض می‌شود. سپس با مقدارIK، XOR می‌شود و به اندازه CIRCV به راست می‌چرخد و سپس با مقدارIK0، XOR می‌شود. خروجی این مرحله را A می‌نامیم. مقدار N در این مرحله از مقدار ۴ بیت اول A (به علاوه ۱۶) به دست می‌آید که مقداری بین ۱۶ تا ۳۱ است. ماتریس جایگشت P نیز در همین قسمت ساخته می‌شود. بعد از ساختن P آن را بر A اعمال می‌کنیم. خروجی را به اندازه CIRCV به راست می‌چرخانیم و آنگاه در IK، XOR می‌کنیم. برای ساختن اولین کلید هر دو ورودی۹۶ بیتی را برابر SK در نظر می‌گیریم. مطابق شکل (۴) تابعی که مخصوص تولید ماتریس جایگشت P است با استفاده از دو مقدار اولیه که یکی (Q) ناشی از بیت‌های ۹۳ تا ۹۶ دنباله A و دیگری (I) ناشی از بیت‌های ۸۹ تا ۹۲ دنباله A هستند، مقادیر عناصر ماتریس جایگشت را تولید می‌کند. برای این کار در یک چرخه، مقدار باقیمانده مجموع دو متغیرهای I و Q بر عدد ۱۶ به علاوه یک با حذف حالت‌های تکراری به عنوان عناصر ماتریس تعیین می‌شود. مقدار I در هر دور یک واحد افزایش می‌یابد و مقدار Q با مقدار عنصر جدید ماتریس جایگزین می‌شود.

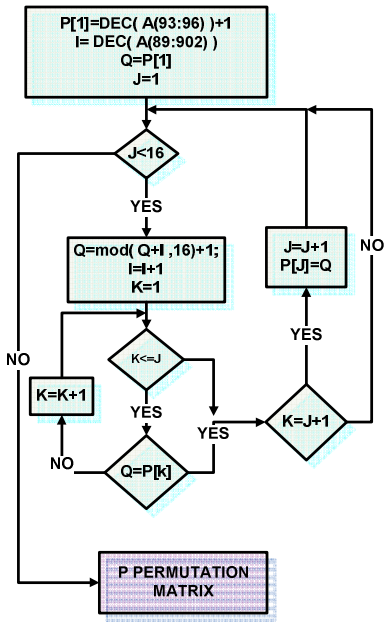
این‌گونه رمزنگاری با تغییر دادن کلید رمزنگاری در طول زمان منجر به تغییر خروجی حتی با وجود ورودی یکسان می‌گردد و چون عملیات تغییر کلید، بدون رد و بدل شدن داده میان گیرنده و فرستنده صورت می‌گیرد، به‌طور عملی شناسایی زمان تغییر کلید غیرممکن است. در مورد حمله جستجوی فراگیر[۱۴] نیز با فرض نامشخص بودن ورودی، تعداد دنباله کلیدهای اولیه $۲^{۹۶}$ حالت مختلف است و تعداد حالات ورودی نیز $۲^{۳۲}$ می‌باشد. پس در حالت کلی تعداد حالت‌ها برای پیدا کردن SK عدد $۲^{۱۲۸}$ است که عددی نسبتاً بزرگ است و حتی اگر شکسته شود مستقیماً باعث تشخیص کلیدهای IK و IK0 نمی‌گردد. البته اگر مهاجم نتواند زمان تغییر کلید را بفهمد تشخیص کلید در حال استفاده به دلیل تغییر دائمی آن کار مشکلی است. برای کاهش احتمال تشخیص زمان تغییر کلید، مقدار اولیه بر چسب زمانی هر بار با مقدار ۱۶ بیت اول از دنباله کلید SK پر می‌شود.

روش رمزنگاری پیشنهادی، به دلیل نداشتن توابع غیر خطی، استفاده از توابع منطقی ساده XOR و عدم ساختن کلید در هر چرخه دارای پیچیدگی کم‌تری نسبت به روش‌های AES و DES می‌باشد و در نتیجه تأخیر زمانی آن کمتر است. امنیت در روش رمزنگاری پیشنهادی از طریق وابستگی ماتریس جایگشت و مقدار چرخش به راست‌ها بر اساس کلید ورودی به دست می‌آید.



