بسمه تعالی

امنیت در اینترنت اشیاء

تمرین پنجم: CoAP و Wireshark

CoAP مخفف عبارت Constrained Application Protocol است و توسط گروه IEFT توسعه داده شده است. CoAP از نظر معماری شباهت زیادی به HTTP دارد، با این تفاوت که این پروتکل برای دستگاه‌های محدود (Constrained) طراحی شده است و پکت های بسیار کوچکتری نسبت به HTTP دارد. در این تمرین قصد داریم به صورت عملی، با این پروتکل آشنا شویم.

صورت تمرین

- برنامه ماژول ESP خود را به نحوی توسعه دهید که پس از اتصال به شبکه وای فای محلی، به عنوان یک سرور CoAP عمل کند. مانند کاری که در تمرین قبلی و با استفاده از پروتکل HTTP انجام دادید، این سرور قرار است پس از دریافت دستور از سمت client، LED روی ماژول را روشن یا خاموش کرده و سپس نتیجه را به client ارسال کند.
  توجه: دقت کنید که در تمرین قبل با استفاده از ESP یک wifi hotspot ایجاد کردیم. در این تمرین نیازی به این کار نیست و می‌توانید با آدرس ip که به ESP از سمت شبکه محلی داده می‌شود به ESP متصل شوید.
- با استفاده از یک CoAP client، به شبکه وای فای محلی و سپس به سرور CoAP خود که با استفاده از ESP بالا آورده اید متصل شوید. به این منظور می‌توانید از ابزارهای معرفی شده در درس مانند libcoap یا اکستنشن copper استفاده کنید. با ارسال پیام های روشن و خاموش، LED روی بورد را روشن و خاموش کرده و نتیجه را گزارش کنید.
- Wireshark از قوی‌ترین ابزارهایی است که برای مشاهده پیام ها و پکت های جابجا شده در شبکه استفاده می‌شود. با استفاده از این نرم‌افزار و فیلتر کردن پیام ها بر اساس پروتکل آن‌ها، پیام های رد و بدل شده با پروتکل CoAP بین سیستم خود و ESP را نشان دهید.
  توجه کنید که ظاهر این نرم افزار کمی پیچیده به نظر می‌آید، اما کار کردن با آن خیلی ساده تر از ظاهرش می‌باشد!

نکات قابل توجه

- کدهای ESP، خروجی فایل wireshark در قالب pcap و همچنین گزارش تمرین را در یک فایل زیپ و با فرمت نامگذاری زیر در CW آپلود کنید:

SIOT_HW5_StudentID

- گزارش شما شامل توضیحات لازم و تصاویر مربوطه می‌باشد. توجه کنید که نمره اصلی این تمرین باتوجه به گزارش شما محاسبه می‌شود؛ بنابراین تلاش کنید توضیحات و تصاویر گزارشتان کامل باشد.