



Mozgásban lévő csomópontokból álló IoT szenzorhálózat

Acikksorozat előző részében áttekintettük az IoT lehetséges felhasználási területeit az okosváros-koncepció vonatkozásában és ígéretet tettünk arra, hogy a következő részben tovább vizsgálódunk, megnézzük, hogyan lehet élő erőforrásokat monitorozni az E-IoT eszközökkel. Elmélyedünk benne, hogy milyen technológia teszi lehetővé például egy folyamatosan mozgásban lévő csomópontokkal rendelkező hálózat felépítését, továbbá hogy milyen technikai és gazdasági megfontolások alapján lehet eldönteni, hogy az adott feladatra saját internetkapcsolattal rendelkező okosszenzort vagy helyi hálózatban működő változatot célszerű-e telepíteni.

A megoldandó probléma

Korábbi cikkeinkben részleteztük, hogy IoT okosszenzor-hálózatok tervezésekor gyakran érdekesebb lokális vezetéktelen technológiákat használni és az összegyűjtött szenzordatokat egyetlen ponton – célszerűen egy LPWAN átjárón keresztül – az Internet felé kicsatolni. A mérnökök számára számtalan lokális vezeték nélküli technológia áll rendelkezésre a feladat megoldásához, van amelyik energiatakarékossági szempontból, van amelyik gyorsaság szempontjából előnyösebb. Előfordulhat azonban olyan eset, amikor az előírt feladat a szokásosnál is nagyobb kihívás elé állítja a rendszerintegrátort. Ilyen esettel pályafutásom során először Franciaországban találkoztam, ahol állami építkezésen dolgozó munkások nagy hőségnek, illetve extrém páratartalomnak való kitettségét kellett ellenőrizni – a preferált megoldás egy a röntgenben dolgozó egészségügyi személyzet által viselt online doziméterhez hasonló eszköz volt. Mivel a munkások állandóan mozgásban vannak egy nagy kiterjedésű munkaterületen, nagyon nehéz volt az üzemeltetőnek gazdaságosan megoldani ezt az előírást. Az alkalmazott, jelentősen egyszerűsített módszer az



1| Mesh hálózati protokoll segítségével követhető a munkások mozgása

volt, hogy a munkás egy UHF chippel ellátott kártyát viselt, ezzel azonosítva magát a területen relatív nagy sűrűségben elhelyezett mérőállomások előtt elhaladva, amiből a rendszer hozzávetőlegesen ki tudta kalkulálni az adott (magas) hőmérsékleten és páratartalmon eltöltött időt. Sokkal pontosabb eredményt kaphatunk akkor, ha a szenzorok felkerülnek az azonosítókártyára, és egy nagyon alacsony fogyasztású, lokális mesh hálózati protokoll segítségével adataikat maguk tudják az átjáró felé kommunikálni (1. ábra).

Az ilyen hálózatok legfontosabb tulajdonsága az, hogy a csomópontjaik folyamatos mozgásban vannak, és így kell egy változó felépítésű mesh hálózatot fenntartani. Az olvasó joggal

kérdezheti, hogy miért nem használunk csillagtopológiát, illetve az ilyen feladatokra ideálisnak látszó celluláris hálózat adta lehetőségeket, hiszen az E-IoT eszközkészletében is megtalálható NB-IoT és LTE-M kommunikációra épülő okosszenzorok ezt a feladatot pillanatok alatt megoldanák. Gondoljunk bele abba is azonban, hogy miként oldható meg gazdaságosan a tápellátás, és mekkorák lesznek a kommunikációs költségek, ha például ezer csomópont esetén van szükség ilyen megoldásra. Ahogy egy másik klasszikus feladatnál, ami mezőgazdasági területen jelentkező dél-amerikai projektjeink során. Adott egy nagyszámú szarvasmarhacsorda, amelynek tagjai hatalmas területen legelnek és napi rendszerességgel megjelennek az itatónál, ahol lehetőség nyílik az egyedek számbavételére (2.