شکل (۳): تابع F

Fig. (3): F function



شکل (۴): روش تولید ماتریس جایگشت P

Fig. (4): Generation algorithm of Permutation Matrix P

۴- نحوه اجرای روش رمزنگاری

در این مقاله برای مقابله با حملات تقلب از شیوه‌ای شبیه به"سازوکار انتقال امن" نظیر [۷-۸]، استفاده شده است. ابتدا به بررسی یکپارچگی داده پرداخته می‌شود و در صورتی که داده از یکپارچگی برخوردار باشد با استفاده از برچسب زمانی، داده‌های جدید از داده‌های قدیمی جدا می‌شود و به سامانه اعمال می‌گردد. برای بررسی یکپارچگی به جای به‌کارگیری روش‌های درهم‌ریز، رابطه‌ی (۱) به کار رفته است. از تساوی نتایج ناشی از OUTL و OUTU در گیرنده، یکپارچگی داده نتیجه می‌شود.

روش رمزنگاری پیشنهادی در نرم‌افزار MATLAB بر روی یک رایانه ۳۲ بیتی با سیستم‌عامل ویندوز ۷ اجراشده و سپس با اجرای مکرر، زمان رمزنگاری با میانگین‌گیری به دست آمده است.

برای مقایسه مدت زمان تأخیر ناشی از روش‌های AES، DES با روش پیشنهادی با ورودی داده اصلی ۱۶ بیتی از روابط (۲) که از شبیه‌سازی مکرر این دو الگوریتم بدست آمده است[۹] برای محاسبه زمان تأخیر ناشی از روش‌هایDES و AES استفاده می‌شود.

$$\begin{cases} t_{DES} = (19\,P_{Length} + 1.1)\,ms \\ t_{AES} = (65.2\,P_{Length} + 3.22)\,ms \end{cases} \qquad (۲)$$

در این رابطه‌ها P_{Length} تعداد بلوک داده در روش رمزنگاری است. طول یک بلوک داده در DES برابر ۶۴ و در روش AES برابر ۱۲۸ است. با توجه به روش به کار رفته در [۷-۸] تعداد بلوک ورودی به الگوریتم‌های رمز نگاری DES و AES به تر تیب ۳ و ۲ است (۱۲۸ بیت ناشی از الگوریتم درهم‌ریز، ۶۴ بیت حاصل از داده اصلی و برچسب زمانی مجموعاً ۱۹۲ بیت است). این مقدار برای الگوریتم پیشنهادی، ۱ بلوک (۳۲ بیت) است زیرا در روش پیشنهادی از الگوریتم‌های درهم‌ریز استفاده نمی‌شود و لذا داده اضافی ناشی از آنها وجود ندارد. مقدار تأخیر ناشی از روش پیشنهادی همان مقدار اجرای آن در نرم‌افزار MATLAB در نظر گرفته شده است. به علاوه از تأخیر ناشی از تابع درهم‌ریز به علت سرعت زیاد اجرای آن صرف‌نظر شده است. همان‌طور که در سطر آخر جدول (۱) نشان داده شده است، تأخیر زمانی روش رمزنگاری پیشنهادی در حدود ۱۰٪ روش DES و ۵٪ روش AES می‌باشد، که در مقایسه با هر دو روش مقدار بسیار کمتری می‌باشد.

برای بررسی عملکرد روش پیشنهادی، از یک موتور DC در سامانه کنترل از طریق شبکه استفاده می‌شود. تابع تبدیل موتور DC به فرم فضای حالت پیوسته در رابطه (۳) بیان شده است.

