9th SASTech Symposium on Advances in Science & Technology (2014)
نهمین سمپوزیوم پیشرفت های علوم و تکنولوژی
مشهد- ۱۳ آذر- ۱۳۹۳
کمیسیون دوم: همایش ملی علوم و مهندسی کامپیوتر
بامحوریت
امنیت ملی و توسعه پایدار
برگزارکننده: موسسه آموزش عالی خاوران
www.khi.ac.ir

افزایش امنیت سیستم اسکادا با مدیریت کلید و الگوریتم منحنی فرابیضوی

اکرم ابراهیمی نژاد[۱]، فرخ کروپی[۲] و حمیدرضا ناجی[۳]

۱- دانشجوی کارشناسی ارشد دانشگاه آزادکرمان

۲- هیئت علمی دانشگاه آزاد بافت

۳- هیئت علمی دانشگاه تحصیلات تکمیلی کرمان

Aebrahimi.computer@gmail.com

نام ارائه‌دهنده: اکرم ابراهیمی نژاد

خلاصه

هر جا که یک مرکز کنترل یا پایانه مرکزی از یک یا چند پایانه راه دور اطلاعات دریافت کند و به آنها فرمان هایی نیز بدهد، یک سیستم اسکادا وجود خواهد داشت. برای جلوگیری از خرابیهای این سیستم، از رمزنگاری برای حفاظت اطلاعات در حال انتقال و ذخیره استفاده میشود. در این مقاله، محیط امنی را در شبکه اسکادا برای ایجاد ارتباط مناسب بین مرکز کنترل وRTU ها با استفاده از پروتکل مدیریت کلید به همراه احراز هویت دوطرفه ارائه دادیم که برای این منظور از رمزنگاری منحنی فرابیضوی استفاده کردیم. منحنی فرابیضوی درمواقعی که در اندازه عملگرهای سخت‌افزاری محدودیت توان، زمان و ذخیره‌سازی وجود دارد، بسیار مناسب میباشد. از طرفی سرور باید مطمئن به امنیت و دستکاری نشدن کلیدها و پیام‌ها و اطلاعات ارسال و دریافت باشد. بدین منظور امضای دیجیتالی را مطرح کردیم. در عین حال شبکه‌های مبتنی بر منحنی فرابیضوی به دلیل نیازمند بودن به محاسبات کمتر نسبت به بیضوی و RSA امنیت بالاتری دارند. الگوریتم منحنی فرابیضوی در برابر بقیه الگوریتمهای رمزنگاری پارامترهای کمتری را شامل میشود، بعنوان نمونه ۸۰ بیت فضا برای فیلد HECC نیاز است درحالی که در ECC،۱۸۰ بیت و در RSA ۱۰۲۴ بیت لازم میشود. نتایج عملکردی طرح پیشنهادی ویژگیهای محرمانگی، صحت، عدم جعل و عدم انکار را حفظ میکند و نسبت به طرح های مشابه بدلیل ایجاد طول بیت کمتر سربار ارتباطی را بهبود بخشیده است.

کلمات کلیدی: اسکادا، مدیریت کلید، رمزنگاری منحنی فرایضوی، امضاء دیجیتال.

۱. مقدمه

تجهیزات صنعتی مدرن از قبیل نیروگاه های تولید برق، سیستم هائی هستند که کنترل نظارت و اکتساب داده ها (SCADA)[۴] را انجام میدهند. از آنجا که شبکه های اسکادا در سیستم های دولتی و صنعتی هر کشور مورد استفاده هستند میتوان فهمید که اهمیت و ضرورت آنها هم جنبه ملی و هم جنبه سیاسی برای آن دولت دارد در نتیجه امنیت در آنها بسیار مهم میباشد و همچنین اتصال سیستمهای SCADA به شبکه های باز، مطالعه آنها را به یک مسئله و فرضیه مهم تبدیل کرده است. در ژوئن ۲۰۱۰، ویروس بلاکادا اولین حمله خطرناک یک ویروس مخرب به اسکادا را گزارش نمود که به سیستمهای اسکادای نصب شده برروی سیستمهای ویندوز(سیستمهایWinCC/PCS زیمنس)حمله میکرد نام این ویروس مخرب استاکس نت بود و

[4] **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition