**سیویلیکا - ناشر تخصصی مقالات کنفرانس ها و ژورنال ها**
گواهی ثبت مقاله در سیویلیکا
CIVILICA.com

## عنوان مقاله:
تحلیل ظرفیت امن کانال شنود دو طرفه متقارن

## محل انتشار:
ششمین کنفرانس بین المللی انجمن رمز ایران (سال: 1388)

تعداد صفحات اصل مقاله: 6

## نویسنده:
فرشید فرحت - *تهران دانشگاه صنعتی شریف دانشکده مهندسی برق*

## خلاصه مقاله:
بحث امنیت در تئوری اطلاعات با پیدایش کانالهای شنود آغاز شد. کانالهای شنود کانالهایی هستند که در آنها گیرنده های غیرمجاز نیز قادرند اطلاعات فرستنده ها را دریافت و بهره برداری می کنند. بطور کلی میزان نرخ اطلاعات قابل ارسال توسط فرستنده هاه که بوسیله هیچ گیرنده ای جز گیرنده های مجاز قابل پردازش نباشد تحت عنوان ظرفیت امن شناخته می شود در ابتدا دستیابی به ظرفیت امن مثبت تنها با فرض نازل بودن کانال شنود کننده امکان داشت همچنین مدل کانال شنود برای گیرنده های مجاز و غیرمجاز نامتقارن بود. سپس طرح کانال شنود به مدل کانال پخش با پیام محرمانه تعمیم داده شد. با طرح کانال گفتگوی همگانی برای ارتباط بین فرستنده و گیرنده مجاز نشان داده شد که ظرفیت امن درحالتی که کانال دشمن کاراتر باشد اکیدا مثبت خواهد شد.

## کلمات کلیدی:
امنیت تئوری اطلاعاتی ، کانال شنود دوطرفه متقارن،ظرفیت امن کانال، کانال گفتگوی همگانی، کانال پخش با پیا م محرمانه

## لینک ثابت مقاله در پایگاه سیویلیکا:
https://civilica.com/doc/96879