Table (1): Packet length and average of run time in different encryption methods

جدول (۱): طول بسته و میانگین زمان اجرا برای روش‌های مختلف رمزنگاری

روش / پارامتر	رمزنگاری DES	رمزنگاری AES	رمزنگاری پیشنهادی
طول بلوک پیش فرض الگوریتم (بر حسب بیت)	64	128	32
مدت زمان رمزنگاری برای یک بلوک داده	21.1	68.44	7.7
تعداد بلوک داده در رمزنگاری برای شبیه سازی	3	2	1
تأخیر زمانی رمزنگاری در شبیه سازی	59.1	133.42	7.7

$$\begin{bmatrix} \dot{I}_a \\ \dot{\omega} \end{bmatrix} = \begin{bmatrix} -\frac{R}{L} & -\frac{K_b}{L} \\ \frac{K_t}{J} & -\frac{B}{J} \end{bmatrix} \begin{bmatrix} I_a \\ \omega \end{bmatrix} + \begin{bmatrix} \frac{1}{L} \\ 0 \end{bmatrix} u(t)$$
$$y(t) = \begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} I_a \\ \omega \end{bmatrix} \qquad (۳)$$

کنترل‌گر به‌کاررفته در این مقاله، یک کنترل‌گر تناسبی-انتگرالی با ضریب تناسبی (K_p) و ضریب انتگرالی (K_i) و به ترتیب با مقادیر ۱ و ۰/۱ می‌باشد. رابطه (۴) نحوه محاسبه سیگنال کنترلی را توسط کنترل‌گر نشان می‌دهد.

$$u_R(n) = K_p\,e(n) + K_i \sum_{k=1}^{n} e(k) \qquad (۴)$$

مدت زمان شبیه‌سازی سامانه کنترل از طریق شبکه ۳۰ ثانیه و نرخ متوسط ازدست‌رفتن بسته ۳۵ ٪ می‌باشد. تأخیر زمانی شبکه به صورت تصادفی برای هر بسته در بازه ۱۰۰ تا ۶۰۰ میلی‌ثانیه در نظر گرفته شده و نرخ نمونه‌برداری ۱۰ میلی ثانیه است.

احتمال خطای تقلب برای هر بسته ۲۵٪ است که در صورت وقوع، با احتمال ۵۰٪ منجر به افزایش تأخیر و با احتمال ۵۰٪ باعث تغییر مقدار داده حداکثر به اندازه ۱۰۰٪ خواهد شد. تصحیح شامل حذف بسته‌هایی با مقادیر نادرست یا حذف بسته‌هایی با تأخیر بیش از اندازه می‌شود.

جهت مقایسه میان نتایج، شاخص عملکرد سامانه برای روش‌های مختلف رمزنگاری طبق رابطه (۵) به صورت تحلیلی محاسبه شده است و نتایج در جدول (۲) آورده شده است. مقدار J_3 در این رابطه برابر فراجهش است که برابر اختلاف میان بیشینه خروجی با مقدار نهایی

تقسیم بر مقدار نهایی است. نمونه‌ای از خروجی نیز در پنج حالت مختلف در اشکال ۱ تا ۵ نشان داده شده است.

در رابطه (۵) T_s و E_r به ترتیب زمان نشست و خطای خروجی نسبت به ورودی در حالت سامانه بدون تأخیر و از دست رفتن بسته‌ها هستند که مقادیر آن‌ها به ترتیب برابر ۶۱/۱ نمونه و ۴/۷۹۳۸ است. بر اساس رابطه (۵)، مقدار کمتر J به معنای عملکرد کنترلی بهتر سامانه می‌باشد چون هرچه مقدار J کمتر باشد، عملکرد سامانه کنترلی به عملکرد سامانه کنترلی ایده‌آل شبیه‌تر می‌شود.

$$J_1 = \frac{T_S - \overline{T}_S}{\overline{T}_S}$$

$$J_2 = \frac{Er - \overline{Er}}{\overline{Er}}$$

$$J_3 = OVERSHOOT \qquad (۵)$$

$$J = (J_1 + J_2 + J_3)$$

$$P = \frac{100}{J}$$

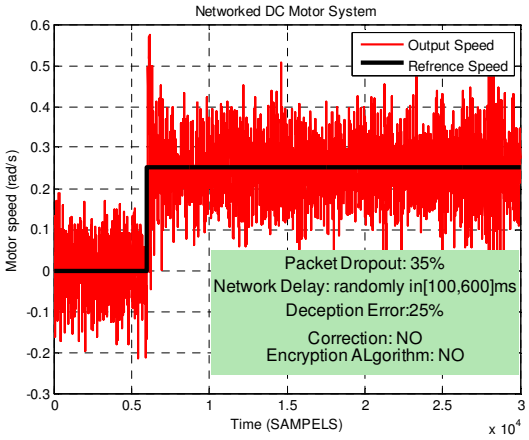
شکل (۵) نشان‌دهنده پاسخ سامانه کنترلی تحت حمله و بدون استفاده از رمزنگاری است که در این حالت، مقدار J برابر با ۱۴/۷۵ می‌باشد و عملکرد کنترلی مناسبی را ندارد. شکل (۶) سامانه کنترلی را نشان می‌دهد که تحت حمله قرار گرفته است و فرض شده که توسط روشی رمزنگاری شده که دارای تأخیر رمزنگاری صفر است (سامانه رمزنگاری ایده‌آل). همانطور که ملاحظه می‌شود، پاسخ سامانه در این حالت بدون فراجهش و پایدار می‌باشد. شکل (۷) پاسخ سامانه کنترلی را نشان می‌دهد که تحت حمله قرار گرفته و توسط روش DES رمزنگاری شده است. در این حالت پاسخ سامانه دارای فراجهش می‌باشد و مقدار J برابر با ۸۰/۹۴ است. شکل (۸) پاسخ سامانه کنترلی را در حالت حمله و استفاده از رمزنگاری AES نشان می‌دهد. در این حالت پاسخ سامانه کاملاً ناپایدار شده است و مقدار J بی‌نهایت می‌شود. شکل (۹) پاسخ سامانه کنترلی را نشان می‌دهد که تحت حمله قرار گرفته است و در آن از روش رمزنگاری پیشنهادی استفاده شده است. در این حالت، پاسخ سامانه پایدار شده است و مقدار J برابر با ۱۶/۵۸ می‌شود که در مقایسه با روش‌های رمزنگاری AES و DES کمترین مقدار را دارد و در نتیجه دارای عملکرد کنترلی بهتری می‌باشد و به حالت ایده‌آل نزدیک‌تر است.

جدول (۲) نشان می‌دهد که با افزایش تأخیر ناشی از روش‌های رمزنگاری عملکرد سامانه کنترلی کاهش می‌یابد. روش‌های رمزنگاری معمول مانند AES و DES به علت تأخیر زیادی که ایجاد می‌نمایند، نمی‌تواند نیازهای کارایی یک سامانه کنترل از طریق شبکه را فراهم نمایند و حتی در برخی از موارد باعث ناپایداری آن می‌شود.

Table (2): Values of performance for different encryption methods

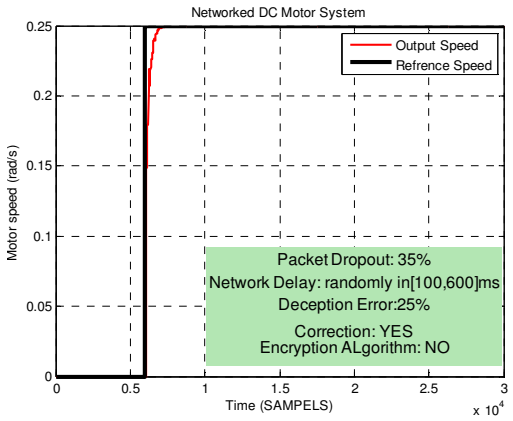
جدول (۲): مقادیر هزینه کارایی و کارایی برای روش‌های رمزنگاری مختلف

روش / شاخص عملکرد	بدون رمزنگاری	رمزنگاری DES	رمزنگاری AES	رمزنگاری پیشنهادی
J	14.75	80.94	∞	16.58
P	6.779	1.23	0	1.603