Élőállomány vezetékmentes hálózata

Szarvasmarhák számlálása az
ítatónál napi rendszerességgel

2| Állatok nyilvántartása a szabadban

ábra). Erre az egyik jó megoldás a csorda – tagjainak – hálózatba kapcsolása, ahol is a csomópont megjelenése adott időpontban a hálózatban elvi lehetőséget ad a megoldásra. A fő kérdések tehát, hogy vajon melyik technológia teszi (egyszerűen) lehetővé ezres nagyságrendben csomópontok integrálását, hogyan fognak ezek egy nagy mesh hálózatot alkotni, és hogyan jut el az adat az egyed által viselt szenzorból bonyolult útvonalkalkuláció és adatvezérlő nélkül az átjáróra?

A technológia kiválasztása

A lokális vezetékmentes hálózatok és technológiák, mint például a Bluetooth, WiFi, Zigbee és Thread, egyre fontosabb szerepet játszanak a modern

kommunikációs rendszerekben. A mozgó és folyamatos mozgásban lévő csomópontok esetében azonban számos problémával kell szembenézni. Az egyik legnagyobb kihívás a jel stabilitása; hiszen a mozgás során a csomópontok távolsága folyamatosan változik, ami a jel minőségének ingadozásához vezethet. Ezenkívül a mozgó csomópontok gyakran lépnek be és ki a hálózatból, ami a kapcsolatok megszakadásához és látenciához vezethet.

A Bluetooth technológia esetében a rövid hatótávolság korlátozza a mozgó csomópontok közötti kommunikációt, különösen nagy távolságok esetén. Az alacsony energiafogyasztású Bluetooth (BLE) megoldások általában korlátozott sávszélességgel rendelkeznek, ami problémát okozhat a nagy

adatmennyiségek átvitelénél, itt azonban minimális adatmennyiség átvitele a feladat, a problémát inkább a csomópontok maximális száma okozhatja. A WiFi technológia alkalmazása jobb megoldásnak tűnhet a nagyobb távolságok áthidalására, de mozgó csomópontok esetén a jelcsökkentés és a zavarok, például más WiFi hálózatok interferenciája súlyos problémákat okozhat, nem beszélve a kezdeti installációs költségekről és az energiafogyasztásról.

A Zigbee és Thread protokollok előnye, hogy alacsony energiaigényűek és kiterjedt hálózati topológiát támogatnak, de mozgó csomópontok esetében a hálózat stabilitása és az automatikus újrapcsolódás nem mindig garantált. A csomópontok közötti koordináció hiánya nehezíti a gyors adatátvitelt, ezért a valós idejű alkalmazásoknál, mint például az IoT rendszerek, komoly problémát jelent. Az energiatakarékosság szempontjából a mozgó csomópontoknak optimalizálniuk kell az energiafogyasztásukat, hogy fenntarthatóak a hosszú távú működést.

A működési megbízhatóság mellett az adatbiztonság is kulcsfontosságú kérdés. A mozgó csomópontok könnyen sebezhetővé válnak a lehallgatás és az adathalászat révén. A titkosítás és a megfelelő hitelesítési protokollok hiánya miatt a felhasználói adatok veszélybe kerülhetnek. A skálázhatóság is jelentős probléma, mivel a mozgó csomópontok

számának növekedése új kihívásokat teremt a hálózati tervezésben és menedzsmentben.

Folyamatosan mozgó csomópontok esetében a csatlakozási idő csökkentése és a zavarok minimalizálása elengedhetetlen a zökkenőmentes működéshez. Az újabb technológiák, mint az 5G, ígéretes megoldásokat kínálnak, de a régi rendszerekkel való kompatibilitás még mindig problémát jelenthet. A jövőbeli fejlesztéseknek figyelembe kell venniük a mozgó csomópontok különleges igényeit, hogy a vezetékmentes hálózatok hatékonyabbá tudjanak válni.

A lokális vezetékmentes hálózatok folyamatos fejlődése és a mozgó csomópontok kihívásai közötti egyensúly megtalálása kulcsfontosságú a jövő technológiái számára. A tervezőknek és a mérnököknek folyamatosan új módszereket kell keresniük a problémák megoldására, hogy a lokális vezetékmentes hálózatok továbbra is hatékonyan működhessenek. A felhasználói élmény javítása érdekében a zavarok minimalizálása és a hálózati teljesítmény optimalizálása elengedhetetlen. Az ilyen kihívások leküzdése érdekében a kutatásoknak új megoldásokat kell kidolgozniuk, amelyek a mozgó csomópontok igényeit szolgálják.

