عنوان مقاله:
شناخت آسیب های امنیتی پروتکل احراز اصالت MAP و ارائه پروتکل بهبودیافته امن

محل انتشار:
فصلنامه علوم و فناوری های پدافند نوین, دوره 7, شماره 3 (سال: 1395)

تعداد صفحات اصل مقاله: 9

نویسندگان:
محمد مردانی شهر بابک - *مخابرات-مدیریت استراتژیک*

شهاب عبدالملکی - *علوم و تحقیقات تهران*

خلاصه مقاله:
امروزه سامانه‌های شناسایی با امواج رادیویی (RFID) عمدتا در زندگی روزمره اشخاص استفاده می‌شود. این سامانه‌ها در زمینه‌هایی نظیر پزشکی، نظامی و تشخیص هواپیماهای خودی از دشمن کاربرد دارد. از حیث اهمیت امنیت این سامانه‌ها، پروتکل‌های متفاوتی برای احراز هویت پیشنهاد شده است. آقای پنگ و همکاران، یک پروتکل احراز هویت مبتنی بر استاندارد EPC C-1 G-2 ارائه دادند. طراحان آن ادعا کردند که از لحاظ امنیتی و محرمانگی امن و در مقابل حملات مقاوم است. در این مقاله نشان داده می‌شود که برخلاف ادعای طراحان، پروتکل مذکور امن نیست و در مقابل حملاتی نظیر کشف کلید، جعل برچسب، جعل کارت‌خوان و ناهم زمانی ضعف دارد. همچنین به منظور افزایش امنیت کاربران این سامانه ها، یک پروتکل بهبودیافته پیشنهاد داده و نشان می دهیم این پروتکل در مقابل حملات ذکرشده امن است. بعلاوه پیچیدگی و کارایی پروتکل‌های ارایه شده با پروتکل پیشنهادی مقایسه گردیده و نشان داده می‌شود که با تغییراتی در پروتکل، مشکلات امنیتی آن به طور کامل برطرف شده است. در نهایت، امنیت پروتکل بهبودیافته با برخی از پروتکل‌های مشابه مقایسه می شود..

کلمات کلیدی:
پروتکل های احراز هویت سامانه های RFID, استاندارد EPC C1 G2, امنیت, محرمانگی, حمله ها