بخشی از ترجمه مقاله

عنوان فارسی مقاله :

رمزگذاری داده های مبتنی بر مکان برای شبکه های حسگر بی سیم با استفاده از کلیدهای پویا

عنوان انگلیسی مقاله :

Location-based data encryption for wireless sensor network using dynamic keys

توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، اینجا کلیک نمایید.

بخشی از ترجمه مقاله

5 Conclusions

Combining the concept of location with the merits of key-insulated systems, we introduced the first location-based data encryption for WSNs using dynamic keys. Our scheme allows a sensor node to generate a flexible ciphertext for some packet composed of many datagrams such that only the designated data aggregator has the ability to decrypt. To demonstrate the authenticity of some packet, the data aggregator is capable of revealing an ordinary signature for public verification. Our proposed protocol is conversion-free and provides unlimited time periods and random-access key-updates. In the proposed scheme, each sensor node can periodically update its private key while the corresponding public one remains unchanged. The underlining security assumption of our scheme is based on the well-known BDHP along with CDHP over elliptic curves. We also addressed detailed security proofs and precise advantage analyses to show the feasibility of our work.

5. نتیجه گیری

با ترکیب مفهوم مکان با سیستم های عایق گذاری کلید، ما به معرفی رمزگذاری داده های مبتنی بر مکان اول برای شبکه گیرنده بی سیم با استفاده از کلید های پویا پرداختیم. طرح ما اجازه می دهد تا یک گره حسگر به ایجاد یک متن رمزگذاری شده انعطاف پذیر برای برخی از بسته متشکل از بسیاری از دیتاگرام بپردازد به طوری که تنها جمع آوری داده ها تعیین شده دارای توانایی رمزگشایی باشند.

برای نشان دادن صحت برخی از بسته ها، جمع آوری داده ها قادر به آشکار سازی یک امضای عادی برای تأیید عمومی می باشد. پروتکل پیشنهادی ما بدون تبدیل است و مدت زمان نامحدودی و با دسترسی تصادفی کلید به روز رسانی را فراهم می کند. در طرح پیشنهادی، هر گره حسگر می تواند به طور دوره کلید خصوصی خود را به روز رسانی کند در حالی که کلید عمومی مربوط بدون تغییر باقی خواهد ماند.

فرض امنیت مورد تاکید طرح ما بر اساس شناخت BDHP همراه با CDHPبیش از منحنی های بیضوی است. ما همچنین اثبات امنیتی دقیقی را مورد بررسی قرار داده ومزیت دقیقی برای نشان دادن امکان سنجی کار ما مورد تجزیه و تحلیل قرار گرفت.