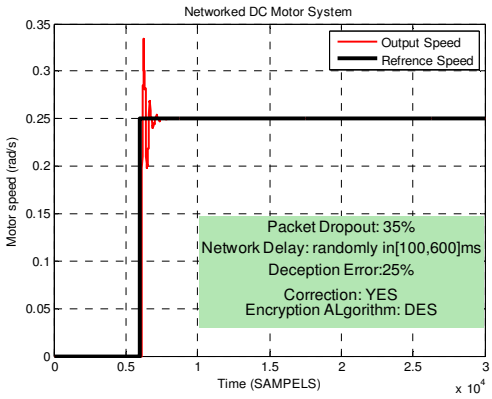
شکل (۵): پاسخ سامانه کنترلی تحت حمله و بدون رمزنگاری

Fig. (5): Response of control system in attack conditions and whithout any encryptions



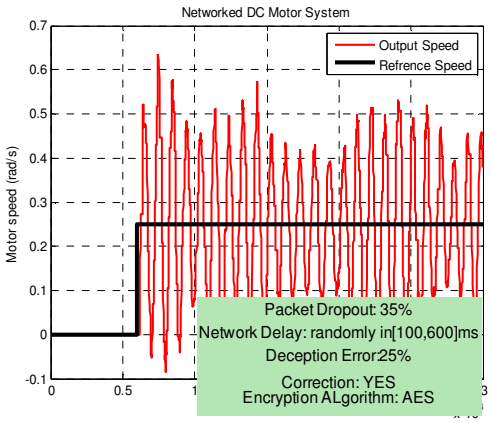
شکل (۶): پاسخ سامانه کنترلی تحت حمله و رمزنگاری با تأخیر رمزنگاری صفر

Fig. (6): Response of control system with encryption in attack conditions and with zero encryption time delay



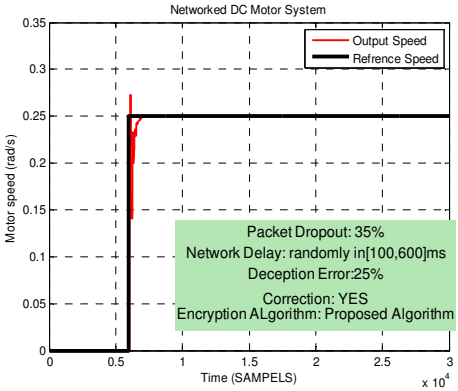
شکل (۷): پاسخ سامانه کنترلی تحت حمله و رمزنگاری DES

Fig. (7): Response of control system in attack conditions and with DES encryption.



شکل (۸): پاسخ سامانه کنترلی تحت حمله و رمزنگاری AES.

Fig. (8): Response of control system in attack conditions and with AES encryption



شکل (۹): پاسخ سامانه کنترلی تحت حمله و رمزنگاری پیشنهادی

Fig. (9): Response of control system in attack conditions and with proposed encryption

این در حالی است که با استفاده از روش رمزنگاری پیشنهادی که دارای تأخیر کمی باشد، می‌توان ضمن حفظ امنیت، کارایی سامانه را نیز تا حد قابل قبولی بالا برد. استفاده از روش رمزنگاری پیشنهادی منجر به بهبود بیش از ۳۸/۸ درصدی عملکرد سامانه کنترل ازطریق شبکه در مقایسه با رمزنگاری DES شده است.

۵- نتیجه‌گیری

سامانه‌های کنترل از طریق شبکه اخیراً در حوزه‌های وسیعی از مهندسی کنترل و مخابرات مورد توجه قرار گرفته است. مهمترین چالش موجود در این سامانه‌ها، تأخیر تصادفی در ارسال و دریافت داده‌ها می‌باشد. همچنین استفاده گسترده از شبکه‌های مخابراتی بخصوص اینترنت، اهمیت امنیت داده‌ها را در چنین سامانه‌هایی نشان می‌دهد. در این مقاله برای بهبود عملکرد سامانه‌های کنترل از طریق شبکه، روش رمزنگاری جدیدی پیشنهاد شده است که علاوه بر امنیت داده‌ها، تأخیر زمانی ناشی از روش رمزنگاری را کاهش داده است. روش رمزنگاری پیشنهادی در این مقاله برای مقابله با حمله تقلب توانسته است با فراهم آوردن یکپارچگی داده و تأخیر زمانی کم، عملکرد سامانه را بیش از ۳۰٪ بهبود بخشد.

