dc_1727_20

Új biztonsági mechanizmusok vezeték nélküli ad hoc és szenzorhálózatokban

Buttyán Levente, Ph.D.

tézisfüzet

Budapest
2020

Tartalom

Bevezetés

Disszertációm vezeték nélküli ad hoc és szenzorhálózatok biztonságával, illetve az ezen hálózatokban felmerülő privacy problémákkal kapcsolatban tartalmaz új kutatási eredményeket. A vezeték nélküli ad hoc hálózatok olyan önszerveződő vezeték nélküli hálózatok, melyekben a végfelhasználói eszközök telepített hálózati infrastruktúra nélkül valósítják meg az összes hálózati funkciót. Ezeket a hálózatokat sosem arra szánták, hogy teljes mértékben felváltsák a jelenlegi vezeték nélküli hálózati technológiákat, ugyanakkor egy érdekes alternatív hozzáférési módszert jelentenek számos előnnyel a jelenlegi hozzáférési technológiákkal szemben bizonyos alkalmazási területeken. A vezeték nélküli szenzorhálózatok az ad hoc hálózati technológia speciális alkalmazási területét jelentik, ahol az eszközök nem személyes kommunikációs eszközök, hanem kis méretű és teljesítményű berendezések, melyek rendelkeznek érzékelési, számítási, és kommunikációs képességekkel is. Ezek az eszközök a környezetük paramétereit mérik, és a mérések adatait több ugrásos vezeték nélküli kommunikáció segítségével juttatják el egy nyelő csomóponthoz vagy bázisállomáshoz további feldolgozás céljából. Mivel minden hálózati funkciót maguk a szenzor csomópontok látnak el, ezért a szenzorhálózatok lényegében önszerveződő ad hoc hálózatoknak tekinthetők.

A fent leírt új vezeték nélküli hálózati technológiák számos hasznos alkalmazás előtt nyitják meg az utat. Ugyanakkor, érdekes kihívásokat is rejtegetnek az informatikai biztonság tekintetében. Sok alkalmazásban például a hálózat olyan fizikai környezetben működik, ahol nincs lehetőség a hálózati eszközök fizikai védelmének megvalósítására. Továbbá az egyes eszközök bontásellenállóvá tétele túl nagy költséggel járna, ezért ez sem lehet járható út, főleg olyan alkalmazásokban, ahol nagy mennyiségű eszközről van szó (pl. szenzorhálózatokban) és fontos az eszközök egységárának alacsony szinten tartása. Ez tehát azt jelenti, hogy az eszközök fizikailag támadhatók, kompromittálhatók, így a biztonsági és privacy mechanizmusokat úgy kell megterveznünk, hogy azok ne omoljanak össze teljesen néhány eszköz kompromittálódása következtében. A gazdaságosság követelményéből következik az is, hogy az ad hoc és szenzorhálózatok általában erőforrásokban korlátozottak, az eszközök nem rendelkeznek komoly CPU teljesítménnyel, memória kapacitással, kommunikációs képességeik is korlátozottak mind hatótávolság mind pedig sebesség tekintetében, és sokszor akkumulátor biztosítja a működésükhöz szükséges energiát. Ezért a biztonsági és privacy mechanizmusokat úgy kell megtervezni, hogy azok hatékonyak legyenek és képesek legyenek a kitűzött célok elérésére ebben az erőforrás korlátozott környezetben is. Disszertációmban olyan új biztonsági mechanizmusokat javaslok, melyek kielégítik a fenti kihívásokból származó követelményeket: képesek tolerálni a kompromittált eszközök jelenlétét és erőforrás igényük moderált.

A konkrét biztonsági mechanizmusokon túl, munkám fontos eredményét jelentik azok az új modellek és módszerek, melyeket ezen mechanizmusok analízise céljából javaslok. Ezen modellek és módszerek segítségével egy-egy konkrét biztonsági követelmény vagy cél precízen definiálható és kielégítése formálisan bizonyítható vagy cáfolható. Ez a hozzáállás elengedhetetlen a biztonság területén, ahol az informális érvelés sok esetben nem vezet elegendően megalapozott eredményre egy mechanizmus biztonságát illetően.

