

عنوان مقاله:

مقایسه و بررسی پروتکل‌های امنیتی مبتنی بر توافق کلید گروهی در شبکه های بی سیم موردی

محل انتشار:

دومین کنفرانس ملی مهندسی نرم افزار دانشگاه آزاد لاهیجان (سال: 1391)

تعداد صفحات اصل مقاله: 5

نویسندگان:

مجید اعتمادی - دانشگاه آزاد اسلامی واحد کیش ایران

ندا قاسمی پورثابت

خلاصه مقاله:

یکی از مهمترین چالش‌های مدنظر در شبکه های موردی دارای پروتکل امنیتی مبتنی بر توافق کلید گروهی الگوریتم انتشار و محاسبه کلید گروهی در این شبکه است دلیل آن هم ماهیت خاص و محدودیت های ناشی از این شبکه می باشد بررسی این پروتکل ها با توجه به ساختار پروپا و کاربردهای گروهی این نوع شبکه ها و استفاده های متنوع در زمینه های اطلاعاتی داده های مخابراتی رایانه نظامی و تمرکز بر گروهی بودن این پروتکل ها دارای اهمیت خاصی است در این مقاله سعی بر این است که به بررسی و مقایسه برخی از این پروتکل ها پرداخته و میزان مصرف هزینه ها دورها و محاسباتی که برای انجام این الگوریتم ها نیاز است را بیان کنیم یکی از مزایای این دسته از پروتکل ها مناسب بودن آنها برای استفاده در مواردی که نیاز به انرژی محدود است می باشد.

کلمات کلیدی:

شبکه های موردی، الگوریتم مدیریت کلید، رمزنگاری پروتکل امنیتی ، توافق کلید گروهی

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/184950>

