Správa informačních technologií Plzeň

PLZEN LoRa

Návod na použití

Autor	Datum	Verze
SITMP	25.5.2017	1.0

SPRÁVA INFORMAČNÍCH TECHNOLOGIÍ MĚSTA PLZNĚ, příspěvková organizace

Dominikánská 4, 301 00 Plzeň, sit@plzen.eu, **www.sitmp.cz**
T +420 378 035 101, **F** +420 378 035 102, **IČ:** 66362717, **DIČ:** CZ66362717

1. Popis infrastruktury sítě PLZEN LoRa

Síť PLZEN LoRa je komunikační síť IoT vybudovaná na otevřené platformě LoRaWAN v nelicencovaném pásmu 868 MHz. Jedná se o bezdrátovou síť založenou na LPWAN (Low Power Wide Area Network) technologii, která umožňuje jednoduchou a energeticky nenáročnou komunikaci s velkým dosahem.
Pomocí této sítě lze zajistit připojení a komunikaci senzorových jednotek z lokalit, ve kterých není dostupná jiná vhodná přístupová technologie nebo el. napájení, a následně umožnit zpracování přenesených dat.

Gateway (brána)
Je základním prvkem sítě PLZEN LoRa a je analogií k vysílačům mobilních operátorů. Každá brána umožňuje připojení až desítkám tisíc věcí (nodů). Přes gateway procházejí data šifrovaně a proto je komunikace zabezpečná. Jedna gateway umožňuje pokrytí okolí s poloměrem cca 10 km, respektive 2-3 km v městské zástavbě.

Koncové zařízení (senzor/node)
Node v internetu věcí představuje koncové zařízení tzv. „věc“, ze které chceme získávat data. Tento node potřebuje ke své činnosti napájení (baterii nebo el. síť) a komunikační modul LoRaWAN. Node se dále musí zaregistrovat do sítě PLZEN LoRa v administraci uživatelského profilu. Node může být reprezentován například parkovacím senzorem, teplotním čidlem, hladinovým spínačem, odečtem elektroměru/plynoměru/vodoměru a dalšími „věcmi“.

PLZEN LoRa APP
Webová aplikace, která slouží pro registraci uživatelů, jejich nodů a zobrazení uložených dat. Uživatelé si jednotlivé nody mohou kategorizovat do jednotlivých virtuálních aplikací pro lepší orientaci ve větším množství připojených senzorů. Aplikace umožňuje vizualizaci přijatých dat pomocí tabulek, grafů, map a jejich export. Ke každému senzoru/veličině je možné nastavit v aplikaci PLZEN LoRa notifikace na email.

MQTT BROKER
MQTT broker je centrální bod systému, který se stará o výměnu zpráv v síti LoRaWAN. Zprávy jsou tříděny do tzv. témat (topic) a zařízení buď publikuje v daném tématu (publish), to znamená, že posílá data brokeru, který je ukládá a distribuuje dalším zařízením, nebo je přihlášeno k odběru tématu či témat (subscribe), a broker pak všechny zprávy s daným tématem posílá do zařízení.

Jedno zařízení samozřejmě může najednou být v některých tématech publisher, v jiných subscriber.

2. Definice pojmů

AES (Advanced-Encryption-Standard)
Standardizovaný šifrovací algoritmus. V síti LoRa se používá se 128-bitovými klíči.

DEVEUI
64-bitový identifikátor zařízení, který je zařízení (NODE) přiřazen výrobcem.

APPEUI
64-bitový identifikátor aplikace.

APPKEY
128-bitový aplikační klíč, slouží k autentizaci zařízení v síti a odvozují se od něho další klíče.

NwkAddr
Adresa sítě - 7-bitový identifikátor sítě

DevAddr
Adresa zařízení - 32-bitový identifikátor zařízení (NODE) v dané síti, prefix adresy zařízení je tvořen adresou sítě.

AppSkey
Aplikační šifrovací klíč je 128-bitový šifrovací klíč. Používá se pro zašifrování přenášených aplikačních dat. V případě OTAA je odvozen od APPKEY,, v případě ABP je jeho hodnota pro dané zařízení konstantní.

NwkSkey
Síťový šifrovací klíč je 128-bitový šifrovací klíč. Používá se pro výpočet MIC, tj. ověření integrity odeslaných dat. V případě OTAA je odvozen od APPKEY,, v případě ABP je jeho hodnota pro dané zařízení konstantní.

MIC (Message-Integrity-Code)
MIC je 4-bitový kód sloužící k ověření integrity zprávy. Je vypočítán pomocí NwkSkey a slouží jako “elektronický podpis” - umožňuje ověřit, že zpráva pochází z důvěryhodného zařízení a nebyla během přenosu modifikována.

OTAA (Over-The-Air Activation)
Zařízení (NODE) se připojí do sítě na základě APPEUI, DEVEUI, APPKEY a je mu dynamicky přiřazena síťová adresa.

ABP (Activation-By-Personalization)
Zařízení (NODE) se připojí do sítě na základě statické DevAddr a klíčů AppSkey, NwkSkey, jež jsou trvale uloženy v zařízení.

MQTT (MQ-Telemetry-Transport)
Je jednoduchý protokol pro předávání zpráv mezi klienty - NODY, aplikace - prostřednictvím centrálního uzlu - brokeru.

MQTT Topic
Topic je téma nebo kategorie, v níž se publikují jednotlivé zprávy. Klient buď může publikovat (publish) zprávy v určitém topicu (klient posílá data na broker) a nebo odebírat (subscribe) zprávy z určitého topicu (broker přeposílá data přijatá v rámci daného topicu klientovi).

Relax frame counter
Server a zařízení (NODE) udržují synchronizovanou hodnotu čítače, jež slouží k číslování přenášených datových rámců. Jsou akceptovány pouze takové rámce, které mají vyšší číslo, než rámce předchozí - toto je ochrana proti replay attack. Pokud zvolíte relax frame counter, nebudou se čísla rámců kontrolovat, čímž snížíte bezpečnost LoRa aplikace.

Receive window
Koncové zařízení (NODE) periodicky posílá data na server - po určité době, která se nazývá Receive window delay - dojde k otevření přijímacího okna, během něhož koncové zařízení naslouchá a očekává data ze serveru. LoRa používá dvě přijímací okna (RX1 a RX2)

RX1 data-rate offset
Změna přenosové rychlosti v okně RX1 oproti rychlosti použité koncovým zařízením pro vysílání.

RX2 data-rate
Přenosová rychlost v okně RX2