Opponensi vélemény

Buttyán Levente

„Új biztonsági mechanizmusok vezeték nélküli ad hoc és szenzorhálózatokban”

című

MTA Doktori értekezéséről

Általános értékelés

Az értekezés tématerülete: Az értekezés a vezeték nélküli ad hoc és szenzorhálózatok kutatási területének különféle biztonsági kérdéseivel foglalkozik. E hálózatokat kisméretű és kisteljesítményű kommunikációs eszközök és technológiák jellemeznek, viszont nincs lehetőség a hálózat fizikai védelmére. Fizikai elkülönítés hiányában ezek az eszközök könnyebben támadhatók, ezért a kapcsolódó biztonsági (security) módszereket úgy szükséges megtervezni, hogy azok limitált erőforrások (processzor, hálózat, energia stb.) esetén is hatékonyan és gazdaságosan (azaz limitált erőforrásigénnyel) működjenek.

A kutatás jelentősége és hatása: Ahogy maga a szerző is kiemeli, a vezeték nélküli szenzorhálózatok területe különösen a 2000-es években időszakban volt aktívan vizsgált kutatási terület. Viszont a kutatási területen elért eredményeknek jelentős hatása van a napjainkban aktívan kutatott kiberfizikai rendszerek és tárgyak internete (Internet of Things) tudományterületeire is, ahol a biztonság talán még fontosabb követelmény (lásd önvezető autók, okos gyárak, stb.).

Az értekezésben bemutatott tudományos eredmények – többek között – biztonságos útvonalválasztást, kooperatív adattovábbítást, féregjárat detekciót, biztonságos kódolás alapú adattárolást illetve privacy-megőrző hitelesítést tesznek lehetővé, nagyban elősegítve a vezeték nélküli ad hoc és szenzorhálózatok biztonságos működtetését. A szerző által kidolgozott módszereket később több kutató is továbbfejlesztette önállóan vagy a szerzővel együttműködve.

Szakmai színvonal. Az értekezés az algoritmuselmélet, a kódoláselmélet, a hálózattudomány, a gráfelmélet és az információbiztonság területének igen mély ismeretéről tesz tanúbizonyságot. Bár az egyes problémák különböznek, a javasolt megoldások szisztematikusan felépítettek és követik a tudományterület nemzetközi módszertanát. A probléma formális definíciójának és/vagy modelljének leírását a javasolt algoritmusok és módszerek precíz bemutatása követi. A módszerek elméleti tulajdonságait formális (vagy félformális) bizonyítások igazolják, a gyakorlatban releváns paraméterek felmérése pedig (az 1. tézis kivételével) kísérleti szimulációk elvégzésével történik.

Publikációs eredmények: Első pillantásra talán meglepő, hogy a disszertáció mindössze 9 kapcsolódó tudományos publikációra épül, amelyek 2003 és 2011 között születtek. Ez azonban a szerző (összességében több mint 150 cikkből álló) kiemelkedő tudományos pályájának, valamint korrektségének újabb jelentős bizonyítéka. Noha a szerző igen eredményes doktori témavezetői tevékenységet is végzett (hét sikeres PhD védéssel), a disszertációjában kizárólag olyan eredményeket közöl, amelyek saját eredményei, a kapcsolódó publikációknak pedig saját maga a fő szerzője. A kapcsolódó mindhárom nemzetközi folyóiratcikk kiemelten rangos, az IEEE által gondozott szaklapokban jelent meg (2x IEEE Transactions on Mobile Computing, 1x IEEE Transactions on Dependable and Secure Computing).

Szerkesztettség, nyelvezet: A 96 oldalas disszertáció angol nyelven készült, gondosan szerkesztett, igényes munka. Az értekezés matematikai eszköztára precíz, nyelvezete gördülékeny és lényegre törő. A javasolt algoritmusok legtöbb esetben jól követhetők, a szimulációs eredményeket bemutató ábrák (a túlságosan kisméretű 32. ábra kivételével) jól áttekinthetők.

A tézisek értékelése

Az értekezés öt lazán csatolt problémakörben mutat be új tudományos eredményeket:

1. tézis: Az útvonalválasztás a vezeték nélküli hálózatok alapvető feladata, ezért a támadók egyik elsődleges célpontja, hiszen hamis útvonalinformációk terjesztésével a teljes hálózat könnyen működésképtelenné tehető. A szerző két ismert és biztonságosnak vélt ad hoc hálózati protokollt (SRP és Ariadne) vizsgált meg, és azonosított új, korábban ismeretlen támadásokat. Ezután egy szimuláción alapuló kétszintű formális modellezési keretrendszert és bizonyítási technikát javasol az útvonalválasztó protokollok biztonságának vizsgálatára. Végezetül egy új útvonalválasztó protokoll mutat be, és formálisan igazolja a protokoll biztonságát a modellezési keretrendszer felhasználásával.

