عنوان مقاله:
ارائه الگوریتم ترکیبی از رمزنگاری AES و RSA و سیستم اعداد مانده ای درراستای افزایش امنیت شبکه های حسگر بی سیم

محل انتشار:
سومین کنفرانس ملی کامپیوتر، فناوری اطلاعات و کاربردهای هوش مصنوعی (سال: 1398)

تعداد صفحات اصل مقاله: 12

نویسندگان:
امیدرضا خوش کام - *گروه مهندسی کامپیوتر، واحد دزفول، دانشگاه آزاد اسلامی، دزفول، ایران*

علی براتی - *گروه مهندسی کامپیوتر، واحد دزفول، دانشگاه آزاد اسلامی، دزفول، ایران*

خلاصه مقاله:
بطور کلی، شبکه های حسگر بی سیم شامل تعدادی گره بصورت متحرک بوده که این گره های در محیط مربوط به شبکه، پخش شده اند و بااستفاده از سنسورهای خود، اقدام به جمع آوری اطلاعات از محیط پیرامون خود میکنند. این اطلاعات جمع آوری شده توسط گره ها، در واقع برای گزارش داددن به گره های بالاتر مانند گره چاهک و گره نماینده استفاده میشوند که بیشترین کاربرد را در شبکه های حسگر بی سیم دارند. یکی از جنبه هایی که در شبکه های حسگر بیسیم در تحقیقات کنونی بسیار موردتوجه قرار گرفته است، جنبه امنیت این شبکه ها می باشد. از جمله راهکارهایی که برای افزایش امنیت در شبکه های حسگر بی سیم مورد استفاده قرار گرفته است، رمزنگاری اطلاعات در این شبکه های میباشد. در واقع با توجه به اینکه ارسال بسته از سمت گره ها برای گره چاهک در شبکه های حسگر بی سیم از درجه اهمیت بالایی برخوردار است، لذا برای این ارسال باید مکانیزمهای امنیتی خاصی درنظرگرفته شود. به همین علت، تحقیقات بسیاری در زمینه برقراری این امنیت در شبکه های حسگر بیسیم انجام شده است. لذا در این پایان نامه، روشی در راستای افزایش امنیت در شبکه های حسگر بیسیم ارائه شده است که حاصل ترکیب دو الگوریتم AES و RSA و سیستم اعداد مانده ای است. در واقع فایل ارسالی به بلوکهای 16 بایتی تقسیم شده و بلوکهای فرد با استفاده از الگوریتم AES و بلوکهای زوج با استفاده از الگوریتم RSA رمزنگاری می شوند. همچنین جهت سهولت انجام کار، تمامی محاسبات الگوریتم های رمزنگاری ذکر شده در سیستم اعداد ماندهای انجام میشود. نتایج حاصل از پیاده سازی روش پیشنهادی نشان داده است که میزان امنیت نسبت به سایر روشهای دیگر، بهبود یافته است.

کلمات کلیدی:
شبکه حسگر بی سیم، رمزنگاری، الگوریتم AES ،الگوریتم RSA ،امنیت، سرعت.