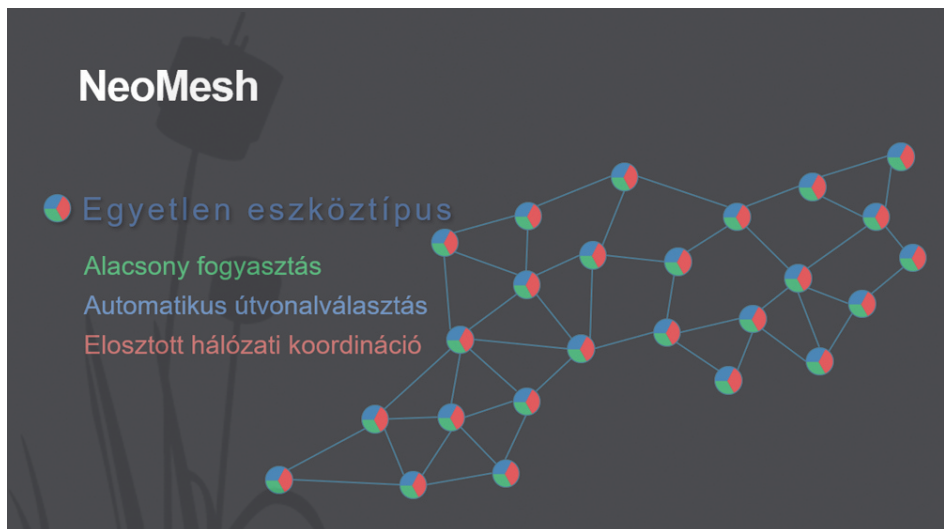
A NeoMesh mint az egyik lehetséges megoldás

Az Endrich az E-IoT eszközeiben az elosztott okosszenzor-hálózatok esetén a NeoMesh technológiát preferálja. Szemben a hagyományos lokális WLAN technológiákkal ez a protokoll egyetlen eszközben egyesíti a három fő funkciót, az alacsony fogyasztás melletti automatikus útvonalválasztást, az ad-hoc hálózatfelépülést és az elosztott hálózati koordinációt. Nincs szükség külön-külön eszközökre, egy NeoMesh modulon futó szoftverprotokoll mindezt elintézi számunkra.

A NeoCortec NeoMesh technológia egy új típusú mesh architektúrát kínál, amely eltér a hagyományos topológiáktól (3.

ábra). A NeoMesh egy teljesen összekapcsolt hálózatot biztosít, ahol a csomópontok egyszerre több feladatot is ellátnak: mint irányítás, koordináció és végberendezés-funkciók. Ez a megoldás a Wireless Mesh Networking Protocol segítségével paradigmaváltást jelent a hagyományos hálózati architektúrákhoz képest.

Ahelyett, hogy központi hálózatkezelő irányítaná a csomópontok közötti kommunikációt, a NeoMesh autonóm intelligens csomópontokat alkalmaz alapként, amelyek lehetővé teszik a közvetlen kommunikációt a csomópontok között központi fennhatóság nélkül. Ennek eredményeként egy egységes hálózat jön létre, amely zökkenőmentesen működik,



3| A NeoMesh technológia mesh architektúrája

függetlenül attól, hogy mekkorára nő vagy mennyire válik bonyolulttá. Ahogy egyre több csomópont csatlakozik a hálózathoz, azok zavartalanul kapcsolódnak a meglévő csomópontokhoz, létrehozva egy összekapcsolt kommunikációs hálót, amely nagy távolságokat is képes áthidalni.

Ez a rugalmasság és skálázhatóság különösen értékes az E-IoT platform kiterjesztéseként, ahol száz vagy akár ezer érzékelőt kell lefedni. A protokoll egyik lenyűgöző tulajdonsága a szabadalmaztatott irányítási mechanizmus, amely biztosítja, hogy az adatok zökkenőmentesen áthaladjanak a hálózaton, még akkor is, ha akadályok merülnek fel az RF (rádiófrekvencia) úton, vagy ha a csomópontok mozognak a hálózaton belül.

