

## عنوان مقاله:

بهبود احراز هویت پیامهای همپخششی چندکاربره در شبکه های حسگر بیسیم مبتنی بر رمزنگاری منحنی بیضوی

## محل انتشار:

دومین همایش ملی مهندسی رایانه و مدیریت فناوری اطلاعات (سال: 1394)

تعداد صفحات اصل مقاله: 10

## نویسندگان:

حامد بشیرپور - کارشناسی ارشد مهندسی فناوری اطلاعات، دانشگاه امام رضا

توفیق فرامرزی - کارشناسی مهندسی نرم افزار، دانشگاه پیام نور تهران شمال

بهزاد مولوی - کارشناسی ارشد فناوری اطلاعات، دانشگاه امام رضا (ع)

## خلاصه مقاله:

مکانیزم احراز هویت همپخششی به کاربران مجاز اجازه میدهد که به شبکه وصل شوند و پیامهایشان را داخل شبکه انتشار دهند. با توجه به بیسیم بودن ارتباطات در شبکه های حسگر، دشمنان به راحتی میتوانند مابین گرهمها مستقر شوند و دادههای انتقالی راشنود کنند و یا محتوای دادههای قانونی را تغییر و به داخل شبکه تزریق کنند. از اینرو، این مکانیزم در شبکه های حسگر بیسیم ضروری و بسیار حیاتی است. در این مقاله، یک راهحل عملی برای احراز هویت همپخششی چندکاربره مبتنی بر رمزنگاری منحنی بیضوی در شبکه های حسگر بیسیم پیشنهاد شده است. در مقایسه با کارهای مشابه و از جمله روش فن و همکارانش که جدیدترین آنها است، پیچیدگی زمانی مورد نیاز روف پیشنهادی در این مقاله به طور چشمگیری کاهش یافته است. علاوه بر این، امنیت قابل اثبات را فراهم کرده و پیادهسازی سادهای دارد. بنابراین، روف پیشنهادی مناسب برای بکارگیری در شبکه های حسگر بیسیم مناسب است

## کلمات کلیدی:

احراز هویت، همه پخششی، شبکه های حسگر بیسیم، منحنی بیضوی، امضای دیجیتال، لگاریتم گسسته

## لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/423043>

