Bírálat

Dr. Buttyán Levente

Új biztonsági mechanizmusok vezeték nélküli ad hoc és szenzorhálózatokban

című MTA doktori értekezéséről

Buttyán Levente az informatikai biztonság rendkívül elismert szakértője. Oktatási, csoportépítési és ipari szakértői tevékenysége mellett – és ezektől nem függetlenül - alkalmazott kutatási munkássága is kiemelkedő. A jelen disszertáció ezen kutatási tevékenységének összefoglalója és „bizonyítéka". A benne szereplő eredmények 2003 és 2011 között születtek, a szerző részletezi is ennek körülményeit és a témaválasztás okait. Egy ennyire gyorsan változó területen kritikaként merülhetne föl, hogy miért csak most született meg ez a disszertáció, de én inkább úgy fogalmaznék, hogy régen kiérdemelt cím odaítélése került most napirendre. A témaválasztás izgalmas, bár a kutatás időszaka óta jelentős változások voltak, ahogy azt a szerző is leírja: mára az ad hoc és szenzorhálózatok eredményei mintegy beépültek az Internet of Things (IoT) világába.

Az ad hoc, ezen belül a vezeték nélküli szenzorhálózatok tipikusan kis méretű és teljesítményű eszközökből állnak, melyekben a hálózati funkciókat is maguk a szenzor csomópontok látják el, melyek nagyon védtelenek még a fizikai támadás ellen is. Gazdaságossági megfontolások miatt pedig viszonylag olcsónak kell lenniük, azaz számítási, memória, kommunikációs képességük és energiaellátottságuk is alacsony. Nehéz feladat olyan biztonsági eljárásokat kialakítani, melyek ezen korlátozott erőforrású környezetben is hatékonyak. A disszertációban Buttyán új biztonsági mechanizmusokat javasol, emellett olyan új modelleket és módszereket, melyek alkalmasak arra, hogy bizonyos konkrét biztonsági célokat (ill. ezek teljesülését) precízen és formálisan igazoljuk (vagy cáfoljuk).

A dolgozat eredményeit Buttyán (társszerzőivel) három nemzetközi folyóiratcikkben (*IEEE Transactions on Mobile Computing* illetve *IEEE Transactions on Dependable and Secure Computing*) valamint hat rangos nemzetközi konferenciacikkben publikálta.

A dolgozat a bevezető rész után öt érdemi fejezetből, egy összegző és lezáró részből áll.

Az első fejezetben (Biztoságos útvonalválasztás vezeték nélküli ad hoc hálózatokban) a szerző két (ill. három), korábban biztonságosnak gondolt hálózati útvonalválasztó protokollról

mutatja meg, hogy azok támadhatók, úgy, hogy konkrét támadásokat ad meg. Definiál egy modellezési keretrendszert útvonalválasztó protokollok elemzéséhez, bemutat egy bizonyítási technikát, mely a gyakorlatban is használható protokollok biztonságának bizonyítására. Végül „teljessé teszi" a képet azzal, hogy egy igényvezérelt forrás útvonalválasztó protokollt ad meg (endairA), mely az új bizonyítási módszer segítségével bizonyíthatóan biztonságos.

A második fejezetben (Kooperatív adatcsomag továbbítás vezeték nélküli ad hoc hálózatokban) azt a problémakört vizsgálja, hogy hogyan lehet játékelméleti eszközökkel spontán kooperációra sarkallni az ad hoc hálózatok adattovábbítást esetleg „vonakodva", önző módon végző hálózati végberendezéseit. Buttyán bevezet egy játékelméleti modellt (és egy kapcsolódó meta-modellt), és némi gráfelméleti megfontolásokat is bevetve elemzi ezeket, különösen a Nash-egyensúly kialakulását. Végül szimulációt is végez, amelynek eredménye részben pesszimista, de nagyobb részt optimista: nagyon ritkán (a szimulációban egyszer sem) alakul ki a teljes spontán kooperáció, viszont a kisszámú nem-kooperáló csomópont csak a hálózat kis részére van hatással és nem okoz gondot.

