WSN és IoT

Az IoT megnevezés sokaknak már talán ismerősen cseng, az internet of things, azaz a dolgok internete gyakorlatilag a jelenlegi ismereteinkben létező internet ugrásszerű bővülését/bővítését jelenti. Az IoT az (egyik) oka az IPv6 bevezetésének, mivel a „klasszikus” IPv4 egyszerűen már nem rendelkezik elegendően nagy címtartománnyal ennyi új „bevándorló” számára.

A klasszikus interneten számítógépek kommunikálnak többnyire szerverekkel, és ez a séma bővült ki jó pár szereplővel az utóbbi pár évben. Megjelentek a felhők a konkrét szerverek mellett, és a klasszikus böngésző-PC-k mellett megjelentek a laptopok, tabletek, mobiltelefonok, okos karon hordozható kütyük, majd a különféle intelligens, vagy legalábbis annak mondott mindenféle egyéb, net-kapcsolattal rendelkező kütyük.

Net-kamerák, hőmérséklet-érzékelők, szórakoztató-elektronikai kütyük, otthoni világítás és fűtésfelügyeleti eszközök, gombnyomásra valami árut rendelő pvb-k (parasztvakító bigyók), intelligens hűtőszekrények, amik a tulaj tudta nélkül is képesek ezt-azt rendelni,..

Lehet, hogy a szöveg felütéséből érződik, hogy személy szerint nem vagyok nagy barátja az efféle kezdeményezések nagy részének, de jellemzően minden újdonság a menő dolgokkal villogó hipszterek kényszerű közreműködésével kerül be a köztudatba, és terjed el ott, elég csak a favágószakállas baltát soha nem látott egyedekre gondolni. Zárójel bezárva.

Szóval van egy nagy rakás kütyünk, ami saját IP-vel és jó eséllyel egyedi MAC címmel rendelkezik, és csatlakoznak a hálózatra, dobálják fel az adataikat a felhőkbe, vagy csak egyszerűen elérést biztosítanak az internet felől.

WSN

A WSN ennél a megoldásnál kicsit bővebb rendszert jelöl, sőt, ha úgy vesszük, az IoT is a WSN része. A rövidítés a wireless sensor network-öt takarja, azaz a vezeték nélküli szenzorhálózatot. Ennek alapjait 2003-ban a **DARPA** finanszírozásában a **Berkley Egyetem** fektette le a *„Smart dust”* (inteligens por) projekt keretein belül.

A hálózat technikailag szenzorokból áll, melyek leggyakrabban ad-hoc hálózatot hoznak létre az adattovábbítás céljára. Az adatfolyam ezekben a hálózatokban az átjátszókig (gateway) tart, ahol az

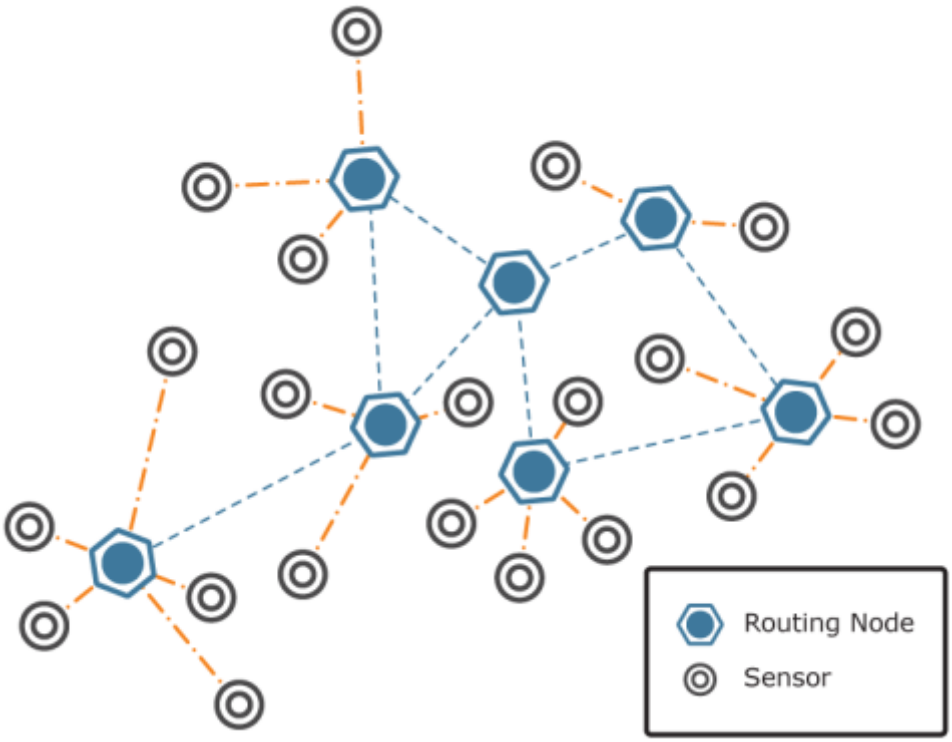
összegyűjtött adatok a feldolgozó rendszer felé kerülnek továbbításra.

