عنوان مقاله:
مدل سازی و اعتبارسنجی پروتکل تصدیق هویت دانایی صفر گوئیلو- کوئیس کواتر

محل انتشار:
هفتمین کنفرانس ملی مهندسی برق و الکترونیک ایران (سال: 1394)

تعداد صفحات اصل مقاله: 5

نویسندگان:
حمیدرضا خیرمند - *دانشگاه پیام نور تهران، ایران*

مهدی جوانمرد - *دانشگاه پیام نور تهران، ایران*

خلاصه مقاله:
وارسی مدل روشی خودکار برای بررسی سیستم های همزمان و سیستم هایی با حالات متناهی می باشد. امروزه وارسی مدل به شکل گسترده ای در آنالیز و ارزیابی صحت سخت افزار، سیستم های نرم افزاری و به خصوص پروتکل های امنیتی مورد استفاده قرار می گیرد. پروتکل گوئیلو- کوئیس کواتر که یک پروتکل مبتنی بر دانایی صفر است، برای اهداف تصدیق هویت کاربرد دارد. در این مقاله ما مدلی از این پروتکل در قالب ماشین حالت متناهی ارائه، ویژگی هایی را به صورت CTL بیان، و پس از پیاده سازی توسط ابزار وارسی مدل نمادین NuSMV اقدام به وارسی و ارزیابی این پروتکل کردیم. با توجه به نتایج حاصل شده، این پروتکل در تمام حالات به درستی عملیات اعتبارسنجی را انجام نمی دهد.

کلمات کلیدی:
وارسی مدل، پروتکل تصدیق هویت دانایی صفر، پروتکل گوئیلو-کوئیس کواتر، NuSMV ،CTL