عنوان مقاله:
ارائه راهکار دو مرحله ای جدید برای مدیریت کلید در شبکه های حسگر بی سیم

محل انتشار:
پنجمین کنفرانس ملی کامپیوتر، فناوری اطلاعات و کاربردهای هوش مصنوعی (سال: 1400)

تعداد صفحات اصل مقاله: 9

نویسندگان:
فاطمه مهدیانی - *کارشناسی ارشد مهندسی کامپیوتر گرایش نرم افزار دانشگاه علوم تحقیقات تهران*

سیدعلی مهدیون - *دانشجوی دکتری دانشگاه شاهدتهران*

سیدحمید حاج سیدجوادی - *عضو هیئت علمی دانشگاه شاهد دکتری تخصصی جبر محاسباتی دانشگاه امیرکبیر*

خلاصه مقاله:
یک شبکه حسگر بی سیم از تعدادی گره تشکیل شده است. که دارای محدودیت های انرژی، حافظه پردازش و پهنای باند هستند. یکی از کاربردهای اساسی این گونه شبکه جمع آوری اطلاعات از محیط های گوناگون است. بنابراین تبادل امن اطلاعات بینابن حسگرها مساله مهمی است. ولی باتوجه به محدودیت های موجود در حسگرها، رمزنگاری های متداول از جمله رمزنگاری نامتقارن ECC,RSA و..نمی تواند برای این گونه شبکه ها در تبادل اطلاعات مورد استفاده قرار گیرد. بنابراین از راه کار سبک، پیش توزیع کلید استفاده می شود در این مقاله روش های مختلف پیش توزیع کلید مورد مطالعه قرار گرفته و استفاده از طرح های قطعی در پیش توزیع کلید، به عنوان یک روش کارآمد مورد توجه قرار می گیرد سپس طرح های قطعی جدیدی معرفی شده، که در مقایسه با انواع مشابه، در برآورده ساختن شاخص های ارزیابی توزیع کلید، مانندامنیت عملکرد مناسب تری دارند.

کلمات کلیدی:
شبکه های حسگر بی سیم، پیش توزیع کلید، طرح های قطعی