عنوان مقاله:
طرح پیش توزیع کلید بر اساس باقیمانده در شبکه های مه

محل انتشار:
هجدهمین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات (سال: 1401)

تعداد صفحات اصل مقاله: 13

نویسندگان:
کمال پایکن - *استادیارگروه ریاضی، واحد گرمسار دانشگاه آزاد اسلامی، گرمسار، ایران*

محمد حبیبی - *دانشیار گروه ریاضیء دانشگاه تفرش تفرش, ایران*

میترا حاجی سیدجوادی - *کارشناسی ارشد نرم افزار، آموزش پرورش منطقه ۷، تهران؛ ایران*

خلاصه مقاله:
شبکه های حسکر بی سیم (WSN) از هزاران گره حسگر کوچک تشکیل شده اند که قادر به شناسایی، محاسبه و انتقال داده ها ازطریق شبکه ها هستند. اگرچه محدودیت های منابع خاصی وجود دارد. انتقال بی سیم هنوز یک روش موثر برای انتقال اطلاعاتاست و انتقال امن داده ها در WSN بسیار مهم است. تکنیک های مدیریت کلیدی برای اهداف امنیتی ایجاد شده است. پیشتوزیع کلید یکی از روش های مدیریت کلیدی است که برای تخصیص کلیدها به دستگاه ها قبل از استقرار آن ها در شبکه هایحسگر بی سیم استفاده می شود. چالش های این طرح ها شامل مصرف حافظه به دلیل منابع محدود دستگاه. مقیاس پذیری،اتصال و انعطاف پذیری در برابر حملات گره گیری است. طرح های ترکیبی با ویژگی های خنثی. که مبتنی بر ساختار ریاضیهستند و هزینه محاسباتی و ارتباطی کم را تحمیل می کنند». در پیش توزیع کلیدی و امنیت اطلاعات شبکه های حسگر بی سیماستفاده می شوند. به علاوه، امنیت در محاسبات مه چند وجهی بوده و یک چالش خاص ایجاد یک کانال ارتباطی امن بینگره های مه و دستگاه های پایانی است. این امر بر اهمیت طراحی طرح توزیع کلید کارآمد و مخفی برای تسهیل گره های مه ودستگاه های پایانی برای ایجاد کانال های ارتباطی ایمن تاکید می کند. طرح های توزیع کلید امن موجود که برای شبکه هایسلسله مراتبی طراحی شده اند ممکن است در محاسبات مه قابل اجرا باشند. اما هزینه های محاسباتی و ارتباطی بالایی رامتحمل می شوند و بنابراین حافظه قابل توجهی را مصرف می کنند. در این مقاله. ما یک طرح سلسله مراتبی پیش توزیع کلیدجدید بر اساس "طراحی باقیمانده " برای شبکه های مه پیشنهاد می کنیم. طرح توزیع کلید پیشنهادی برای به حداقل رساندنهزینه ذخیره سازی و مصرف حافظه و در عین حال افزایش مقیاس پذیری شبکه طراحی شده است. این طرح هم چنین به گونهای طراحی شده است که در برابر حملات تسخیری گره ایمن باشد.

کلمات کلیدی:
محاسبات مه شبکه های سلسله مراتبی، توزیع کلید، امنیت، شبکه های حسگر بی سیم

لینک ثابت مقاله در پایگاه سیویلیکا: