عنوان مقاله:
ارائه یک زیرساخت احراز اصالت دوسویه ایمن و کارا برای سامانههای رادیوشناسه RFID

محل انتشار:
دومین همایش ملی مهندسی کامپیوتر و فناوری اطلاعات دانشگاه پیام نور (سال: 1394)

تعداد صفحات اصل مقاله: 8

نویسندگان:
ابراهیم نجفی - *محقق و مدرس، دانشگاه صنعتی مالک اشتر، مرکزآموزشی تحقیقاتی ریاضیات و رمز*

محمدجعفر هاشمی گرم دره - *محقق و مدرس، مرکز آموزش علمی –کاربردی تیران و کرون*

خلاصه مقاله:
هرچند استفاده ازسامانههای تشخیص هویت رادیویی RFID روز به روز درحال گسترش است، با این حال استفاده ازاین سامانهها با چالشهای امنیتی عمدهای نیز روبرو است. برای تامین امنیت یک سامانه RFID در لایه پروتکل، تنها ابزاری که میتواند به کارگرفته شود پروتکل احراز هویتی است که بین برچسب وکارتخوان اجرا میشودو درحین اجرای آن طرفین هویت یکدیگر را بررسی کرده ودر صورت صحت میپذیرند.پروتکل های موجود از بعضی حملات مانند حمله جعل ،حمله تکرار،غیرهم زمانی ،حمله مرد میانی ،ردیابی وحمله فیزیکی رنج میبرند.دراین مقاله پروتکلهای موجود مبتنی بر سیستم رمزنگاری خم بیضوی را بررسی کرده وپروتکلی را پیشنهاد میدهیم که درمقابل حملات مشهور مقاوم بوده ویک مقایسه با پروتکلهای موجود انجام میگیرد

کلمات کلیدی:
پروتکل احرازهویت ، احراز هویت رادیویی RFID حمله مردمیانی ، سیستم رمزنگاری خم بیضوی