

افزایش نرخ انتقال سامانه مک‌الیس مبتنی بر کدهای QC LDPC با استفاده از کد کردن به

کلمات وزن ثابت

سهیلا رادبوی^۱، حسین بهرامگیری^۲

۱- کارشناسی ارشد مخابرات رمز دانشگاه مالک اشتر

۲- عضو هیئت علمی دانشگاه صنعتی مالک اشتر

چکیده

در این مقاله، روشی برای انتخاب بردار خطای تصادفی در سامانه مک‌الیس مبتنی بر خانواده کدهای LDPC ارائه شده است. این روش شامل استفاده از توابع کد کردن کلمات کد با وزن ثابت، موسوم به توابع فی است که در سامانه نیدررایتر و های‌مس کاربرد دارند و به منظور تبدیل بلوک-های اطلاعات به کلماتی با وزن ثابت مورد استفاده قرار می‌گیرند. هدف از انجام این تحقیق افزایش نرخ انتقال سامانه مک‌الیس مبتنی بر خانواده کدهای LDPC است به گونه‌ای که امنیت سامانه مذکور به خطر نیفتد. به همین منظور می‌توان بجای انتخاب تصادفی بردار خطا، بلوک‌هایی از اطلاعات را به بردار خطا تبدیل کرد. در این راستا طرحی تلفیقی از دو سامانه های‌مس و مک‌الیس مبتنی بر خانواده کدهای QC LDPC ارائه شده است. استخراج روابط حاکم بر نرخ انتقال طرح تلفیقی نشان می‌دهد که انتخاب بردار خطا با کمک توابع کد کردن کلمات با وزن ثابت در مقایسه با بردار خطای تصادفی موجب افزایش نرخ انتقال خواهد شد. همچنین نتایج حاصل از بررسی امنیت و پیچیدگی طرح نشان می‌دهد این سامانه قابل پیاده‌سازی بوده و اضافه کردن اطلاعات در بردار خطا، امنیت سامانه را به خطر نخواهد انداخت.

واژگان کلیدی: سامانه رمزنگاری مک‌الیس مبتنی بر کدهای QC LDPC، نرخ انتقال، توابع

کد کردن به کلمات وزن ثابت، اثبات امنیت.