عنوان مقاله:
پروتکل توافق کلید گروهی مقاوم در برابر تقلب با ویژگی تصحیح خطای ناشی از اختلال کانال

محل انتشار:
هفتمین کنفرانس بین المللی فناوری اطلاعات و دانش (سال: 1394)

تعداد صفحات اصل مقاله: 6

نویسندگان:
زیبا اسلامی - *گروه علوم کامپیوتر، دانشکده ریاضی، دانشگاه شهید بهشتی، تهران*

مهناز نوروزی - *گروه علوم کامپیوتر، دانشکده ریاضی، دانشگاه شهید بهشتی، تهران*

خلاصه مقاله:
گسترش روزافزون کنفرانس های اینترنتی و استفاده از کانال های عمومی برای تبادل اطلاعات گروهی، پروتکل های توافق کلید گروهی را به یک موضوع فعال تحقیقاتی بدل نموده است. در یک پروتکل توافق کلید گروهی، افرادی که هیچ اطلاع مخفی مشترکی ندارند، با همکاری یکدیگر و با استفاده از یک کانال ناامن می توانند یک کلید مشترک تولید نموده و از آن برای اهداف رمزنگاری استفاده کنند. دراین مقاله، از پروتکل توافق کلید گروهی ارائه شده توسط اسلامی و همکاران استفاده نموده و طرحی ارائه م یکنیم که علاوه بر ویژگی های قبلی، این قابلیت را دارد که خطاهای بوجود آمده در حین ارسال اطلاعات را نیز اصلاح کند. برای این منظور، بوسیله یک رویه ی تشخیصو تصحیح خطای کارامد، تغییرات بوجود آمده در اطلاعات ارسالی را که ناشی از وجود اختلال در کانال ارتباطی است، مدیریت می کنیم.

کلمات کلیدی:
توافق کلید گروهی، شرکت کننده متقلب، خم بیضوی، کدهای LDPC