A hagyományos hálózatok gyakran teljesítményproblémákkal küzdenek, amikor a csomópontok el vannak zárva vagy dinamikusan változtatják helyüket. Ezzel szemben a NeoMesh Networking Protocol (4. ábra) kiküszöböli ezeket a gondokat, garantálva a megbízható adatátvitelt minden időben. A rendszer így ellenáll a környezeti tényezőknek és a hálózaton belüli dinamikus változásoknak. Függetlenül attól, hogy a csomópontokat hozzáadják, eltávolítják vagy áthelyezik, a hálózat robusztus és teljesen működőképes marad, biztosítva az összes eszköz és felhasználó megszakítás nélküli csatlakozását.

A protokoll figyelemre méltóan képes kezelni a gyenge pontokat a valós hálózatokban. Egy újabb csomópont egyszerű hozzáadásával, amely

A NeoMesh kiküszöböli a korlátokat



• Masszív skálázhatóság

- Decentralizált hálózatmenedzsment
- Egyedi SpeedRouting protokoll
- Lehetővé teszi az ezres nagyságrendű csomópontszámot



• Elemes táplálás

- A szoros szinkronműködés lehetővé teszi a kis energiafogyasztást



• Kábelszintű megbízhatóság

- Handshake minden periódusban (32-bit CRC), hiba esetén újraküldés
- A zajszűrésre a 15 csatorna közötti frekvenciaváltogatás

4) A NeoMesh Networking Protocol garantálja a megbízható adatátvitelt

megkapja a megfelelő hálózati azonosítót, zökkenőmentesen integrálódik a meglévő hálózatba, erősítve annak lefedettségét és teljesítményét. A NeoMesh technológia középpontjában egy robusztus protokollverem áll, amely integrált biztonsági és megbízhatósági funkciókat kínál. A biztonság egyik kulcsfontosságú eleme, hogy az összes vezeték nélküli kommunikációt AES128 titkosítással védik, így a payload adatok és a hálózati kommunikáció elérhetetlenné válnak a megbízhatatlan entitások számára.

A rendszer hosszú távú teljesítményre van tervezve, alacsony energiafogyasztással, ami lehetővé teszi, hogy az akkumulátorok évekig működjenek. A NeoMesh hálózat egy idősinkronizált protokollt követ, amelynek során minden csomópont idejének nagy részét alvó állapotban tölti. Ez az architektúrális megközelítés előre jelezhető energiafogyasztási mintázatot biztosít, így minden csomópont szinte azonos mennyiségű energiát fogyaszt, lehetővé téve, hogy évekig hatékonyan működjenek.

Az E-IoT Neo-Mesh helyi érzékelőhálózati kiterjesztése 868 MHz frekvencián működik, hogy áthidalja más protokollok problémáit zord ipari környezetekben. Ha a szub-GHz hálózatokat összehasonlítjuk a WiFi-vel és a Bluetooth-szal, a hasonló antennák és adási teljesítmény mellett, nyilvánvaló, hogy a szub-GHz hálózatok

hosszabb hatótávolságot kínálnak. Ennek oka, hogy az alacsonyabb rádiófrekvenciás hullámok nem olyan könnyen nyelődnek el fizikai anyag által, mint a WiFi és Bluetooth esetében használt 2,4 GHz-es jelek.

A NeoMesh veremben beágyazott automatikus irányítás lehetővé teszi a hálózati koordinációt a csomópontok között alacsony energiafogyasztás mellett. A decentralizáció, a hatékony sebességirányítási protokoll és az ad-hoc hálózatépítés lehetővé teszik a hatalmas skálázhatóság elérését akár ezres nagyságrendű csomóponttal.

A NeoMesh protokoll képességei ideálissá teszik azt intelligens érzékelők számára, amelyek nagy léptékű ipari komplexumokban, például gyárakban, épületekben, ingatlanokban és üzletekben kerülnek telepítésre, tökéletes helyi vezeték nélküli hálózati megoldást kínálva az E-IoT koncepció kiterjesztéséhez a fent említett mozgásban lévő hálózatokra is.