Eredményeimet 5 téziscsoportban mutatom be, melyek téziseinek összefoglalóját tartalmazza ez a tézisfüzet.

1. Biztonságos útvonalválasztás vezeték nélküli ad hoc hálózatokban

Az útvonalválasztás az egyik legalapvetőbb hálózati funkció a vezeték nélküli ad hoc hálózatokban. Egy támadó könnyen működésképtelenné teheti az egész hálózatot az útvonalválasztó protokoll megtámadásával (pl. hamis útvonalinformációk terjesztésével). Ezt sok kutató felismerte, és válaszként számos „biztonságos" útvonalválasztó protokollt javasoltak az irodalomban vezeték néküli ad hoc hálózatok számára [22]. Ugyanakkor ezen protokollok biztonságáról csupán informális úton érveltek, vagy olyan formális módszereket próbáltak alkalmazni, melyeket nem az ilyen protokollok elemzésére fejlesztettek ki (pl. a BAN logikát [9]).

Az első téziscsoportban új támadásokat mutatok létező, korábban biztonságosnak vélt ad hoc hálózati útvonalválasztó protokollok ellen. Ezek a támadások egyértelműen azt mutatják, hogy a hibák, melyek ezekhez és hasonló támadásokhoz vezetnek sokszor egyáltalán nem triviálisak, és ezért nehezen azonosíthatóak a protokollok informális elemzése útján. Ezért az informális elemzésnél szisztematikusabb hozzállást javaslok, ami egy új modellezési keretrendszerre épül, melyben a biztonság fogalma precízen definiálható és melyben különböző útvonalválasztó protokollok modellezhetők és biztonságuk matematikailag egzakt módon bizonyítható. A bevezetett keretrendszer elsősorban igényvezérelt (on-demand) forrás útvonalválasztó (source routing) protokollok elemzésére használható, bár az általános elvek, melyekre a keretrendszer épül, más típusú protokollokra is alkalmazhatóak. Javaslok továbbá egy új, igényvezérelt, forrás útvonalválasztó protokollt is ad hoc hálózatok számára, aminek az endairA nevet adtam, és ennek biztonságát formálisan bebizonyítom a javasolt keretrendszerben, ezzel mintegy demonstrálva annak gyakorlati használhatóságát.

1.1. TÉZIS. *Elvégeztem két, az irodalomban javasolt és biztonságosnak vélt ad hoc hálózati útvonalválasztó protokoll, az SRP [28] és az Ariadne [23] biztonsági elemzését, melynek során új, korábban ismeretlen támadásokat azonosítottam az SRP protokoll ellen, valamint az Ariadne protokoll és annak egyik optimalizált változata ellen. Ezen támadások fő jellemzője, hogy megfelelő körülmények között, a támadó nem létező útvonal elfogadására képes rávenni az útvonalválasztást kezdeményező hálózati csomópontot. [C4, J1]*

1.2. TÉZIS. *Egy új modellezési keretrendszert javaslok útvonalválasztó protokollok elemzéséhez, mely lehetővé teszi az útvonalválasztás biztonságának precíz definícióját és útvonalválasztó protokollok biztonságának egzakt úton történő bizonyítását. A definíció és a bizonyítás alapja a szimulációs paradigma, mely jól ismert a kriptográfiai szakirodalomban, ám én alkalmaztam először ad hoc hálózati útvonalválasztó protokollok kontextusában. Ebben a tézisben bevezetem a modellezési keretrendszer elemeit, majd definiciót adok az útvonalválasztás biztonságára igényvezérelt forrás útvonalválasztó protokollok esetén, valamint javaslatot teszek egy bizonyítási technikára, ami a gyakorlatban is lehetővé teszi létező protokollok biztonságának bizonyítását. [J1]*

1.3. TÉZIS. *Egy új igényvezérelt forrás útvonalválasztó protokollt javaslok ad hoc hálózatok számára, melyet endairA-nak neveztem el, és a fent bevezetett modellezési keretrendszert és bizonyítási technikát használva bebizonyítom, hogy ez a protokoll biztonságos. [J1]*