A harmadik fejezetben (Féregjárat detekció vezeték nélküli szenzorhálózatokban) a támadó a hálózat geometriáját torzítja el, és ezáltal pl. az útvonalválasztásban okoz problémákat. Általában a féregjárat sima kriptográfiai eszközökkel nem deríthető fel. Buttyán három algoritmust konstruál a felderítésre. Kettő (a szomszédságszám-teszt és az összes-távolság-teszt) a hálózat topológiájában keres anomáliákat (ezek központosítottak, és olyan szenzorhálózatokban működhetnek, melyekben van egy központi bázisállomás), a harmadik pedig elosztott módon működik, tehát elvben bármely ad hoc hálózatban működhet. Az első két algoritmus statisztikai elemzést, hipotézistesztelést végez. A harmadik pedig egyfajta távolságbecslésen alapszik.

A negyedik fejezetben (Biztonságos kódolás alapú adattárolás szenzorhálózatokban) véletlen kódolás alapú elosztott adattárolási rendszerek elleni úgynevezett szennyezéses támadásokkal foglalkozik. Minden javasolt algoritmusa ügyel arra, hogy a korábban említett korlátozott erőforrásokat ne terhelje meg: nem ad további redundanciát a csomagokhoz, hanem szellemesen használja ki az elosztott rendszerben a már meglévő redundanciákat. A három leírt algoritmusa közül az első a szennyezéses támadás detektálására, a másik kettő pedig szennyezéses támadásból való helyreállításra alkalmazható. Az első algoritmus több szempontból optimális, hamis negatív detekciójának valószínűsége kicsivé tehető; a hamis pozitív detekció valószínűsége ugyan nem kicsi, de ez „csak" egy feleslegesen meghívott helyreállító algoritmus lefutását eredményezi. A két helyreállító algoritmus számítási komplexitása függ a kompromittálódott csomópontok számától (és lehet nagy a futásídő), de a gyakorlati példákon elfogadhatónak bizonyultak (közülük a második a kedvezőbb).

Az ötödik fejezetben (Privacy megőrző hitelesítés erőforrás korlátozott környezetben) a partner hitelesítés során egy külső lehallgató előtt szeretnénk megőrizni az identitását éppen bizonyító fél privacy-jét. Itt több protokoll is ismert a bizonyító és ellenőrző felek közötti kommunikációra, ezek tipikusan erőforrás-igényesek. Buttyán az úgynevezett kulcsfa alapú hitelesítési rendszereket vizsgálta. Konkrétan a binárisnál akart jobb kulcsfát készíteni, amely minimalizálja a bizonyító felek kompromittálódásából származó (további) privacy veszteséget. Ecélból egy érdekes, a privacy szintet mérő metrikát vezetett be (mely kb. azt méri, hogy mennyire ellenálló a rendszer egyetlen szereplő kompromittálódása esetén), majd ennek segítségével algoritmust adott egy bizonyos értelemben optimális kulcsfa paramétereinek beállítására. Közelítő formulát adott az „átlagos anonimitás halmaz" méretére (amelyet a privacy szint méréséhez vezetett be), végül szimuláció segítségével megmutatta, hogy a közelítő formula a gyakorlatban jó eredményt ad.

A disszertáció értékes kutatási tevékenységet foglal össze. Az egyes témakörök szépen, logikusan vannak felépítve, látszik a „nagy vonulat" a gondolatmenetben. A szerző – egyéb értékes tevékenységei mellett – érett kutató. Téziseit elfogadom, fokozatszerzését melegen támogatom.

Budapest, 2021. május 8.

Dr. Sziklai Péter
MTA doktora
tszv. egyetemi tanár
ELTE TTK
Számítógéptudományi tszk.