

عنوان مقاله:

یک روش بهبود یافته مدیریت کلید مبتنی بر ID در شبکه حسگر بی سیم

محل انتشار:

اولین کنفرانس ملی مهندسی کامپیوتر و فناوری اطلاعات (سال: 1395)

تعداد صفحات اصل مقاله: 6

نویسندگان:

احسان بیگی ساکی
سیدجواد میرعابدینی

خلاصه مقاله:

شبکه های سیار اقتصادی مجموعه ای از گره های متحرک هستند که در یک محیط پخش شده و به جمع آوری اطلاعات می پردازند. یکی از خصوصیت های این شبکه ها این است که از زیرساخت مشخص و طراحی شده ای استفاده نمی کنند. از ویژگی های مهم در این شبکه ها سهولت در پیاده سازی و عدم محدودیت در استفاده می باشد. با توجه به ساختار این شبکه ها امنیت و مدیریت کلیدها از اهمیت فوق العاده ای برخوردار می باشد. بیشتر شبکه های حسگر از یک کلید مشترک بین تمام گره ها استفاده می کنند تا سربار ارتباطی را حداقل کنند. این روش ها نسبت به بسیاری از حملات مثل حمله ی سرقت-تایید کننده، حمله ی اجرای مجدد، حملات عدم مصالحه و غیره، آسیب پذیر است. در این مقاله، ما با استفاده از جفت سازی دو خطی یک روش کارآمد مبتنی بر ID برای مدیریت کلید ارایه می کنیم. روش پیشنهادی بار محاسباتی کمی دارد و در برابر بسیاری از حملات در شبکه حسگر بی سیم مقاوم بوده و همچنین امنیت ارتباطات شبکه را نیز به طور همه جانبه تامین می کند.

کلمات کلیدی:

شبکه حسگر بی سیم، جفت سازی دوخطی، رمزگذاری مبتنی بر ID، امنیت

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/584624>