بررسی سامانه‌های تشخیص نفوذ، پیکربندی و استانداردهای مختلف شبکه می‌تواند از موارد بسیار مهم تحقیق و پژوهش در زمینه سامانه‌های کنترل از طریق شبکه باشد. همچنین طراحی استانداردهایی برای تعیین سامانه امنیتی مناسب برای شبکه کنترلی، متناسب با کاربرد آن از زمینه‌های پژوهشی آینده است.

پی‌نوشت:

1. Networked control systems(NCS)
2. Ethernet
3. Supervisory control and data acquisition(SCADA)
4. Data encryption standard(DES)
5. Advanced encryption standard(AES)
6. Distibuted Control Systems
7. Digital
8. Band limited
9. Stochastic Time Delay
10. Packet Dropout
11. Initial key
12. Time stamp
13. Secondary key
14. Brute-force attack

References

[1] J.P. Hespanha, P. Naghshtabriz, Y. Xu, "A survey of recent results in networked control systems", Proc. IEEE, Vol. 95, No. 1, Jan. 2007.
[2] U.S. Department of Energy, Office of Energy Assurance, 21 Steps to Improve Cyber. Security of SCADA Networks, 2003.
[3] K. Scarfone, P. Mell, "Guide to intrusion detection and prevention systems (IDPS)", NIST(National Institute of Standards and Technology), 2007.
[4] A. Creery, E.J. Byres, "Industrial cybersecurity for power system and SCADA networks", In Proc. 52nd Annu. Petroleum Chemical Industry Conf. Ind. Appli. Soc., pp.303-309, 2005.
[5] S. Amin, G.A. Schwartz, S.S. Sastry, "Security of interdependent and identical networked control systems", Automatica, Vol. 49, No.1, pp. 186-192, Jan. 2013.
[6] K. Yuan, J. Chen, G. Liu, J. Sun, "Design and implementation of data encryption for networked control systems", In Proc. IEEE Int. Conf. Sys., Man, and Cybern., pp. 2105-2109, 2009.
[7] Z. Pang, G. Zheng, G. Liu, C. Luo, "Secure transmission mechanism for networked control systems under deception attacks", In Proc. IEEE Int. Conf. Cyber Technology Automation, Control, and Intelligent Syst., pp. 27-32, 2011.
[8] P. Hua, L. Guoping, "Secure networked control systems under data integrity attacks", In Proc. 29th Chinese Control Conf., Beijing, China, pp. 5765-5771, 2010.
[9] R.A Gupta, M. Chow, "Performance assessment and compensation for secure networked control systems", In Proc. 34th Annu. Conf. IEEE Ind. Electron., pp. 2929-2934, 2008.
[10] W. Zeng, M. Chow, "Optimal tradeoff between performance and security in networked control systems based on coevolutionary algorithms", IEEE Trans. Ind. Electron., Vol. 59, No.7, pp. 3016-3025, July 2012.
[11] W. Zeng, M. Chow, "A trade-off model for performance and security in secured networked control systems", In Proc IEEE Int. Sympos. Ind. Electron. pp. 1997-2002, 2011.
[12] P. Hajebi, S.M.T. AlModarresi, "Online adaptive fuzzy logic controller using neural network for networked control systems", In Proc. 14th Int. Conf. Advanced Commun. Technology, pp. 888-893, 2012.
[13] P. Hajebi, S.M.T. AlModarresi, "Online adaptive fuzzy logic controller using genetic algorithm and neural network for networked control systems", ICACT Trans. Advanced Commun. Technology, Vol. 1, No. 3, pp. 88-98, Nov. 2012.