

عنوان مقاله:

(تامین امنیت شبکه های حسگر بیسیم با روش رمزنگاری اصلاح شده منحنی بیضوی)

محل انتشار:

اولین کنفرانس بین المللی مکانیک، برق و علوم مهندسی (سال: 1400)

تعداد صفحات اصل مقاله: 10

نویسنده:

حسین قلاوند - کارشناسی ارشد مهندسی کامپیوتر گرایش نرم افزار، لرستان - ایران

خلاصه مقاله:

با توجه به رشد سریع شبکه های حسگر بیسیم (WSN) در جهان امروزی، این شبکه ها در تمام شاخه های علوم و مهندسی وارد شده اند و به دلیل همین کاربردهای وسیع شبکه های حسگر بیسیم، این شبکه ها بیشتر در معرض تهدیدها و حملات امنیتی هستند. لازم است با در نظر گرفتن ویژگیهای منحصر به فرد حسگرها، یک طرح کلیدی موثر برای مدیریت شبکه های حسگر بیسیم ارائه شود که بتواند این شبکه ها را در مقابل کلیه حملات و تهدیدات در امان بگذارد و امنیت را برقرار سازد. در این مقاله با کمک رمزنگاری منحنی بیضوی (ECC)، یک روش امنیتی اصلاح شده برای محافظت از شبکه های حسگر بیسیم ارائه شده است. این طرح با بهره گیری از مزیت ECC، بر اساس تبدیل متن ساده به مقادیر کد ASCII و مبتنی بر عملیات دوتایی به کار رفته در رمزنگاری عمل میکند که میتواند پیچیدگی محاسباتی را تا حد زیادی کاهش بدهد و امنیت مورد نیاز شبکه های حسگر بیسیم را تامین کند.

کلمات کلیدی:

شبکه های حسگر بیسیم، طرح کلیدی، رمزنگاری منحنی بیضوی

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/1219446>