2. Kooperatív adatcsomag továbbítás vezeték nélküli ad hoc hálózatokban

Többugrásos vezeték nélküli ad hoc hálózatokban, a hálózati szolgáltatásokat maguk a hálózati végberendezések nyújtják egymás számára. Az egyik ilyen fontos hálózati szolgáltatás az adatcsomagok továbbítása a forrástól a cél felé, amit a forrás és a cél közötti úton elhelyezkedő végberendezések kooperatív módon kell hogy elvégezzenek. Mivel azonban az adatcsomagok továbbítása erőforrásokat emészt fel, ezért elképzelhető, hogy a végberendezések önző módon nem vesznek részt mások adatcsomagjainak továbbításában, míg szeretnék igénybe venni mások szolgáltatásait saját adatcsomagjaik célba juttatásához. Azonban, ha minden végberendezés önző módon viselkedik, akkor az egész hálózat működésképtelenné válik [11, 25].

A probléma kiküszöbölésére számos kutató javasolta kooperációra ösztönző mechanizmusok bevezetését, pl. a végberendezések kooperációra való hajlandóságának számontartását és a kooperatív végberendezések magasabb minőségben történő kiszolgálását [8, 26], vagy a szolgáltatások ellentételezését valamilyen virtuális fizetőeszköz használatával [12, 31]. Ugyankkor, néhány kutató állítása szerint, a kooperáció akár spontán módon is kialakulhat, speciális ösztönző mechanizmusok bevezetése nélkül [29, 30]. Ezek a munkák azonban nem veszik figyelembe a hálózat topológiáját, hanem absztrakt módon azt feltételezik, hogy bármely végberendezés teljesen véletlen módon kerülhet adatcsomag továbbító szerepbe. Valójában, ha a topológiát nem absztraháljuk el, akkor az eszközök közötti interakciók nagyon is függenek a hálózat topológiájától.

Ebben a téziscsoportban azt vizsgálom, hogy kialakulhat-e a kooperáció spontán módon, külső ösztönző mechanizmusok alkalmazása nélkül, illetve mik ennek a feltételei. Egy játékelméleti modellt vezetek be, melynek segítségével meghatározom a lehetséges egyensúlyok (equilibrium) feltételeit, majd szimuláció segítségével megvizsgálom a kooperatív egyensúlyok kialakulásához szükséges feltételek teljesülésének valószínűségét. Végkövetkeztetésem, hogy statikus ad hoc hálózatokban – ahol a csomópontok közötti relációk stabilak – a spontán kooperáció kialakulásának kicsi az esélye, ezért megalapozott a külső ösztönző mechanizmusok bevezetése.

2.1. TÉZIS. *Az ad hoc hálózatok csomópontjai közötti stratégiai interakciók vizsgálatára bevezetek egy játékelméleti modellt és egy ahhoz kapcsolódó meta-modellt. A játékelméleti modell lényegében egy több szereplős játék definíciójából áll, melyet egy útvonalon elhelyezkedő forrás, cél, és közbenső adatcsomag továbbító csomópontok játszanak egymással. A meta-modell ezen több szereplős játék tulajdonságainak vizsgálatára szolgáló modell, melyben a játékosokat automatákkal modellezem. Ebben a kontextusban bevezetem a függőségi gráf és a függőségi hurok fogalmát. [C6, J3]*

2.2. TÉZIS. *Bebizonyítom az adatcsomag továbbító játékkal kapcsolatos következő állításokat, melyek a kooperatív és nem-kooperatív egyensúlyok feltételeit taralmazzák [J3]:*

- *Ha egy csomópont adatcsomag továbbító szerepet játszik egy útvonalon, de nincs függőségi hurka, akkor legjobb stratégiája az, ha nem továbbít egyetlen adatcsomagot sem, azaz ha egyáltalán nem kooperál. (lásd a 2.1 tételt a disszertációban)*

- *Ha egy csomópont adatcsomag továbbító szerepet játszik egy útvonalon, és minden függőségi hurka nem-reaktív, akkor legjobb stratégiája az, ha nem továbbít egyetlen adatcsomagot sem, azaz ha egyáltalán nem kooperál. (lásd a 2.2 tételt a disszertációban)*

- *Ha minden $j \neq i$ csomópont megtagadja a kooperációt, azaz egyáltalán nem kooperál, akkor i-nek nem lehet reaktív függőségi hurka, és ezért i legjobb válaszstratégiája a többi csomópont viselkedésére a kooperáció megtagadása. Következésképpen, ha minden csomópont folyamatosan megtagadja a kooperációt, akkor Nash egyensúly alakul ki az adatcsomag továbbító játékban. (lásd a 2.1 korollárium ot a disszertációban)*

- *Ha egy i csomópont adatcsomag továbbító szerepet játszik legalább egy útvonalon, akkor a következő feltételek teljesülése esetén lesz legjobb stratégiája a teljes kooperáció: (a) i-nek minden olyan csomóponttal létezik függőségi hurka, akik számára csomagot kell továbbítania valamilyen útvonalon; (b) ezek a függőségi hurkok mind reaktívak; és (c) az adatcsomag továbbítás maximális költsége azon útovonalak felett ahol i adatcsomag továbbító szerepet tölt be kisebb, mint az ezen útvonalakon vett lehetséges jövőbeli átlagos haszon. Ha mindhárom feltétel teljesül, akkor az i csomópontnak van oka a kooperációra, mert ha nem-kooperatívan viselkedne, akkor az negatívan befolyásolná saját jövőbeli kifizetését. (lásd a 2.3 tételt a disszertációban)*

- *Ha az (a) és (c) feltételek teljesülnek minden olyan csomópontra, ami adatcsomag továbbító szerepet játszik valamilyen útvonalon, akkor ha minden csomópont Tit-for-Tat (reaktív) stratégiát választ, Nash egyensúly alakul ki az adatcsomag továbbító játékban. (lásd a 2.2 korollárium ot a disszertációban)*

2.3. TÉZIS. *Szimuláció segítségével megmutatom, hogy a spontán kooperáció kialakulásának feltételei a gyakorlatban kis valószínűséggel teljesülnek. Vizsgálataim során, 1000 véletlen választott esetből, egyetlen esetben sem teljesült az a feltétel, ami azt követeli meg, hogy minden adatcsomag továbbító szerepet játszó i csomópontnak legyen függőségi hurka minden olyan csomóponttal, ami forrás szerepet tölt be azokon az útvonalakon, ahol i adatot továbbít. Ez azt jelenti, hogy nagy valószínűséggel mindig lesz olyan csomópont a hálózatban, aminek legjobb stratégiája a kooperáció megtagadása. Ugyanakkor, szimuláció segítségével megmutatom azt is, hogy ezen nem-kooperáló csomópontok viselkedése csak a hálózat kis részére van hatással, ezért nem kizárt a spontán kooperáció kialakulása a csomópontok kisebb, lokális részhalmazaiban. [J3]*

3. Féregjárat detekció vezeték nélküli szenzorhálózatokban

Mint minden hálózatban, a vezeték nélküli ad hoc és szenzorhálózatokban is fontos, hogy az útvonalválasztást és az adatcsomagok továbbítását megvalósító minden csomópont felmérje és mindig tudatában legyen annak, hogy melyek a közvetlenül, egy ugrással elérhető, ún. szomszédos csomópontok. A szomszédok felderítése egyszerű kérés-válasz típusú protokollokkal történhet, ahol a kérés broadcast jellegű, így minden szomszéd hallja, és egy unicast válaszüzenetben jelezheti jelenlétét a kérdezőnek. Az ilyen protokollok azonban sérülékenyek az ún. féregjárat támadással szemben.

