BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2023
http://excel.fit.vutbr.cz

Bezdrátová senzorová síť

Matúš Nosko

Abstrakt

Práce byla zaměřena na zabezpečenou senzorovou síť založenou na mesh topologii, postavenou na zařízeních ESP32 od společnosti Espressif. Zaměřuje se také na zabezpečení kódu a propojení této sítě s cloudem. Vytvořená síť mesh je dynamická, regenerativní a samoorganizující. Celá síť je postavena na Wi-Fi, takže je snadné ji připojit, protože jedinou podmínkou pro její fungování je mít v místě instalace Wi-Fi, takže není třeba mít žádné speciální zařízení pro připojení sítě k internetu - gateway-less. I když jeden uzel selže, síť se sama zorganizuje podle nově vytvořených podmínek a funguje dál. K zabezpečení zařízení se využívají state-of-the-art metody zabezpečení, jako je bezpečné zavádění firmwaru a šifrování paměti flash. Pro připojení sítě mesh k serveru se používá protokol MQTT. MQTT broker, databáze a rozhraní API jsou na straně serveru dockerizovány, takže je lze v případě potřeby snadno rozšířit. Zařízení mohou mít připojeny různé senzory a aktuátory a data z nich se ukládají na serveru. Celé toto řešení bylo implementováno v prostředí ESP-IDF a odzkoušeno na zařízeních ESP32-S3 a další detaily jsou vysvětleny dále v textu.

xnosko06@stud.fit.vutbr.cz, *síť mesh, mesh, ESP32, šifrování paměte flash, bezpečné spuštění firmwaru, asymetrická kryptografie, symetrická kryptografie, gateway-less, MQTT, Docker*

1. Úvod

Zařízení internetu věcí jsou všude kolem nás, např. chytré domácnosti, chytrá města atd., a jejich počet neustále roste. Motivací této práce je tedy vytvoření bezpečné bezdrátové sítě víceúčelových zařízení s připojením k internetu. Vytvoření ekosystému připraveného na škálovatelnost a rozmanitost měřených hodnot a řízených zařízení.

Stávající řešení často závisí na centralizované topologii, tj. na jediném bodě, ke kterému jsou připojena ostatní zařízení v dané síti. Z povahy centralizované topologie vyplývá, že existuje jediný bod selhání, a pokud tento bod selže, selže připojení celé síti k internetu a také selže celá síť. Obvykle jsou zařízení v senzorové síti jednoúčelová, tj. měří pouze jednu veličinu.

Internet věcí jako celek je velmi populární odvětví a odhaduje se, že tento trh bude v budoucnu dále růst [1]. Trh je nasycen velkými společnostmi, např. společnosti Xiaomi, Netatmo, Sonoff, a proto je v této oblasti velmi silná konkurence. Tyto společnosti se zaměřují především na populární Smart Home, ale také Smart Cities. Velkou nevýhodou takto nasyceného trhu je však také roztříštěnost ekosystémů, kdy mnoho značek potřebuje pro ovládání samostatnou aplikaci. Tuto nevýhodu si uvědomují i samotní výrobci, a proto se zaměřují na sjednocení do větších komunit, např. Home Assistant, Google Home, často však za cenu ořezání podporovaných funkcí zařízení.

Cílem tohoto projektu je vytvořit bezdrátovou senzorovou síť, která bude zahrnovat modifikovatelná zařízení zaměřená spíše na specializovanou část trhu, o kterou nemají velcí hráči z hlediska velikosti zájem. Takový trh zahrnuje zařízení, jako jsou fotovoltaické elektrárny, elektrické brány, technologie pro vodní hospodářství (např. frekvenční měniče) a vzhledem k splnění vysoké bezpečnosti a také zabezpečení zařízení, je možné využit toto řešení i v průmyslu a kritické infrastruktuře.

Výstupem je gateway-less senzorová síť postavená na technologii Wi-Fi s konfigurovatelnými zařízeními připojenými na server.

2. Architektura senzorové sítě

Implementovaná síť je založena na zařízení ESP32 společnosti Espressif[2]. Výhodou této platformy je Wi-Fi přímo na čipu, velikost paměti flash a její šifrování, pro představu běžné modely mají 4 - 16 MB paměti flash. Jako programovací jazyk je využit

C/C++, což má za následek delší dobu vývoje, ale lepší správu zdrojů a periferií. Zařízení jsou také chráněna bezpečným zavedením firmwaru, co znamená, že v zařízení může být spuštěn pouze firmware od autorizované osoby/autority. K propojení zařízení se používá technologie Wi-Fi - Mesh, která zajišťuje samouzdravování, samoorganizaci a autonomní fungování. Z názvu vyplývá, že se jedná se o decentralizovanou topologii typu mesh. Díky rozšířenosti a popularitě Wi-Fi není potřeba žádný propojovací bod tzv. gateway, a tak každé zařízení v síti (poz. v dosahu místní sítě Wi-Fi) může zprostředkovat připojení k internetu. Odesílání zpráv na server zajišťuje protokol MQTT. Zprávy jsou pak odesílány na MQTT brokera běžícího na serveru, kde jsou zpracovávány a ukládány, aby byla data ze senzorů k dispozici pro další zpracování, např. ve formě grafů. Na implementaci serverových technologii je primárně použit programovací jazyk Python. Databáze, MQTT broker, API jsou zadockerovány, co umožňuje jednoduchou škálovatelnost serverového řešení.