Az eredeti koncepció szerint az adatfolyam csak egy irányban haladhat, azaz az érzékelők információit továbbítja, a fejlettebb WSN rendszerek lehetővé teszik a kétirányú forgalmazást is, azaz például a résztvevő szenzorok paraméterezhetők vagy parancsokkal vezényelhetők is.

Mivel az egységek itt nem, vagy legalábbis nem feltétlenül csatlakoznak az internethez, ez a hálózat egy csomó további kérdést és új definíciókat is felvet.

Ad-hoc hálózat

A WSN igazi előnyét a vezetékes szenzorkapcsolatokkal szemben a hibatűrő és alkalmazkodóképessége jelenti. Csakúgy, mint az maga az internet, a WSN is voltaképpen központi vezérlőrendszer nélkül, decentrális rendszerek összességeként működik. A kommunikáció formája (az osi modell alsó két-három szintje) nem definiált, azaz bármely rádiókommunikációra alkalmas protokoll és ezeknek a legkülönfélébb kombinációi is alkalmazhatók. A legtöbb ad-hoc hálózatnál alapfeltevés, hogy a kommunikáció egy „ugrásból”, azaz p2p nem valósítható meg.



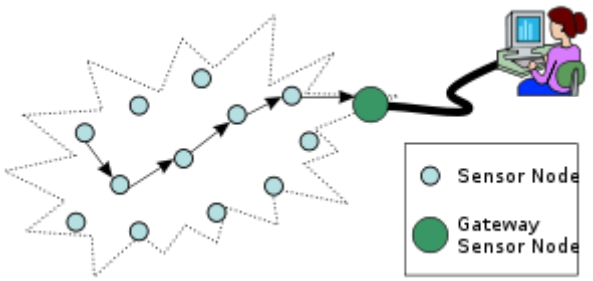
A szenzorok egy-egy rádiókapcsolattal rendelkező mikrokontrollerhez csatlakoznak és ezeknek az egységeknek a hálózata adja ki voltaképpen a WSN-t. Ezek az egységek az alábbi jellemzőkkel rendelkeznek:

- Minden egység rendelkezik rádiókapcsolattal
- A szenzorok ezekhez az egységekhez kapcsolódnak, a méréseket ezek továbbítják
- Az egységek képesek átjátszóállomásként is működni (multi-hopping)
- Az egységek adott esetekben parancsokat is képesek fogadni és értelmezni
- Bizonyos egységek átjáróként szolgálnak más hálózatok vagy rendszerek felé (gateway)

Multi-hop routing

Első nekifutásra foglalkozzunk csak az útvonallal. A multi-hop, azaz a többszörös ugrás azt jelenti, hogy a szenzortól a gatway-ig nincs közvetlen kapcsolat, hanem egy vagy több szenzort „átjátszó-állomásként” kell igénybe venni az adatok (vagy parancsok) célba juttatásához.

Még az is lehetséges, hogy a szenzor nagyobb energia felhasználásával (a rádióteljesítmény növelésével) közvetlenül is – azaz singe-hop routing-gal – el tudná érni a célállomását, de a WSN egyik definiált célra az alacsony energiafelhasználás, így ez a teljesítménynövekedés nem megoldható. Ez egyben azt is jelenti, hogy a WSN-nek nincs a klasszikus (ipari kommunikációs) értelemben vett topológiája, felépítése az internethez hasonlít (robusztus káosz-hálózat).



