A UbiSec&Sens és a WSAN4CIP projektek

BUTTYÁN LEVENTE

Budapesti Műszaki és Gazdaságtudományi Egyetem, Híradástechnikai Tanszék,
Adat- és rendszerbiztonság laboratórium (CrySyS)
buttyan@crysys.hu

Az elmúlt fél évtizedben jelentős mennyiségű kutatástámogatás irányult a vezeték nélküli szenzorhálózatokkal kapcsolatos kutatások finanszírozására Európában és a tengerentúlon egyaránt. Ez az új technológia számos érdekes és hasznos alkalmazást tesz lehetővé a fizikai környezet paramétereinek (például hőmérséklet, nyomás, páratartalom, vibráció, fényerősség, akusztikai zaj stb.) folyamatos monitorozása, valamint a mért adatok automatikus begyűjtése és feldolgozása által.

A potenciális alkalmazások köre többek között magában foglalja a mezőgazdasági folyamatok optimalizálását, az ökológiai megfigyeléseket nagy kiterjedésű vagy fizikailag nehez megközelíthető területeken, a természeti katasztrófák előrejelzését, az ipari automatizálási folyamatok vezérlését, az épületek automatizálását, a közlekedési balesetek megelőzését, az idős emberek, illetve bizonyos krónikus betegségben szenvedők távoli megfigyelését és orvosi felügyeletét, valamint taktikai katonai alkalmazásokat.

Számos potenciális alkalmazás esetében felmerül az informatikai biztonság kérdése, ami magában foglalja egyrészt a vezeték nélküli kommunikáció védelmét, másrészt a szenzorhálózat működését biztosító algoritmusok és protokollok védelmét különböző rosszindulatú támadások ellen. Bár léteznek kipróbált biztonsági megoldások mind vezetékes mind vezeték nélküli hálózatokban, a szenzorhálózatok esetében új kihívásokkal és problémákkal kell szembenéznünk, melyeknek köszönhetően a hagyományos hálózatokban használt megoldások csak igen korlátozott mértékben vagy egyáltalán nem használhatóak.

Ilyen kihívás például az, hogy a hálózati csomópontok erőforrásai erősen korlátozottak: a csomópontok általában kis méretű, kis teljesítményű, csökkentett számítási és tárolási képességekkel rendelkező beágyazott számítógépek, melyek a tápellátást elemről kapják. Ezért olyan biztonsági algoritmusokra és protokollokra van szükség, melyek kis számítási igényűek, lehetőleg kis kódmérettel rendelkeznek és kis energiafogyasztással bírnak. A hagyományos hálózatokban használt biztonsági algoritmusok és protokollok többsége nem elégíti ki ezeket a követelményeket.

Egy másik fontos probléma, hogy az alkalmazások jellegéből adódóan a hálózat csomópontjai sok esetben fizikailag megközelíthetőek és manipulálhatóak. Ez azt jelenti, hogy számolnunk kell azzal, hogy egy támadó a csomópontok egy részét kompromittálhatja, azaz megszerezheti a csomópontban tárolt kriptográfiai kulcsokat és tetszőleges módon megváltoztathatja a csomópont működését. Hagyományos hálózatokban is előfordulhat, hogy egy támadó megszerzi az uralmat egy hálózati eszköz felett, de mivel hagyományos hálózatokban az eszközök általában fizikailag védett helyen találhatóak, ezért a támadó ott lényegében csak logikai támadásokkal próbálkozhat. A csomópontok kompromittálódásának problémája tehát a szenzorhálózatokban fokozottabb mértékben jelentkezik.

Mivel a fentiekben leírtak miatt a hagyományos hálózatokban használt biztonsági megoldások alkalmazása szenzorhálózatokban nem praktikus, ezért új, a szenzorhálózatok speciális tulajdonságait is figyelembe vevő megoldásokra van szükség. Ez az igény hozta létre a *UbiSec&Sens* (Ubiquitous Security and Sensing in the European Homeland) projektet, mely az EU támogatásával (szerződés száma: 026820), a 6. keretprogram keretében, 3 évig tartott.

A projekt célja egy, a szenzorhálózatokban jól használható biztonsági algoritmusokat és protokollokat tartalmazó toolbox létrehozása volt, valamint a toolbox használhatóságának demonstrálása három példaalkalmazás kifejlesztésén keresztül. A projekt a kitűzött célt elérte és sikeresen záródott 2008 decemberében.

