عنوان مقاله:
پروتکل مدیریت کلید محرمانگی در شبکه وایمکس

محل انتشار:
اولین همایش ملی فناوریهای نوین در علوم مهندسی (سال: 1389)

تعداد صفحات اصل مقاله: 10

نویسنده:
محمد عباسی آذر - *کارشناسی ارشد مخابرات-رمز، دانشگاه امام حسین*

خلاصه مقاله:
استاندارد IEEE 802.16 برای برقراری ارتباط در قسمت بی سیم شبکه WNAM طراحی شده است این استاندارد از یک زیرلایه امنیتی که در پایین لایه MAC قراردارد استفاده میکند . دو پروتکل دراین زیرلایه وجود دارد: یک پروتکل تلفیقی که قالبهای داده را رمز نگاری مینماید، و پروتکل مدیریت کلید محرمانگی PKM) که وظیفه آن انجام عملیات احراز اصالت، جوازدهی و توزیع کلیدها میباشد. در این مقاله PKMv1 و PKMv2 بررسی شده و حملاتی که این پروتکل ها را تهدید می کنند مطرح می شوند. و همچنین با توجه به کاربرد ECC برای مسائل امنیتی در شبکه های بیسیم مانند احراز اصالت، امضا و تبادل کلید، استفاده از ECC به جای RSA در پروتکل مدیریت کلید محرمانگی مطرح می شود.

کلمات کلیدی:
استاندارد 802.16 ، WiMAX ، احراز اصالت، PKM ، ECC