Alkalmazott protokollok

A WSN-nek nincs protokollra vonatkozó előírása, gyakorlatilag azt lehet elmondani róla, hogy az egységek valahogy kell, hogy rádiókapcsolatban legyenek egymással. Ez nyilván azt jelenti, hogy a hálózati kommunikáció egy része (vagy egésze) TCP/UDP átvitelre alkalmas protokollokkal (pl. Wifi, Bluetooth) működik, és akkor ezt a részt IoT-nek is nevezhetjük. De nyilván a kommunikációhoz bármely egyéb protokollt is felhasználhatjuk, például: IR, Wiegand, DASH7, ZigBee, WirelessHART, LoRaWAN, nRF24, RFID, GPRS,Thread, MiWi, Z-Wave, EnOcean, Eddystone, ANT, Insteon, stb…

A kommunikációs protokollok nagy része az ISM liszenszmentes rádiósávokat alkalmazza átvitelre, így a WSN alkalmazása legtöbb esetben nem igényel hatósági engedélyezést.

Energiafelhasználás

A WSN egyik törekvése az alacsony energiafelhasználás. Sok esetben a szenzorok és a rádiós mikrokontroller valahonnan a semmi közepéről kell, hogy sugározza a mérési eredményeit, ahol jó esetben napcella és akkumulátor, rosszabb esetben tartós alkáli-elem biztosítja a tápellátást.

Sérülékenység

Az IoT – bár erről nagyon kevés szó esik a propaganda-anyagokban – rendkívül sérülékeny és adott esetben nagyon nagy veszélyt jelenthet az internet felhasználóira. A kínai cégek milliószámra öntik a piacra termékeiket, melyeknek firmware-je általában admin jelszóval módosítható. A gond ezzel csak az, hogy a felhasználóknak erről általában fogalmuk sincs, így az alapértelmezett jelszót érintetlenül

hagyják.

Viszonylag egyszerű módszerekkel (például MAC szkenneléssel) beazonosíthatóak ezek az egységek, és egy egyszerű rápróbálkozással az is megállapítható, hogy a gyári jelszóval működnek-e. Több ilyen jellegű felmérés azt támasztja alá, hogy az internetről elérhető IoT egységek nagyon nagy százaléka probléma nélkül elérhető a default jelszóval (ez leggyakrabban a „tluafed”, azaz default visszafelé).

Így az IoT eszközök adatai (kamerák képei, tárolt felvételek, mérések, privát adatok..) is elérhetők, illetve a firmware is felülírható. Ha ez utóbbi megtörténik, hatalmas botnet hálózatok hozhatók létre ezekből az eszközökből, illetve ezeknek a millióiból, és szinte bármely webhely megbéníthető az ezekről indított túlterheléses (DDOS) támadásokkal. Ráadásul ez úgy is megtörténhet, hogy az IoT egység tulajdonosának fogalma sem lesz arról, hogy készüléke „másodállásban” milyen sötét akciókban vesz részt.

A tágabban értelmezett WSN-en (az IoT részeket leszámítva) ez a veszély egyelőre alacsony. A speciális (nem internetes) protokollok és a hálózatok nagyon egyedi felépítése egyelőre elegendő védelmet nyújt a nagyüzemi (bot-okkal megvalósított) behatolásokkal és zombivá alakításokkal szemben.

Azért persze ezek a hálózatok sem bombabiztosak; ha a hálózaton kevés a gateway, akkor jól elhelyezett rádiófrekvenciás zavaróegységekkel (jammerekkel) ezek a hálózatok is ellehetetleníthetők.

WSN, IoT, IPv6, DARPA, hálózat, smart dust, Berkley, ad-hoc, multi-hop routing, Wifi, Bluetooth, IR, Wiegand, DASH7, ZigBee, WirelessHART, LoRaWAN, nRF24, RFID, GPRS, Thread, MiWi, Z-Wave, EnOcean, Eddystone, ANT, Insteon, sérülékenység, DDOS