عنوان مقاله:
شناسایی و ارزیابی روشهای مدیریت کلید در شبکه حسگر بیسیم

محل انتشار:
اولین همایش ملی کامپیوتر،فناوری اطلاعات وارتباطات اسلامی ایران (سال: 1394)

تعداد صفحات اصل مقاله: 11

نویسندگان:
محمدحسن عطار - *دانشجوی کارشناسی ارشد،*

مهدی خلیلی - *استادیار دانشگاه پیام نور،*

خلاصه مقاله:
تبادل کلید به صورت امن در شبکه های بی سیم از جمله شبکه های ح سگر بی سیم، یکی از مقوله هایی ا ست که علاوه بر م شکلات امنیتی، از نظر بار پردازشی روی گرههای حسگر همیشه مورد توجه جدی بوده است. تکنیک های رمزنگاری پیچیده به راحتی از روش های جابجاییا جایگزینی استفاده نمی کنند. در عوض از یک کلید محرمانه برای کنترل یک توالی طولانی از جابجایی و جایگزینی های پیچیده استفاده می کنند.کلیدهای رمزنگاری و الگوریتم های رمزنگاری با یکدیگر همکاری می کنند تا یک متن اولیه را به یک متن رمزی تبدیل کنند. در اغلب موارد الگوریتم رمزنگاری ثابت و شناخته شده است و این کلید رمزنگاری است که یک نسخه یکتا از اطلاعات رمزنگاری شده تولید می کند. در این مقاله به شناسایی این کلید ها و مدیریت آن ها می پردازیم

کلمات کلیدی:
کلید عمومی، کلید خصوصی، شبکه حسگر، رمزنگاری