عنوان مقاله:
هم طراحی سخت افزار-نرم افزار برای پیاده سازی پروتکل DTLS جهت استفاده در اینترنت اشیاء

محل انتشار:
سومین کنفرانس بین المللی اینترنت اشیاء و کاربردها (سال: 1398)

تعداد صفحات اصل مقاله: 6

نویسندگان:
محبوبه سادات هدائی - *دانشجو کارشناسی ارشد، دانشگاه اصفهان*

علی بهلولی - *عضو هیئت علمی دانشگاه اصفهان*

خلاصه مقاله:
افزایش تعداد دستگاه ها و ارتباطات بین آنها در اینترنت اشیاء باعث شده است که پیاده سازی مکانیزم های امنیتی به یکی از چالشهای این حوزه تبدیل شود. در پیاده سازی این مکانیزمهای امنیتی، باید ویژگیهای اینترنت اشیاء نظیر محدودیت در منابع و انرژی گره ها، زمان پاسخ و انعطاف در پشتیبانی از پروتکلهای جدید در نظر گرفته شود. رویکردهایی که تاکنون در این حوزه بوده اند رویکرد نرم افزاری محض یا سخت افزاری محض بوده است. پیاده سازی نرم افزاری توابع رمزنگاری موجب انعطاف پذیری بالا و کاهش سرعت میشود از طرف دیگر، طراحی کاملا سخت افزاری موجب افزایش سرعت و کاهش انعطاف پذیری میشود. در این پژوهش به منظور استفاده از هر دو مزیت روش نرم افزاری و روش سخت افزاری، روشی بر مبنای هم طراحی سخت افزار-نرم افزار برای پیاده سازی پروتکل DTLS توسط FPGA ارائه شده است. این روش هم از ویژگی سخت افزاری بودن مثل افزایش سرعت و همچنین از مزیت نرم افزاری بودن آن مثل افزایش انعطاف پذیری بهره می برد. در این تحقیق توابع رمزنگاری منحنی بیضوی، Sha256، مولد عدد تصادفی به صورت سخت افزاری پیاده سازی شده اند. این طرح 15% از کل منابع سخت افزاری FPGA را مصرف میکند و توسط نرم افزار ISE شبیه سازی و روی برد XC7Z100-FFG900 پیاده سازی شده است.

کلمات کلیدی:
اینترنت اشیاء، هم طراحی سخت افزار-نرم افزار، پروتکلDTLS ،FPGA