2. tézis: A dolgozat e fejezete a kooperatív adatcsomag-továbbítás problémájával foglalkozik, ahol a forráscsomópont és célcsomópont közötti adatforgalom számos köztes végberendezés együttműködésével történik. Mivel azonban az adatcsomagok továbbítása is erőforrást igényel, előfordulhat, hogy a köztes csomópontok (önző módon) a saját csomagjaik terjesztését preferálják, megtagadva mások csomagjainak továbbítását. Új tudományos eredményként a szerző egy játékelméleti modellt javasol, amelyet a forrás-, cél- és köztes csomópontok „játszanak" annak vizsgálatára, hogy spontán módon milyen feltételek mellett jöhet létre kooperáció. A játékelméleti modell felhasználásával a szerző öt formális feltételt azonosít a kooperatív (és nem-kooperatív) egyensúly teljesülésére. Szimuláció segítségével megmutatja, hogy a spontán kooperáció feltételei a gyakorlatban csak kis valószínűséggel teljesülnek, azaz nagy valószínűséggel lesz nem-kooperatív csomópont. Ugyanakkor azt is kimutatja, hogy e csomópontok viselkedése csak a hálózat kis részére van hatással, így spontán kooperáció mégis kialakulhat lokális részhálózatokban.

3. tézis: Az értekezés 3. fejezete a féregjárat-detekció kérdéskörét vizsgálja vezeték nélküli szenzorhálózatokban, ahol a szomszédos csomópontok folyamatos felderítése és karbantartása szükséges (broadcast jellegű kérés és unicast jellegű válaszüzenet formájában). Féregjárat esetén a támadó két fizikailag távoli pont között létesít közvetlen kapcsolatot, azaz az egyik csomópontra érkező üzeneteket a mások csomópontról továbbítja, amely beavatkozás számos problémához vezethet az útvonalválasztás során. E tézisben a szerző két új, központosított féregjárat-detekciós algoritmusokat javasol, amely a hálózat topológiai gráf fokszámeloszlásának, illetve a legrövidebb utak hosszának eloszlásának statisztikai teszteken alapuló vizsgálatával érzékeli a féregjáratok által előidézett torzulásokat. Mindkét algoritmus esetén széleskörű szimulációs kampány méri fel a detekció legfontosabb minőségi paramétereit (pl. hamis pozitív detekciós ráta). Egy harmadik, többfázisú elosztott algoritmus pedig a csomópontok közötti távolságbecslő protokollra épít, kihasználva, hogy egy féregjárat jellegzetesen a valóságosnál kisebbnek próbálja feltüntetni a végpontjai közötti távolságot.

4. tézis: A disszertáció 4. fejezete a szenzorhálózatok adattárolását vizsgálja, hiszen előfordulhat, hogy a mért adatokat ideiglenes jelleggel magában a szenzorhálózatban szükséges tárolni, mielőtt az adatokat a bázisállomásra továbbítanák. A hatékony tároláshoz felhasználható a hálózati kódolás módszere, ahol az adattároló csomópont a nyers adatok helyett az adatcsomagok egy részhalmazának lineáris kombinációját tárolja. A csomópontokon tárolt kódolt adatok módosításával azonban egy támadó szennyezéses támadást kezdhet, amely meggátolja az adatcsomagok későbbi visszaállítását. A szerző a 4. tézisben olyan új algoritmust javasol a szennyezéses támadás detektálására elosztott adattárolási rendszerekben, amely optimális a kommunikációs és számítási komplexitás tekintetében, a fel nem derített támadás valószínűsége pedig a paraméterek megfelelő megválasztásával kellően kicsivé tehető. Továbbá két új algoritmust vezet be a szennyezéses támadást követő helyreállításnak támogatására változó, illetve fix méretű

tisztítóhalmaz felhasználásával. A szerző mind formális komplexitáselemzés, mind pedig kiterjedt szimulációk segítségével vizsgálja a javasolt algoritmusok hatékonyságát.

5. tézis: Az 5. fejezet a partnerhitelesítés folyamatát vizsgálja, ahol a bizonyító fél az identitását kívánja igazolni az ellenőrző fél számára, azzal a további peremfeltétellel, hogy a résztvevők identitását (privacy) se tudja egy harmadik (lehallgató) fél egyértelműen kideríteni. Ehhez egy kulcsfa alapú protokollt vesz alapul, és annak módosításával készít olyan kulcsfát, amelyik minimalizálja a bizonyító felek kompromittálódásából származó privacy veszteséget. A szerző új tudományos eredményként elsőként egy privacy-szint mérésre szolgáló metrikát, majd egy új algoritmust javasol az optimális kulcsfa paramétereinek meghatározására. Több kompromittált fél esetén egy közelítő módszert ad a privacy-szint mérésére, és szimuláció segítségével mutatja meg a közelítő módszer pontosságát.

