نوزدهمین کنفرانس ملی سالانه انجمن کامپیوتر ایران
دانشکده مهندسی کامپیوتر، دانشگاه شهید بهشتی، تهران، ۱۵-۱۳ اسفندماه ۱۳۹۲

یک طرح احراز اصالت امن و کارآمد برای شبکه‌های ماهواره‌ای

سیده فاطمه افتخاری[۱]، کیان کیقباد[۲]

[۱] دانشجوی کارشناسی ارشد، گروه فناوری اطلاعات، ارتباطات و امنیت، دانشگاه صنعتی مالک اشتر، تهران.
s_f_eftekhari@yahoo.com

[۲] استادیار، گروه فناوری اطلاعات، ارتباطات و امنیت، دانشگاه صنعتی مالک اشتر، تهران.
keyghobad@irsig.ir

چکیده

احراز اصالت از جمله پارامترهای مهمی است که یک شبکه ماهواره‌ای برای تامین امنیت خود به آن نیاز دارد. در همین راستا در سال‌های اخیر مقالات متعددی جهت تامین این نیاز ارائه شده‌اند. در سال ۲۰۱۲ آقای Chang و همکارانشان یک طرح احراز اصالت و توافق کلید ارائه دادند. طرح پیشنهادی آنها در برابر حمله جعل هویت و ممانعت از سرویس آسیب‌پذیر است. در این مقاله یک طرح احراز اصالت امن و کارآمد برای سیستم‌های ارتباطات ماهواره‌ای متحرک ارائه شده است که ضعف‌های پروتکل‌های گذشته و بخصوص پروتکل آقای Chang را برطرف نموده است. پروتکل پیشنهادی به دلیل مبتنی‌بودن بر تابع درهم‌ساز و عملیات XOR دارای محاسبات سبک بوده و در برابر حملاتی مانند جعل هویت، ممانعت از سرویس، تکرار، الحاق، تصدیق‌کننده مسروقه و دزدیدن کارت هوشمند امن می‌باشد.

کلمات کلیدی

سیستم ارتباطات ماهواره‌ای متحرک، احراز اصالت، تابع درهم‌ساز.

۱- مقدمه

سیستم‌های ارتباطات ماهواره‌ای متحرک[۱] با پیشرفت تکنولوژی ارتباطات، که اتصال بین شبکه‌های زمینی دور، دسترسی شبکه مستقیم، سرویس‌های اینترنت، کاربردهای چندرسانه‌ای متقابل و انتقال نرخ بالای داده را فراهم می‌کند، بسیار مورد توجه قرار گرفته‌اند. این شبکه‌ها ترکیبی از ماهواره، گذرگاه[۲]ها، کاربران متحرک و مرکز کنترل شبکه[۳](NCC) می‌باشند. ماهواره قسمت فضایی این شبکه است که اتصال بین کاربران متحرک و گذرگاه‌ها را فراهم می‌کند. این قسمت شامل یک یا چند منظومه ماهواره‌ای است. گذرگاه‌ها قسمتی از شبکه هستند که در هر سوی زمین مستقر شده و دسترسی به و از بخش فضایی را فراهم می‌کنند و نیز رابطی بین شبکه‌های زمینی هستند. کاربران متحرک از طریق ماهواره به گذرگاه‌ها متصل می‌شوند. NCC برای هماهنگ کردن دسترسی به منابع ماهواره‌ای و انجام عملیات منطقی به همراه مدیریت شبکه و کنترل، به سیستم مدیریت اطلاعات کاربر متصل می‌شود[۱].

سیستم‌های ارتباطات ماهواره‌ای متحرک خدمات گوناگونی از تلفن و سخن پراکنی[۴] تا شبکه‌های اینترنت را ارائه می‌دهند. البته این شبکه‌ها در کنار کاربردهای فراوان چالش‌های امنیتی نیز دارند و به علت ماهیت پخش بی‌سیم در آنها، استراق سمع برای کاربران تصدیق-نشده خیلی راحت‌تر از شبکه‌های متحرک یا ثابت زمینی است[۱]. به دلیل آنکه توانایی ذخیره‌سازی و پردازش گره‌های ماهواره محدود است، منابع محاسباتی در شبکه ماهواره‌ای باید به طور کامل مورد استفاده قرار گیرند[۲] و نیز به دلیل متحرک بودن ماهواره و کاربر در شبکه‌های ماهواره‌ای متحرک، مدت زمانی که کاربر در دید ماهواره قرار دارد و می‌تواند با آن ارتباط برقرار کند محدود بوده و در نتیجه،