2.1 Komentář k plagátu

Obrázek 1 Jedná se o přístup ke konstrukci bezdrátové sítě v IoT, v níž jsou všechny uzly navzájem propojeny, aniž by byly všechny připojeny k hlavnímu uzlu. Tyto topologie se používají nejen v sítích internetu věcí, ale také např. v počítačových sítích, elektrických vedeních a při přepravě zboží. Tyto sítě se obvykle dokáží zotavit a reorganizovat, když jeden uzel, dokonce i hlavní uzel, selže a síť je opět funkční. V IoT sítích je hlavní zařízení obvykle připojeno současně k síti zařízení IoT i k síti Wi-Fi. Tento princip se používá ve známých technologiích, jako jsou ZigBee, Wi-Fi Mesh, Thread, a je použit i v tomto projektu.

Obrázek 2 Ukazuje architekturu sítě IoT vytvořené v tomto projektu. Jedná se o částečnou mesh síť, zařízení jsou připojena všechna, ale ne každé ke každému. Síť využívá Wi-Fi k připojení k internetu, ale také k vzájemnému propojení zařízení. To má obrovskou výhodu v tom, že pokud dojde k výpadku propojovacího bodu mezi sítí senzorů a Wi-Fi routrem, může roli hlavního zařízení převzít jiné zařízení v dosahu lokální Wi-Fi sítě, protože jedinou propojovací technologií je Wi-Fi. V příkladu na Obrázku 3 by v případě, že by zařízení Světlo vypadlo, převzalo by hlavní roli zařízení Zámek, a připojilo by se ke směrovači Wi-Fi. Ostatní zařízení by se přeorganizovala, např. obě zařízení Teploměr by se připojila k Vlhkoměru a ten k Zámku. Významnou výhodou je, že zařízení rozšiřují vlastní síť, a nemusí tak být všechna v dosahu místní sítě Wi-Fi, takže tato síť může být různě rozprostřena v prostoru a využívána na větších plochách, jako jsou zahrady, sady, parky. Zařízení komunikují mezi sebou a se serverem pomocí zpráv MQTT. Veškerá shromážděná data putují na server, kde jsou následně zpracována a uložena.

Obrázek 3 Zobrazuje připojení více sítí senzorů k serveru. Třeba poznamenat, že těchto sítí je `n`. Na serveru běží nástroj docker, který vytváří kontejnery, v nichž běží různé služby. Kontejner docker je v podstatě samostatný spustitelný softwarový balíček, který obsahuje vše potřebné pro spuštění služby, programu atd. Tyto kontejnery jsou izolovány od hostitelského systému a lze je vzájemně propojovat a umožnit tak jednotlivým programům vzájemnou komunikaci. Celá serverová část je ve formě kontejnerů docker. Toto řešení má obrovskou výhodu ve škálovatelnosti, protože pokud je třeba spravovat více spojení/dat, stačí spustit více kontejnerů. U velkých systémů se přidává load balancer, který rozděluje úlohy. Senzorové sítě se připojují ke MQTT brokeru na serveru, který zpracovává zprávy a odesílá je do rozhraní API, které je zpracovává a ukládá do databáze. Rozhraní API zároveň poskytuje data pro procházení stránek, kde může uživatel sledovat aktuální stav.

Obrázek 4 Zařízení jsou zabezpečena pomocí asymetrické i symetrické kryptografie. Asymetrická kryptografie zajišťuje bezpečné spuštění firmwaru. Soukromý klíč je v držení výrobce a veřejný klíč je bezpečně uložen v zařízení. Symetrická kryptografie se naproti tomu používá při šifrování paměti flash, kdy výrobce i zařízení mají stejné klíče. Tím je zařízení zabezpečeno proti neoprávněnému čtení a spuštění firmwaru. Zařízení spustí pouze firmware od ověřené osoby/výrobce. Komunikace mezi uzly je šifrovaná a také komunikace se serverem je rovněž šifrovaná, opět na principu symetrické a asymetrické kryptografie. Z principu Wi-Fi mesh sítě vyplývá, že nepotřebujeme žádnou bránu a tímto prostředníkem se může stát jakékoli zařízení. Koncová zařízení jsou zároveň víceúčelová, a mohou tedy měřit více fyzikálních jevů.

3. Závěr

Cílem práce bylo vytvořit zabezpečenou bezdrátovou senzorovou síť, tento cíl byl splněn. Navázal jsem spolupráci s firmou z průmyslu, která instaluje zařízení založené na ekosystému z této práce, v průmyslu, kritické infrastruktuře a vodohospodářství. V hledání nových spoluprací budu nadále pokračovat. Možnou budoucí prací je zaměřit se na spotřebu elektrické energie, implementaci kompatibility se technologiemi jako ZigBee, Thread.

Poděkování

Rád bych poděkoval svému vedoucímu prof. Dr. Ing. Pavlu Zemčíkovi za jeho rady a odborné vedení. Také mému bratrovi Ing. Svetozáru Noskovi za rady a trpělivost.

Literatura

[1] Shadi Al-Sarawi, Mohammed Anbar, Rosni Abdullah, and Ahmad B. Al Hawari. Internet of things market analysis forecasts, 2020–2030. In *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, pages 449–453, 2020.

[2] Espressif Systems Shanghai. ESP-IDF Programming Guide Get Started ESP32-S3. https://docs.espressif.com/projects/esp-idf/en/v4.4.4/esp32s3/get-started/index.html, 2023. Version: v4.4.4 Accessed: 2023-04-20.