عنوان مقاله:
الگوریتم پیشنهادی رمزنگاری مجدد با استفاده از RSA جهت افزایش امنیت درسیستم هایRFID

محل انتشار:
دومین کنفرانس ملی مهندسی نرم افزار دانشگاه آزاد لاهیجان (سال: 1391)

تعداد صفحات اصل مقاله: 4

نویسندگان:
زینب کرمان ساروی - *دانشگاه آزاد اسلامی واحد بابل، گروه کامپیوتر، بابل، ایران،*

بهاره قلی پورگودرزی - *دانشگاه آزاد اسلامی واحد بابل، گروه کامپیوتر، بابل، ایران،*

خلاصه مقاله:
با توجه به توسعه فن آوری RFID و به کارگیری گسترده از این تکنولوژی، امکان بروز تهدیداتی جدی علیه امنیت و حریم خصوصی کاربران وجود خواهد داشت. این تهدیدات می تواند ناشی از ردیابی تگ ها، جایگزینی تگ های جعلی و یا هرنوعتعقیب و جعل جهت اختلال سیستم و یا دستیابی به اطلاعات محرمانه تگ ها توسط مهاجمان باشد. بنابراین استفاده از مکانیزم های امنیتی برای سیستم هایRFID از اهمیت بسیار بالایی برخوردار خواهد بود. در این مقاله ضمن تجزیه و تحلیل میزان آسیب پذیری این سیستم ها، چند پروتکل امنیتی رایج را مورد بررسی قرار داده و با توجه به مزایا و معایب این روش ها، یک الگوریتم پیشنهادیمبتنی بر رمزنگاری مجدد برای تگ های گروه بندی شده مطرح گردیده است. در نهایت روند اجرای این الگوریتم از جنبه های مختلف مانند جلوگیری از ردیابی و ارسال تگ های جعلی، امنیت بالا و امکان پیاده سازی برای تگ های با قابلیت بالا و هزینه کم، مورد بررسی قرار گرفته است

کلمات کلیدی:
RFID ، پروتکل امنیت، تگ های گروه بندی شده، رمزنگاری مجدد