A *féregjárat* egy gyors, out-of-band kapcsolat két fizikailag távoli pont között, amit a támadó azzal a céllal hoz létre, hogy az egyik ponton lehallgatott adatcsomagokat a féregjáraton keresztül átjátszhassa a másik pontra, ahol újra a hálózatba injektálhatja azokat. Könnyű észrevenni, hogy ezzel a támadó befolyásolni tudja a szomszédok felderítését: a féregjárat egyik végepontja közelében található i csomóponttal el tudja hitetni, hogy egy tőle távoli, a féregjárat másik végpontjánál elhelyezkedő j csomópont közel van és i közvetlen szomszédja. Ez számos problémához vezethet, főleg az útvonalválasztás területén. Sok útvonalválasztó protokoll pl. a legrövidebb utakat preferálja, amelyek egy

része így a féregjáraton keresztül vezet majd, hiszen a féregjárat a két végpontja közötti távolságot lényegében eltünteti a csomópontok számára.

Vezeték nélküli hálózatokban, a féregjárat két végpontja két vezeték nélküli adó-vevő eszközt tartalmaz, ezekkel tudja a támadó lehallgatni és a hálózatba injektálni az adatcsomagokat. A két végpont közötti összeköttetés lehet vezetékes vagy használhat más vezeték nélküli technológiát, mint maga a hálózat. A támadó a féregjáraton keresztül szelektív továbbítást is végezhet a két végpont között, és rejtjelezett, a támadó számára érthetetlen adatcsomagokat is lehallgathat, továbbíthat, majd újra a hálózatba injektálhat. Ezért pusztán kritpográfiai módszerekkel a féregjárat általában nem detektálható.

A probléma megoldására, ebben a téziscsoportban, új féregjárat detekciós algoritmusokat javaslok. Két javasolt algoritmusom elsősorban szenzorhálózatokban alkalmazható, ahol a bázisállomás központi szerepet tölthet be. Mindkét algoritmus arra épül, hogy a szenzorok elküldik a vélt szomszédaik listáját a bázisállomásnak, ami a kapott információ alapján rekonstruálja a hálózat topológiáját, és olyan anomáliákat keres benne, melyek féregjárat jelenlétére utalnak. A harmadik javasolt detekciós algoritmus ezzel szemben elosztott módon működik, ezért tetszőleges ad hoc hálózatban használható. A harmadik algoritmus alapját két szomszédos csomópont között végrehajtott, hitelesített távolságbecslő (distance-bounding) protokoll alkotja.

3.1. TÉZIS. *Két új, központosított féregjárat detekciós algortimust javaslok vezeték nélküli szenzorhálózatok számára, melyek statisztikai hipotézis tesztelésre épülnek. Mindkét algoritmusban, a hálózati csomópontok elküldik vélt szomszédaik listáját egy kitüntetett csomópontnak, ami szenzorhálózatokban a bázisállomás lehet. A szomszédlisták alapján a kitüntetett csomópont rekonstruálja a hálózati topológiát és féregjáratra utaló inkonzisztenciákat keres benne. Az első algoritmus (Neighbor Number Test – NNT) a topológia gráf csúcsainak fokszám eloszlásában, a második algoritmus (All Distances Test – ADT) pedig a csúcspárok között vett legrövidebb utak hosszának eloszlásában azonosít torzulásokat. Mindkét algoritmus χ^2–tesztet használ, mint hipotézis tesztelő módszer, melynek paraméter választására is javaslatot teszek. Szimuláció útján megmutatom, hogy az NNT algoritmus akkor detektálja a féregjáratot pontosan, ha a féregjárat végpontjai hatókörének mérete összemérhető a hálózati csomópontok hatókörének méretével és a féregjárat végei által befolyásolt területek távolsága kellően nagy. Ellenben, mikor a féregjárat végpontjainak hatóköre szignifikánsan kisebb, mint a halózati csomópontoké, az NNT algoritmus detekciós pontossága elfogadhatatlanul alacsony. Hasonlóan, szimuláció segítségével megmutatom, hogy az ADT algoritmus nagyon pontos detekcióra képes, ha a féregjárat végpontjainak hatóköre összemérhető a csomópontok hatókörének méretével, és a detekciós pontossága még akkor is elfogadható, ha a féregjárat végpontjainak hatóköre kicsi, de a féregjárat végei által befolyásolt területek távolsága kellően nagy. Továbbá, mindkét algoritmus hamis pozitív detekciós rátája alacsony. [C2]*

3.2. TÉZIS. *Egy új, elosztott féregjárat detekciós algoritmust javaslok, mely egy új, csomópontok közötti távolság-becslő (distance bounding) protokollra épül. Az új távolságbecslő protokoll kölcsönösen hitelesíti a protokoll résztvevőit egymás felé, és egy olyan elkötelezés (commitment) fázist tartalmaz, mely megakadályozza azokat a támadásokat, ahol a támadó a résztvevők által becsült távolságot megpróbálja kisebbnek feltüntetni, mint amekkora az valójában. Informális elemzés útján megmutatom, hogy a protokoll alkalmas a féregjárat detekcióra, mivel a féregjárat tipikusan a végpontjai közötti távolságot próbálja kisebbnek feltüntetni, mint amekkora az valójában. [C5]*

4. Biztonságos kódolás alapú adattárolás szenzorhálózatokban

A vezeték nélküli szenzorhálózatokban előfordul, hogy a szenzorok által mért adatokat nem lehet azonnal a bázisállomás felé továbbítani (pl. mobil bázisállomás esetén), hanem magában a szenzorhálózatban kell azokat hatékonyan tárolni ideiglenes jelleggel. Természetesen az adatok tárolásakor és későbbi lekérdezésekor figyelembe kell venni a csomópontok erőforrás korlátait, ami a számítási és a tárolási kapacitások szűkösségét, valamint a kommunikációból eredő energiafogyasztás minimalizálására vonatkozó követelményt jelenti.

Az adattárolás hatékonysága növelhető a hálózati kódolás [5, 20, 21, 24] alapelveit felhasználva, a nyers adatok helyett azok kódolt formájának elosztott tárolásával. Tegyük fel például, hogy k adatforrás adatait szeretnénk $n > k$ adattároló csomóponton elosztottan tárolni. A nyers adatcsomagok helyett, minden adattároló csomópont tárolhatja a k adatcsomag egy részhalmazának lineáris kombinációját. A [15, 16, 17, 18] forrásokban bevezetett véletlen kódolási technikákat (erasure codes, fountain codes) alkalmazva, a paraméterek megfelelő megválasztásával elérhető, hogy az adatok begyűjtését végző (mobil) bázisállomás mind a k adatcsomagot nagy valószínűséggel vissza tudja állítani tetszőleges k adattároló csomópont lekérdezésével és egy k egyenletből álló lineáris egyenletrendszer megoldásával. Így a bázisállomás lekérdezheti a hozzá legközelebb eső k adattároló csomópontot, ezzel is minimalizálva a kommunikációs overhead-et.

Sajnos a fenti előnyök mellett, támadó környezetben, a véletlen kódolásra épülő elosztott adattárolásnak vannak hátrányai is. A támadó ugyanis megtámadhatja az adattároló csomópontokat és módosíthatja az azokon tárolt kódolt adatokat. Ezt a támadást *szennyezéses támadásnak* (pollution attack) hívják. A kódolás miatt már pár adattároló csomópont megtámadása esetén is elérhető, hogy a később visszaállított adatcsomagok nagy része hibás legyen. Ez azért van, mert egyetlen kódolt adat változtatása több eredeti adatcsomag dekódolását befolyásolja. Ez a fajta erősítő hatás különösen aggasztó, és fontossá teszi a szennyezéses támadás detekcióját, illetve a támadásból való felépülést.

Ebben a téziscsoportban a fő kontribúcióm egy új hozzáállás a szennyezéses támadás detektálására és az abból történő helyreállásra véletlen kódolás alapú elosztott adattárolási rendszerekben. Más korábbi megoldásokhoz képest az én módszerem előnye, hogy nem adok rendundanciát az eredeti adatcsomagokhoz, nem használok kriptográfiai mechanizmusokat, és nem feltételezem új funkciók bevezetését az adattároló csomópontokon. Ezek ugyanis mind növelik a felhasznált erőforrásokat, melyek szűkösek a szenzorhálózatokban. Ehelyett a megoldásom az alkalmazott kódolási séma saját belső redundanciáját aknázza ki. Vizsgálom továbbá a javasolt algoritmusok teljesítményét kommunikációs és számítási komplexitás, illetve sikervalószínűség szempontjából.