A kifejlesztett toolbox a következő algoritmusokat és protokollokat tartalmazza:

- TinyRNG
  – kriptográfiai véletlenszám-generátor
- RoK
  – robusztus kulcs-szétosztó protokoll
- PRESENT
  – nagyon kevés erőforrást igénylő blokkrejtjelező algoritmus
- EC-ElGamal
  – ElGamal algoritmus megvalósítása elliptikus görbéken
- CDA
  – rejtjelezett adatok aggregálását végző algoritmus
- RANBAR és CORA
  – input támadásoknak ellenálló adataggregációs algoritmusok
- PANEL és SANE
  – biztonságos aggregátor csomópont választó algoritmusok

- TinyLUNAR és S-TinyLUNAR
  - címke alapú útvonalválaszó protokoll és annak biztonságos verziója
- DTSN
  - elosztott megbízható transzport protokoll
- TinyPEDS és DSM
  - elosztott, perzisztens és rejtjelezett adattárolási protokollok
- configKit
  - biztonsági konfigurációt segítő szoftvercsomag

A fenti algoritmusok és protokollok mindegyike implementálásra került TinyOS környezetben, NesC programozási nyelven. Ezen túlmenően, a projekt által készített demoalkalmazások ezen eszközök használatát mutatják be mezőgazdasági, közlekedésbiztonsági és területvédelmi célú alkalmazásokban.

A projektben résztvevő parnerek a következők voltak: Eurescom (D), RWTH Aachen (D), INRIA (F), IHP Microelectronics (D), INOV (P), BME (H), Ruhr University Bochum (D), NEC Europe (GB), Lulea TU (S).

Projektnév: **UbiSec&Sens**

(Ubiquitous Security and Sensing in the European Homeland)

Projektkeret:	EU 6. keretprogram
Idôtartam:	36 hónap (2006-2008)
Résztvevôk száma:	9
Magyar résztvevô:	BME Híradástechnikai Tanszék, CrySyS Laboratórium
Projekthonlap:	http://www.ist-ubisecsens.org/

A UbiSec&Sens projektben fejlesztett toolbox felhasználásra kerül és fontos részét képzi a *WSAN4CIP* (Wireless Sensor and Actuator Networks for Critical Infrastructure Protection) projektnek, mely 2009 januárjában indult, szintén az EU támogatásával (szerződés száma: 225186), de már a 7. keretprogramban. A projekt futamideje 3 év. A projekt célja annak vizsgálata, hogy hogyan alkalmazhatók a vezeték nélküli szenzorhálózatok a kritikus infrastruktúrák működtetésében és védelmében.

Konkrétan két alkalmazásban szeretné a projekt bemutatni a szeznorhálózatok alkalmazhatóságát: ivóvízellátó rendszerekben és nagyfeszültségű távvezetékek monitorozásában. Mindkét esetben nagy fizikai kiterjedésű, kritikus infrastruktúráról van szó, ahol a szenzorhálózatok potenciálisan jól alkalmazhatóak skálázhatóságuk és a viszonylag egyszerű, kábelezést nélkülöző, telepítés miatt. Ugyanakkor, mivel kritikus infrastruktúrákról van szó, ezért nagyon fontos követelmény a biztonság és a megbízhatóság. A projekt ezeket a kérdéseket a hálózat minden szintjén igyekszik vizsgálni, ideértve a csomópontok hardver architektúráját, illetve operációs rendszerét, a hálózati protokollokat és az azokra épülő szolgáltatásokat.

A projektben résztvevő parnerek a következők: Eurescom (D), INRIA (F), IHP Microelectronics (D), INOV (P), BME (H), NEC Europe (GB), Lulea TU (S), EDP (P), FWA (D), Tecnatom (E), Sirrix AG (D), Uni Malaga (E).

Projektnév: **WSAN4CIP**

(Wireless Sensor and Actuator Networks for Critical Infrastructure Protection)

Projektkeret:	EU 7. keretprogram
Idôtartam:	36 hónap (2009-2011)
Résztvevôk száma:	12
Magyar résztvevô:	BME Híradástechnikai Tanszék, CrySyS laboratórium
Projekthonlap:	http://www.wsan4cip.eu/

A fenti projektekben a Műegyetemet a Híradástechnikai tanszék CrySyS Adat- és rendszerbiztonsági laboratóriuma képviseli Dr. Buttyán Levente szakmai irányításával. A CrySyS laboratóriumban több éve folyik kutató munka vezeték nélküli beágyazott rendszerek biztonságával kapcsolatban. A szenzorhálózatok biztonsága és megbízhatósága mellett, a laboratórium munkatársai foglalkoznak vezeték nélküli mesh hálózatokkal biztonságával, gépjárművek közötti vezeték nélküli kommunikáció biztonságával, valamint RFID rendszerekben felmerülő adatvédelmi kérdésekkel.

A bemutatott projektekről és a CrySyS laboratórium munkájáról (valamint más projektjeiről) bővebb információ a laboratórium weboldalán érhető el a *www.c rysys.hu* címen.