عنوان مقاله:
پروتکل احراز اصالت در شبکههای حسگر سلسلهمراتبی

محل انتشار:
چهارمین کنفرانس انجمن رمز ایران (سال: 1386)

تعداد صفحات اصل مقاله: 8

نویسندگان:
هانی صالحی سیچانی - *دانشگاه صنعتی اصفهان*

علی فانیان - *دانشگاه صنعتی اصفهان*

مهدی برنجکوب - *دانشگاه صنعتی اصفهان*

خلاصه مقاله:
احراز اصالت و مدیریت کلید یکی از مسائل مهم در طراحی و توسعه شبکههای حسگر امن میباشد. استفاده از شبکههای حسگری که در آن تمامی گرهها دارای سطح مدیریتی و توان پردازشی یکسانی هستند، باعث پایین آمدن کارایی شبکه میشود. با استفاده از شبکههای حسگر سلسلهمراتبی میتوان کارایی شبکه را چه در پروتکلهای مسیریابی و چه از لحاظ امنیتی افزایش داد. از آنجا که فرایند احراز اصالت و برقراری کلید به عنوان اساسیترین رکن برقراری امنیت در شبکه است، این الگوریتمها بایستی به نحوی در شبکه طراحی و پیاده سازی شوند که کمترین بار محاسباتی و پردازشی را بر گرهها تحمیل نمایند. در این مقاله برای احراز اصالت گرههای دارای توان بالا به گرههای شبکه حسگر، نوعی گواهی بر مبنای الگوریتم رمزمتقارن و پروتکل تسلا پیشنهاد میگردد که در عین حالی که دارای کمترین بار محاسباتی بر روی گرهها است، پیامهای کنترلی کمی را نیز بر روی شبکه تحمیل مینماید.

کلمات کلیدی:
ارتباطات بیسیم، شبکههای حسگر سلسلهمراتبی، احراز اصالت، تسلا، امنیت شبکه

لینک ثابت مقاله در پایگاه سیویلیکا: