Bírálat

Buttyán Levente

Új biztonsági mechanizmusok vezeték nélküli ad hoc és szenzorhálózatokban (New Security Mechanisms for Wireless Ad Hoc Networks)

c. MTA doktori értekezéséről

Bíráló: Jelasity Márk

Bevezető

Buttyán Levente szakterületének nemzetközileg is kiemelkedő, kivételes iskolateremtő teljesítménnyel és kivételes tudományos hatással rendelkező kutatója és oktatója, aki az MTA doktora cím követelményeit nagy valószínűséggel már hosszú idővel ezelőtt teljesítette. Jelen disszertáció érdekes sajátossága, hogy már 10 éve is beadható lett volna, mivel a legfrissebb publikáció, amire épül, 2011-ben jelent meg.

Ez a mű legnagyobb hiányossága is egyben, mert a disszertáció ma már sajnos távolról sem hat frissnek. Az ad hoc hálózatok problémaköre a 2000-es években rendkívül népszerű terület volt, azonban mára már veszített a jelentőségéből, mint ahogy az ad hoc hálózatok egy speciális esete, a szenzorhálózatok területe is. Ugyanakkor az Internet of Things (IoT) ernyője alatt a terület egyes eredményei relevánsak maradtak, vagy esetleg a jövőben még inkább relevánsak lehetnek, ha a decentralizáció jelenleg (újra) erősödő tendenciája folytatódik.

Ugyanakkor, ahogy a szerző is kiemeli, az elmúlt 10 évben is rendkívül intenzív és sikeres kutatási teljesítménnyel rendelkezik, tehát a témaválasztás nem a kutatás leállása miatt lett kevésbé friss. Inkább arról van szó, hogy a szerző nem a legújabb, legnépszerűbb, legmagasabb rangú, legidézettebb publikációit választotta ki, hanem igyekezett olyan koherens történetet "elmesélni", amelynek eredményei a lehető legnagyobb mértékben a saját önálló hozzájárulásaiból állnak. Ez a törekvés pedig méltányolandó.

Kérdés 1: *Az ad hoc útvonalválasztó algoritmusoknak van-e jelenleg alkalmazási területe, illetve lát-e arra esélyt, hogy új alkalmazások merülnek fel (pl. űrkutatásban, stb.) annak fényében, hogy általában éppen a biztonsági szempontok azok, amik miatt a legtöbb piaci szereplő központosításra törekszik ahol csak lehet?*

A továbbiakban az egyes tézisekkel kapcsolatos megjegyzéseimet és kérdéseimet ismertetem.

1. Téziscsoport: biztonságos ad hoc útvonalválasztás

Ebben a téziscsoportban igényvezérelt (on-demand) forrás ad hoc útvonalválasztás biztonságával kapcsolatos eredmények találhatók. Ebben az esetben a csomag küldője először felépíti az útvonalat valamilyen, jellemzően broadcast alapú protokoll segítségével. Ez a protokoll támadható, pl. nem létező útvonalak elfogadására kényszeríthető a küldő csomópont. Az 1.1 tézisben a szerző három ilyen, addig biztonságosnak gondolt protokollal szemben mutat be új támadási lehetőségeket, amelyek ötletes, egyszerű konfigurációkon alapulnak és ugyan nem mindig garantált sikerességűek,

de nem elhanyagolható valószínűséggel működnek.

Kérdés 2: *A támadásokban kulcsfontosságú, hogy a támadó mások nevében tud üzenetet küldeni. Nem lehet ezt kivédeni azzal, ha minden csomópont hitelesített kulccsal rendelkezik és minden üzenetet aláír a küldője? Ha ez fel volt téve, akkor viszont nem túl kicsi annak a valószínűsége, hogy a támadó éppen rendelkezik azzal a kulccsal amire éppen szükség van a támadáshoz?*

Az 1.2 tézis egy elméleti keretet tartalmaz, amelynek segítségével bizonyítható egy útvonalválasztó algoritmus biztonságossága egy jól definiált értelemben. A központban a plauzibilis útvonalak definíciója áll, és egy bizonyítás jellemzően ara fókuszál, hogy egy nem-plauzibilis útvonal csak úgy állhat elő, ha a támadó megsérti valamelyik előfeltételt, pl. képes olyan csomópontok nevében aláírni, amelyeknek nem szerezte meg a privát kulcsát. Az 1.3 tézispont pedig egy konkrét algoritmust javasol, amelyre az 1.2 tézisben bemutatott keret alkalmazásával be is bizonyítja a biztonságosságot.

Kérdés 3: *Nem lett egy kicsit túlságosan megengedő a plauzibilis útvonal definíciója? Lenne bármilyen lehetőség szigorítani azt a feltételt, hogy a támadók tetszőlegesen módosíthatják az útvonalat a megszerzett azonosítók hozzáadásával? Ha nem, az nem jelenti azt, hogy a biztonságos útvonalválasztás lényegében lehetetlen?*

Mindhárom altézist ötletes eredeti kontribúciónak tartom, amelyek a biztonságos ad hoc útvonalválasztás témaköréhez jelentős elméleti és gyakorlati hozzájárulásnak tekinthetők. Megemlítendő, hogy a releváns publikációk nemzetközi idézettsége is jelentős.

2. Téziscsoport: kooperatív adatcsomag továbbítás

A csomagok kooperatív továbbítása izgalmas kutatási terület, és különösen az a kérdés érdekes, hogy pusztán racionális alapon is kialakulhat-e kooperáció egy adott rendszerben. Ennek a problémának nagy irodalma van amiben az iterált fogolydilemma tanulmányozása központi szerepet tölt be, mint egyszerű modell. A szerző az ad hoc hálózatok csomagtovábbítási problémáját formalizálta játékelméleti nézőpontból, és bizonyított elsősorban negatív eredményeket. Ez egy sokszereplős iterált játék, ahol a korábbi döntések több iteráción átívelő hatással lehetnek egy gráf struktúra szerint.

A 2.1 tézis ezt a függőségi gráf struktúrát vezeti be, amelyben különösen a körök játszanak fontos szerepet. A 2.2 tézisben erre alapozva a szerző bizonyítja, hogy azok a csúcsok, amelyeknek a stratégiai döntéseitől nem függ azoknak a csúcsoknak a jövőbeli stratégiája, amelyekre a csúcs támaszkodik, legjobban akkor járnak ha nem továbbítanak csomagokat egyáltalán. Kooperáció erős feltételekkel lesz fenntartható (2.3 tétel), a legerősebb az, hogy minden csúcsnak minden forráshoz reaktív körrel kell rendelkezni (azaz olyan körrel, ahol minden csúcs reaktív stratégiát alkalmaz).

A 2.3 tézis ezen erős feltételek teljesülésének valószínűségét vizsgálja empirikus eszközökkel, és azt találja, hogy ennek a valószínűsége nagyon kicsi. Tehát a tit-for-tat (szemet szemért fogat fogért) stratégia nem Nash egyensúlyi stratégia általában. Viszont a hálózatnak van egy olyan magja, amely nem feltétlenül veszi át a nem-kooperáló stratégiát.

Kérdés 4: *A hálózatban a 2.3 tézis szerint létezhet egy racionálisan kooperáló részhalmaz. Lehet ezt jellemezni valami strukturális módon (pl. maximális erősen összefüggő függőségi részgráf)? Illetve, vajon Nash egyensúly-e az az eset, amikor a 2.1 tétel szerint nem-kooperáló csúcsokon kívüli csúcsok TFT stratégiát használnak?*

3. Téziscsoport: féregjárat detekció

A feladat ebben a téziscsoportban az, hogy egy vezeték nélküli szenzorhálózatban ún. féregjáratokat azonosítsunk. A féregjárat egy olyan kapcsolat, amelyet egy támadó hoz létre, amelyben a kapcsolat két végpontja fizikailag távol van egymástól, de valamilyen technológia segítségével (pl. vezetékes

hálózat, stb) képes kommunikálni, és így képes szimulálni azt a helyzetet, amelyben a valóságban távol levő csomópontok szomszédként érzékelik egymást. Ez pedig számos támadásra ad lehetőséget.

