

عنوان مقاله:

ارایه یک پروتکل احراز هویت گمنام با حفظ محرمانگی جهت ارتباطات بین خودرویی VANET

محل انتشار:

نخستین کنفرانس ملی محاسبات نرم (سال: 1394)

تعداد صفحات اصل مقاله: 8

نویسندگان:

مهناز نوش آذر - دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات گرایش شبکه، پردیس دانشگاهی، دانشگاه گیلان

رضا ابراهیمی آتانی - عضو هیات علمی دانشکده فنی، دانشگاه گیلان

خلاصه مقاله:

سیستم های ارتباط خودرویی این پتانسیل را دارند که به طور قابل توجهی ایمنی در حمل و نقل خودرو را افزایش دهند، جریان ترافیک انباشته بر روی جاده ها را بهبود بخشند و تعداد مرگ و میر مردم و صدمات ناشی از تصادفات خودروها را کاهش دهند. این سیستم یک نوع خاصی از شبکه ی سیار اقتضایی است که شبکه های اقتضایی بین خودرویی (VANET) نامیده شده است. یک شبکه اقتضایی بین خودرویی بدون داشتن امنیت، کاملاً در برابر حملاتی مانند انتشار پیام های هشدار اشتباه و سرکوب پیام های هشدار واقعی آسیب پذیر است، بر همین اساس عامل ایمنی به یکی از مسایل عمده در تولید چنین شبکه هایی تبدیل شده است [3]. یک راه حل مناسب برای کاهش مخاطراتی از قبیل جعل هویت یا جعل سند احراز هویت منبع منتشر کننده پیام است و در کنار آن، حفظ حریم خصوصی کاربر نیز از دیگر نیازهای مهم در شبکه های VANET است. احراز هویت، کمک می کند مهاجمین در شبکه، تشخیص داده شده و از حمله جلوگیری شود. همچنین حفظ حریم خصوصی، گمنامی هویت فرستنده را موجب شده و محرمانگی، مانع از فاش شدن پیام های ارسالی به گره ی غیر مجاز می گردد. در این مقاله، طرحی پیشنهاد دادیم که هر سه ویژگی ذکر شده را تامین کند و یک احراز هویت گمنام با حفظ محرمانگی برای ارتباطات بین خودرویی ارایه دهد. در ضمن، از محاسبات ساده تری نسبت به سایر پروتکل های ارایه شده تا کنون استفاده کردیم. این امر سبب می شود طرح پیشنهادی سربار محاسباتی پایین تری را به همراه داشته باشد.

کلمات کلیدی:

شبکه اقتضایی بین خودرویی، محرمانگی، احراز هویت، امنیت، گمنامی

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/656536>