A megbízható hálózati protokoll alapja a működési megbízhatóság és az adatbiztonság együttes jelenléte

A NeoMesh adatsere egy kábeléhez hasonló megbízhatósággal történik, a csomópontok közötti HandShake révén, amely minden ugrásnál 32-bites CRC-t és automatikus újrapróbálkozást biztosít CRC hiba esetén. A megbízhatóság



5| A NeoMesh által nyújtott biztonság

további fokozása érdekében a NeoMesh frekvenciaugrást alkalmaz, amely kiterjeszti a kommunikációt az egész frekvenciasávra (mind a 15 csatornára), elkerülve a túlhasznált csatornákat, miközben javítja a zajvédelmet is. A megbízhatóság nem csupán azt jelenti, hogy az adatok eljutnak a célhelyre, hanem azt is, hogy a helyes adatok érkeznek meg. A CRC ellenőrzés, ahogy korábban említésre került, jó arra, hogy biztosítsa, hogy nincsenek bithibák, de azt nem tudja garantálni, hogy a payload adatokat nem egy rosszindulatú forrás generálta.

A megbízhatóságot és a biztonságot gyakran összekeverik a hálózatokkal kapcsolatos írásokban, pedig ezek viszonylag jól értelmezhető, de nagyon is eltérő tulajdonságok. Míg a megbízhatóság a hálózat képességét írja

le az adatok és a szolgáltatás integritásának fenntartására, a biztonsági szint azt mutatja meg, hogy mennyire immunis a hálózat a lehallgatással és a támadásokkal szemben.

A NeoMesh (5. ábra) számára az erős adatvédelem alapvető fontosságú, az adatok csomópontok közötti cseréje az ipari szabványú AES128 titkosítási módszerrel történik, és a biztonságos kommunikáció érdekében egy kihívás-válasz kézfogást (challenge-response handshake) valósít meg, amely megakadályozza a visszajátszási támadásokat és biztosítja a biztonságos payload-adatcserét.

A NeoMesh két erős funkcióval rendelkezik a protokollverem magjába ágyazva, tovább növelve a megbízhatóságot a kommunikációs

kapcsolat védelme érdekében. Először is az összes adat, amely a hálózatban csomópontok között cserélődik, valamint a teljes RF kommunikáció AES128 titkosítással védett. Az AES kulcs az a hálózati kulcs, amelyet a rendszer konfigurálója programozhat, és biztonságosan tárol minden modulban. Másodszor, amikor visszaigazolt kommunikációt használunk a forrás és a cél között, automatikus kihívás-válasz kézfogás kerül bevezetésre, amely biztosítja, hogy a célcsomópont csak akkor fogad el payload-adatokat egy másik csomóponttól (forrástól), ha a payload-adatok tartalmazzák a cél által adott kihívásra a helyes választ. Ez a kihívás-válasz hitelesítés egyedi a NeoMesh számára, és teljesen zökkenőmentesen kezeli a

protokollverem. Hatékonyan blokkolja az úgynevezett visszajátsszási támadásokat, ahol egy rosszindulatú eszköz rögzíthetne egy korábban elküldött payload-csomagot, amely bizonyos vezérlőfunkciót tartalmazhat, mint például „ajtónyitás”. A tettes később újra továbbítja (visszajátssza) az üzenetet, amely kinyitná az ajtót – a NeoMesh kihívás-válasz hitelesítéssel ez nem lehetséges.

A NeoMesh-alapú E-IoT szenzoreszközök

A fenti feladatokra szolgáló megoldásokhoz a NeoMesh technológia kiváló elméleti alapot biztosít, azonban elengedhetetlen ezek gyakorlatba való átruházása is. Erre ad lehetőséget az



6) NeoMesh hálózat a standszemélyzet követésében

Endrich által fejlesztett termékkonceptió, a számtalan szenzorvégpont és átjáró, amelyek kiváló alapot adnak a közös termékfejlesztésre.

A müncheni Electronica 2024 kiállításon az Endrich standján a standszemélyzet is egy ilyen mozgó hálózatot alkotott ezzel is demonstrálva a technológiában rejlő lehetőséget (6. ábra) folyamatosan változó, mozgó csomópontok alkotta mesh esetén. A következő lapszámban ezt a kísérletet részletezzük majd.