A 3.1 tézis egyszerű központi statisztikai teszteket javasol a féregjárat felfedezésére, amelyek a hálózat fokszámeloszlását, illetve legrövidebb útjainak eloszlását vizsgálják, bár ezek a tesztek olyan null-hipotéziseket használnak, amelyek rendkívül erős feltevéseket tesznek a szenzorok eloszlásáról (egyenletes eloszlás, megegyező kommunikációs sugár, téglalap alakú terület, stb.) ezért gyakorlati alkalmazhatóságuk kérdéses.

A 3.2 tézis egy decentralizált eljárást ír le, amelynek során a szomszédok közvetlenül becsülik meg felülről a köztük levő távolságot. Ehhez speciális hardver szükséges, amelynek a segítségével késlekedés nélkül küldhetők bitek, és ahol nanoszekundumos időskálán lehetséges időt mérni. Mivel a támadó nem tud a fénysebességnél gyorsabban kommunikálni (hacsak nem valódi féregjáratot nyit) ezért kiderül, hogy a szomszédok nincsenek elég közel. A módszer egyúttal azonosítást is végez, ez a szerző hozzájárulása. Ezen módszer gyakorlati alkalmazhatósága erősen függ a szenzorok hardverétől. Másrészről, a disszertációban tárgyalt beléptető kártyás példa, és hasonló, passzív eszközöket használó példák esetében eleve nem jön szóba, az ilyen esetek különösen nehéznek tűnnek.

Kérdés 5: *15 év távlatából, mely módszerek lehetnek legalkalmasabbak a féregjáratok detekciójára? Ez egy érdekes probléma sok áthallással a komplex hálózatok irányába. Számomra a [79] hivatkozásban leírt ötlet (vagy annak decentralizált megvalósítása, ami szintén lehetséges) pl. ígéretesnek tűnt, és a disszertációban nincs is kritika megfogalmazva ezzel a megközelítéssel szemben. A helymeghatározást használó megoldások sem tűntek reménytelennek, ebben is sok előrelépés volt azóta.*

4. Téziscsoport: adattárolás szenzorhálózatokban

Ebben a téziscsoportban adattárolási problémákról van szó, közelebbről a halózati kódolást használó megoldásokról. Ezen megoldások legfőbb vonzereje, hogy hatékonyabb kommunikációt tesznek lehetővé azáltal, hogy pl. egy fájl letöltésénél nem kell konkrét blokkokat megszerezni, hanem csak egy adott mennyiségű különböző kódolt blokkot kell letölteni, amiből visszaállítható az eredeti tartalom. A lehetséges blokkok száma gyakorlatilag végtelen, így nincsenek pl. ritka blokkok, stb. Minden kódolt blokk az egész fájlról tartalmaz információt, ezért egy ilyen blokk szennyezése a teljes adatot beszennyezheti. Ez ellen a probléma ellen javasol egy megközelítést a téziscsoport.

A 4.1 tézisben az alapötlet az, hogy a visszaállított adat tisztasága ellenőrizhető úgy, ha a felhasznált blokkokon felül további kódolt blokkokon ellenőrizzük a dekódolás helyességét, ami megtehető, mivel tetszőleges tiszta blokknak konzisztensnek kell lenni a helyes dekódolással. Ha nem tapasztalunk konzisztenciát, akkor nagy valószínűséggel támadás történt, ha viszont konzisztenciát látunk, akkor nagy valószínűséggel helyes a dekódolás. Mindez persze függ néhány paramétertől, legfőképpen attól, hogy a támadó a blokkok hány százalékát képes beszennyezni.