4.1. TÉZIS. *Új algoritmust javaslok a szennyezéses támadás detektálására véletlen kódolás alapú elosztott adattárolási rendszerekben. Megmutatom, hogy az algoritmus optimális kommunikációs és számítási komplexitás tekintetében, és hogy a hamis negatív detekció valószínűsége a paraméterek megfelelő megválasztásával kicsivé tehető. Megmutatom továbbá, hogy az algoritmus hamis pozitív detekciós rátája* $\frac{t}{n-k}$*, ahol* k *az adatforrások száma,* n *az adattároló csomópontokszáma, és* t *a kompromittált adattároló csomópontok száma. Látszik tehát, hogy a hamis pozitív ráta potenciálisan nem kicsi, ugyanakkor a hamis pozitív detekció következménye csupán annyi, hogy meghívódik a disszertációban javasolt helyreállító algorimtusok valamelyike, melyek ezt a helyzetet hatékonyan kezelik le. [C1, J2]*

4.2. TÉZIS. *Új algoritmust javaslok a szennyezéses támadásból történő helyreállításra*

véletlen kódolás alapú elosztott adattárolási rendszerekben. Az algoritmus kódolt adatblokkokat használ tisztító halmazként. A tisztító halmaz mérete iteratívan növekszik, melynek köszönhetően a sikeres helyreállítás valószínűsége 1, ha $t < n-k$, és 0 egyébként, ahol k az adatforrások száma, n az adattároló csomópontok száma, és t a kompromittált adattároló csomópontok száma. Mivel a gyakorlatban k akár egy nagyságrenddel is kisebb lehet mint n, ezért $n-k$ közel van n-hez, ami azt jelenti, hogy az algoritmus akkor is sikeres ha az adattároló csomópontok jelentős hányada kompromittált. Az algoritmus kommunikációs komplexitása optimális és megközelítőleg $\frac{kp+1}{1-p}$, ahol $p = t/n$. Az algoritmus számítási komplexitása exponenciális a kompromittált adattároló csomópontok t számában, de a numerikus eredményeim azt mutatják, hogy kis és közepes méretű rendszerekben (pl. 10-50 adatforrás és 100-600 adattároló csomópont esetén) a gyakorlatban elfogadható mennyiségű számítást igényel (az adattároló csomópontok 50-10%-ának kompromittálódását tolerálva). [C1, J2]

4.3. TÉZIS. *Egy második algoritmust is javaslok a szennyezéses támadásból történő helyreállításra véletlen kódolás alapú elosztott adattárolási rendszerekben. Ez az algoritmus fix méretű tisztító halmazt használ, ezért számítási komplexitása kedvezőbb, mint az első helyreállító algoritmusé. Szimuláció segítségével megmutatom, hogy ugyanannyi, a gyakorlatban még elvégezhető számítással ez az algoritmus egy nagyságrenddel nagyobb rendszerekben (pl. 100 adatforrás és 1000 adattároló csomópont) is működik és sikeres helyreállítást végez, ha a kompromittált adattároló csomópontok aránya legfeljebb 10%, viszont a sikervalószínűsége gyorsan csökken, ahogy ez az arány tovább növekszik. Az algoritmus kommunikációs komplexitása is növekszik a kompromittált csomópontok számával, de az elfogadható $n/2$ körüli érték alatt marad, ha a kompromittált csomópontok aránya legfeljebb 10%, és közel optimális, ha ez az arány legfeljebb 5%. [J2]*

5. Privacy megőrző hitelesítés erőforrás korlátozott környezetben

Partner hitelesítésnek nevezzük azt a két fél között lezajló folyamatot, melyben az egyik fél (a bizonyító) bizonyítja identitását a másik fél (az ellenőrző) számára. A feladat megoldására számos, üzenetcserére épülő partner hitelesítő protokoll létezik [7], melyek ellenállnak a felek megszemélyesítését célzó támadásoknak. Ugyanakkor, a kutatók kevesebbet foglalkoztak a felek – különösen a bizonyító fél – magánszférájának (privacy) védelmével ezekben a protokollokban. Lényegében szinte minden, az irodalomban javasolt partner hitelesítő protokoll kiszivárogtatja a bizonyító fél identitását egy lehallgató harmadik fél (a támadó) számára.

