

عنوان مقاله:

بررسی و تحلیل الگوریتم های سبک وزن و کارایی آنها در شبکه حسگر بی سیم

محل انتشار:

پنجمین همایش پژوهش های نوین در علوم و فناوری (سال: 1395)

تعداد صفحات اصل مقاله: 8

نویسندگان:

زهرا سهراب پور - دانشگاه صنعتی مالک اشتر، دانشکده مهندسی رمز، اصفهان، ایران

علی زاغیان - دانشگاه صنعتی مالک اشتر، دانشکده مهندسی رمز، اصفهان، ایران

خلاصه مقاله:

شبکه های حسگر بی سیم نوع جدیدی از شبکه های ارتباطی هستند که دارای کاربرد نظامی و استفاده موثر در مدیریت بحران، کارت های هوشمند، ابزار های مراقبتی سلامت می باشند. شبکه حسگر بی سیم به شدت با محیط در تماس است از این رو امنیت آن ها بسیار اهمیت دارد. به منظور تامین امنیت، نیاز به الگوریتم های سبک وزن می باشد که رمز نگاری سبک وزن برای ابزار هایی با منابع محدود استفاده میشود. بنابراین در شبکه حسگر بی سیم که محدودیت حافظه و توان ظرفیت پردازش دارند، قابل استفاده است. به همین منظور، در این مقاله به معرفی و مقایسه بین رمزهای قالبی سبک وزن DESX، PRESENT، EPCBC، DESL، DES و KLEIN، PUFFIN، TWINE، KATAN، KTANTAN پرداخته شده است.

کلمات کلیدی:

رمز قالبی، سبک وزن، شبکه حسگر

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/531378>