A 4.2 és 4.3 tézisekben egy-egy algoritmust tárgyal a szerző, amik segítségével meg lehet tisztítani egy blokk halmazt, mégpedig a 4.1 tézisben kifejtett ötlet felhasználásával. Mindkét algoritmusban arról van szó, hogy megpróbáljuk addig módosítani a blokkok halmazát, amíg a dekódolás átmegy a teszten. Az algoritmusokra vonatkozóan részletes elemzést kapunk a sikeresség valószínűségéről, és a komplexitásról is.

Az itt tárgyalt tézisek legfőbb vonzereje a módszerek egyszerűsége és természetessége. Bát a módszerek nem védenek nagy fokú támadások ellen, a módszer gyakorlatilag ingyen van, amennyiben a garanciáihoz nincs szükség kriptográfiára, az alapötlet a hálózati kódolás által biztosított redundancia egy olyan újszerű kihasználása, amely a hálózati kódolás eredeti céljai

között nem szerepelt.

5. Téziscsoport: hitelesítés

Ebben a téziscsoportban egy hitelesítéssel kapcsolatos probléma merül fel, nevezetesen a privacy kérdése. Ezen belül a szerző a kulcsfa megközelítést választja, amelynek lényege, hogy a fogadó fél az azonosítás során nem egyszerűen végigpróbálja lineárisan az összes lehetséges általa ismert publikus kulcsot, hanem több kulcsot használ, amelyek hierarchikusan vannak elrendezve: először a legmagasabb szintű kulcsot azonosítja, majd a keletkező részfában megint a legmagasabb szintűt, stb. Ebben a megközelítésben definiál a szerző egy optimalizálási problémát: melyik az a fa topológia (szintenként konstans elágazási faktorral meghatározva) amelyre az azonosítás egy előre adott konstans időnél nem hosszabb ideig tart, és egyúttal egy (vagy több) felhasználó kulcsainak kompromittálódása esetén a privacy sérülése minimális. Ezek versengő szempontok, mert a privacy növeléséhez minél alacsonyabb fa kell, míg a sebesség növeléséhez minél magasabb.

Az 5.1 tézisben az az eset kerül tárgyalásra, ahol egyetlen felhasználó kulcsai kompromittálódnak. Erre az esetre elméleti tárgyalást kapunk az optimalizálási probléma néhány tulajdonságáról, amelyek hatékonyabbá teszik az optimális megoldás megadását. Az 5.2 tézisben pedig az általános eset tárgyalása található, ahol több felhasználó is kompromittálódhat. Itt egy valószínűségi megközelítést javasol a szerző, amit szimulációkkal értékel ki.

Az eredmények érdekes elméleti problémákat vetnek fel, és a gyakorlatban is hasznos megoldásokat javasolnak ezekre.

Kérdés 6: *Nem volt világos számomra, hogy az elágazási faktorok esetében miért kell ragaszkodni ahhoz, hogy a fának pontosan N levele legyen. Pl. ha N prím, akkor csak egyféle fa lehet, ami egész biztosan túl lassú azonosítást adna. Holott ha megengednénk „üres” leveleket, akkor kaphatnánk a korlát alatti időt, persze a privacy árán, de legalább lenne megoldás. Persze akkor további kérdés lenne, hogy mi az „üres” levelek optimális száma.*

Összegzés

A disszertáció összességében rendkívül pontos, mégis világos nyelvezettel, jól érthetően van megfogalmazva. Az egyetlen észrevétel, hogy több helyen nehezíti a megértést az automaták terminológiájának használata algoritmus vagy protokoll helyett, amikor diszkrét dinamikus rendszerek leírásáról van szó, de a kriptográfiai irodalomban ez nem szokatlan.

A disszertációban megfogalmazott tézisek mindegyikét új tudományos eredménynek fogadom el, amely a szerző saját munkája.

A doktori művet az MTA doktora cím elnyeréséhez elegendőnek, egyúttal a nyilvános vitára alkalmasnak tartom.

2021. 02. 23. Szeged

Jelasity Márk
egyetemi tanár
Szegedi Tudományegyetem