عنوان مقاله:
نقص امنیتی در یک طرح احراز اصالت و توافق کلید سبک وزن

محل انتشار:
چهارمین کنفرانس ملی فناوری اطلاعات، کامپیوتر و مخابرات (سال: 1396)

تعداد صفحات اصل مقاله: 9

نویسندگان:
رضا نخجوان شهرکی - *کارشناسی ارشد مخابرات رمز دانشگاه صنعتی مالک اشتر*

کیان کیقباد - *استادیار دانشکده ی فناوری اطلاعات دانشگاه صنعتی مالک اشتر*

داوود منصوری - *پژوهشیار دانشکده ی امنیت اطلاعات دانشگاه صنعتی مالک اشتر*

خلاصه مقاله:
امروزه سیستم های ارتباط ماهواره ای یکی از تکنولوژیهای مهم جهت ارایهی خدمات شخصی به افراد شده است که تامین امنیت این ارتباطات یکی از مسایل مهم و همراه با چالش، در این تکنولوژی است. تا به امروز طرح های امنیتی فراوانی برای برقراری ارتباط امن در سیستم های ارتباط ماهواره ای متحرکارایه شده است که هر کدام از آن ها یا از عدم کارایی و یا از عدم تامین امنیت کافی رنج می بردند. اخیرا Xinghua Wu به همراه همکارانش در سال 2017 طرحی ارایه دادند و ادعا کردند که این طرح می تواند همهی نیازمندیهای امنیتی برای ارتباطات ماهواره ای متحرک را برآورده سازد. با این وجود مامتوجه شدیم که در طرح آنها ضعف امنیتی ناشی از حمله ی دزدیده شدن کارت هوشمند وجود دارد و دشمن می تواند طی محاسباتی در زمان آفلاین به هویت اصلی فرد دست یابد. لذا در این مقاله سعی داریم ابتدا طرح آنها را معرفی کرده، سپس تحلیل امنیتی طرح آنها را بیان کنیم و در نهایت به نقطه ضعف طرح شان اشاره خواهیم کرد و نحوهی انجام آن را توضیح خواهیم داد.

کلمات کلیدی:
ارتباطات ماهواره ای، تحلیل امنیتی، احراز اصالت، توافق کلید