Valamennyi tézist a jelölt által közölt, értékes, új tudományos eredménynek tekintem.

Kérdések a disszertáció értelmezésével és eredményeivel kapcsolatban

1. Az 1. fejezetben a valós modellek (real-world model) matematikailag precíz leírására egy együttműködő Turing gépekre alapuló alacsonyszintű formális modell kerül bevezetésre. *Mi a bevezetett formális modell előnye és hátránya más, a kommunikációs protokollok vizsgálatára elterjedten használt formális modellekhez képest?* (pl. LTS: Labelled Transition Systems, CSP: Communicating Sequential Processes vagy egyéb processzalgebrák)
2. A 2. fejezetben bevezetett kétszintű modell egy rendszermodellt és egy metamodellt foglal magában. A rendszermodell és metamodell viszonya azonban nem követi az objektumorientált programozás és modellvezérelt tervezés területén széleskörben használt metamodell és (példány)modell fogalmát, hanem inkább egy absztrakt és egy konkrét modell közötti viszonyt próbál szemléltetni. *Mi a viszonya a disszertációban bevezetett kétszintű modellnek az (objektum-orientált) metamodell-modell viszonyhoz képest? Miként viszonyul a kétszintű modell a formális helyességellenőrzésben Galois-kapcsolatokon alapuló absztrakciós módszerekhez* (pl. absztrakt interpretáció, predikátumabsztrakció)?
3. A 2.3-as altézishez kapcsolódóan a spontán kooperáció gyakoriságának felmérésére elvégzett véletlen szimuláción alapuló vizsgálatok (1. szimuláció) eredménye azt mutatta, hogy a kooperációt garantáló feltételek teljesülésének valószínűsége igen alacsony. Ez az eredmény azonban nem meglepő, hanem inkább az elvégzett véletlen szimulációk szükségszerű következménye. A függőségi hurok feltétele ugyanis értelmezhető egy strukturális (logikai) konzisztenciafeltételként gráfmodellek felett, amely globális feltételek esetén a gráfméret növelésével 1 valószínűséggel fog sérülni véletlen gráfok generálásakor (azaz, véletlenszerűen generált gráfmodell/hálózat aligha lesz konzisztens). *Segítené-e a kooperáció biztonsági vizsgálatát olyan (konzisztens) gráfok automatikus generálása, amelyek garantáltan teljesítik az előírt strukturális feltételeket*? (lásd pl. [1])
4. A 3. fejezetben elvégzett szimulációs vizsgálatok a hamis pozitív rátát (nincs férégjarat, de van hamis riasztás), valamint a helyes riasztások arányát (valós pozitív) mérik fel, nem egyértelmű azonban, hogy *miként kerülhetők el a hamis negatív esetek* (van féregjárat, de nincs riasztás), illetve ennek jelenlétében *miként mérhető fel ezek aránya*.
5. Miként lenne elvégezhető a 3. fejezetben javasolt elosztott féregjárat-detekciós algoritmus releváns paramétereinek (pl. hamis pozitív ráta, stb.) kiértékelése?
6. Az 5. fejezet privacy-megőrző partnerhitelesítést egy limitált erőforrásokkal rendelkező környezetben vizsgálja, ugyanakkor nem világos, hogy pontosan *milyen erőforrás feltételek teljesülése esetén lesznek érvényesek a javasolt eredmények*.

Összegzés

Buttyán Levente MTA doktori értekezésében összefoglalt tudományos munkája magas színvonalú. Az elért eredmények nemzetközi elismertsége kiemelkedő a vezeték nélküli ad hoc és szenzorhálózatok biztonsági elemzése területén. Mind az öt tézisben bemutatott eredményt jelentős, új tudományos kontribúciónak tartom, melyek messzemenően megfelelnek az MTA doktora cím odaítélése kapcsán támasztott követelményeknek. **Az értekezés nyilvános védését és doktori értekezés elfogadását javaslom.**

2020. december 19.

Varró Dániel
egyetemi tanár
MTA Doktora

Hivatkozások

[1] O. Semeráth, A. Nagy, D. Varró. A graph solver for the automated generation of consistent domain-specific models. In Proc. of the 40th Int. Conf. on Software Engineering (ICSE '18), pp. 969–980. DOI: https://doi.org/10.1145/3180155.3180186