عنوان پایاننامه

تحلیل و طراحی پروتکلهای احراز هویت سبک برای اینترنت اشیاء

چکیده پایان نامه

پیش بینی ها نشان میدهد که اینترنت اشیا (IoT) بسیاری از جنبه های زندگی روزمره را دستخوش تغییر خواهد کرد. این اینترنت به عنوان نسل بعدی سیستمها شناخته شده که انواع مختلفی از دستگاه ها را شامل سنسورها، محرک ها، دستگاههای GPS، موبایل و موارد دیگر را در بر دارد. طبق پیش بینی ها، تا سال ۲۰۲۰، اینترنت شامل بیش از ۵۰ میلیارد دستگاه متصل می شود که میتوانند داده ها را تولید و مبادله کنند.

با توجه به میزان نفوذی که اینترنت اشیاء در زندگی انسان خواهد داشد، باید کارکردش فاقد مشکلات امنیتی و، تا حد ممکن، مشکلات حریم خصوصی باشد. تامین امنیت در شبکه های ناهمگن کار دشواری است. علاوه بر این، باید توجه داشت که بسیاری از دستگاه های IoT قدرت و منابع پردازشی و ذخیره سازی محدودی دارند. از این رو، تکنیکهای متداول تامین امنیت که اغلب متمرکز نیز هستند، ممکن است پاسخگو نباشد و باید تکنیکهای جدیدِ سبک وزنی توسعه داده شوند.

در این پروژه روی مساله احراز هویت و تولید کلید جلسه در اینترنت اشیاء تمرکز شده است و پروتکل احراز هویت سبکی با توجه به قدرت پردازش محدود گرهها طراحی گردیده است. این پروتکل سلسله مراتبی بوده و دارای ویژگی مقیاس پذیری است. در طراحی پروتکل از خم بیضوی استفاده شده است و گرهها در حین احراز هویت کلید جلسه ای برای ارتباط امن تولید می کنند. پروتکل پیشنهادی در مقابل بسیاری از حملات شناخته شده مانند MITM مقاوم است و دارای ویژگی هایی نظیر Forward Secrecy می باشد. امنیت پروتکل طراحی شده هم از طریق استدلال و کاهش (reduction) به مسایل سخت پایه و هم با نرم افزار های بررسی خودکار امنیت مانند AVISPA بررسی شده است. همچنین ویژگی ها و بار محاسباتی پروتکل پیشنهادی با پروتکلهای پیشین مقایسه شده و مزایا و معایب هر یک استخراج شده اند.

کلمات کلیدی

اینترنت اشیا، احراز هویت، رمزنگاری سبک وزن، مدیریت کلیدها، رمزنگاری مبتنی بر هویت، خم بیضوی

کلمات کلیدی انگلیسی

Internet of Things, Authentication, Lightweight Cryptography, key Management, Identity-Based Cryptography, Elliptic Curve, AVISPA