چکیده

یکی از اولویت‌های اصلی تعداد زیادی از دولت‌های جهان تعریف مکانیسم‌ها و طرح‌هایی است که می‌تواند به حل مشکلات ترافیکی و سوانح خودرویی که جامعه‌ی مدرن با آن مواجه است، کمک کند. بهبودهای اخیر در نرم‌افزار، سخت‌افزار و تکنولوژی ارتباطات، در حال قدرت بخشیدن به طراحی و پیاده‌سازی چندین نوع از شبکه‌های توسعه‌یافته و مستقرشده در محیط‌های مختلف می‌باشد. در چند سال گذشته، شبکه‌ای که توجه زیادی را به خود جلب کرده، شبکه‌ی بین خودرویی (VANET) است. در حال حاضر VANET به دلیل چشم‌انداز بدیع و جذاب، از قبیل ایمنی جاده‌ها، بهره‌وری در حمل‌ونقل و سیستم‌های حمل‌ونقل هوشمند توجهات قابل‌ملاحظه‌ای را به سمت خود معطوف کرده است.

امنیت شبکه‌های خودرویی یک چالش اصلی را تشکیل می‌دهد که می‌تواند روی برنامه‌های کاربردی و توسعه‌های آتی تأثیرگذار باشد. علاوه بر امنیت مسافران و رانندگان، داشتن راه‌حل‌های قابل‌اعتماد برای ارتباط بین شرکت‌کنندگان و همچنین دسترسی به خدمات امن و تصدیق شده، مهم می‌باشد. درنتیجه، معماری‌های امنیتی مناسب باید برای فراهم کردن ارتباطات امن بین وسایل نقلیه و اجازه‌ی دسترسی خدمات مختلف در نظر گرفته شوند. علاوه بر این، نیاز به مکانیسم‌های امنیتی مناسب برای هر محیط شبکه خودرویی و باهدف فراهم کردن اطمینان، احراز هویت، کنترل دسترسی، تصدیق و دسترسی خدمات امن وجود دارد.

ما در این پایان‌نامه به بررسی چالش‌های امنیتی موجود در بخش‌های مختلف تکنولوژی VANET، ازجمله چالش‌های امنیتی در انتشار داده و مسیریابی، خوشه‌بندی، انبوهش داده، احراز هویت پرداخته‌ایم. با تجزیه‌وتحلیل تعدادی از مکانیسم‌ها و راهکارهای امنیتی موجود و مقایسه‌ی بین برخی راهکارها و همچنین معرفی مزایا و معایب برخی از طرح‌های موجود، چشم‌اندازی از تلاش‌های صورت گرفته در زمینه‌ی برقراری امنیت در شبکه‌های بین خودرویی را ترسیم نموده‌ایم.

کلمات کلیدی: شبکه‌های بین خودرویی، احراز هویت، چالش‌های امنیتی، حریم خصوصی، محرمانگی، تهدیدات امنیتی