A privacy megőrzésének egyik módja a protokollban résztvevő felek azonosítójának rejtjelezése egy publikus kulcsú rejtjelező algoritmus segítségével. Például, a bizonyító fél azonosítóját az ellenőrző fél publikus kulcsával rejtjelezve elérhetjük, hogy csak az ellenőrző fél tudja, ki végzi éppen a hitelesítést. Egy másik lehetőség egy anonim Diffie-Hellman kulcscsere végrehajtása, majd a partner hitelesítő protokoll futtatása az így létre hozott titkos csatornán keresztül. Ekkor nemcsak a bizonyító fél identitása, hanem a protokoll teljes tartalma rejtve marad a lehallgató támadó elől. Bár a fenti megoldások alkalmasak a privacy védelmére, erőforrás igényes publikus kulcsú kriptográfiát használnak, ezért nem alkalmazhatók erőforrás korlátozott környezetekben, például vezeték nélküli szenzorhálózatokban vagy RFID rendszerekben.

A bizonyító fél identitását megpróbálhatjuk kevésbé erőforrás igényes, szimmetrikus kulcsú rejtjelezéssel rejteni a támadó elől, de ekkor abba a problémába ütközünk, hogy

az ellenőrző fél számára nem adhatunk támpontot arra vonatkozóan, hogy melyik kulcsot használtuk, mert ez a támadó számára is támpontként szolgálna a bizonyító identitásának kiderítésére. Az ellenőrző fél megpróbálhatja a dekódolást minden kulccsal, amit a különböző szóba jöhető bizonyító felekkel oszt meg, míg valamelyik kulcs sikeresen nem dekódolja a bizonyító fél azonosító információját. Ez azonban, nagy rendszerekben, azaz sok lehetséges bizonyító fél esetén, megnöveli a hitelesítési késleltetést, ami szintén nem kívánatos, sőt bizonyos rendszerekben elfogadhatatlan.

A Molnar és Wagner által javasolt kulcsfa alapú protokoll [27] elegáns megoldást ad a fenti problémára. A protokoll csak szimmetrikus kulcsú kriptográfiát használ, elrejti a bizonyító fél identitását egy lehallgató támadó elől, míg az ellenőrző féltől csupán a lehetséges bizonyítók számának logarirmusával arányos dekódolási kísérletet követel a bizonyító fél hitelesítéséhez. Azaz a protokoll minden tekintetben hatékony.

A Molnar-Wagner protokoll alapja egy kulcsfa, ami egy olyan fa, melyben minden élhez egyedi kulcsot rendelünk. A fa levelei reprezentálják a bizonyító feleket, és minden bizonyító fél tárolja a gyökértől hozzá vezető úton található kulcsokat. Az ellenőrző fél ismeri a teljes fát és az éleihez rendelt összes kulcsot. Mikor egy bizonyító fél hitelesíti magát, akkor az összes kulcsát használja, a legfelső szintű (a gyökérhez legközelebbi) kulcstól indulva és az alacsonyabb szintű kulcsok felé haladva. Az ellenőrző fél először a legfelső szintű kulcsokat próbálja ki, és meghatározza, melyiket használta a bizonyító fél. Ezután a következő szinten található kulcsokkal próbálkozik, de már csak az azonosított, felsőbb szintű kulcs alatt elhelyezkedő kulcsokat kell kipróbálnia. Ezt az eljárást folytatva, az ellenőrző fél minden használt kulcsot azonosítani tud, és minden kulcs azonosításához legfeljebb annyi kulcsot kell kipróbálnia amennyi elágazás található a fában az adott kulcs szinjén. Molnar és Wagner eredeti cikkükben bináris fák alkalmazását javasolták, így a fenti keresés komplexitása a bizonyító felek számában logaritmikus.

A kulcsfa alapú hitelesítés problémája, hogy nem tolerálja jól a bizonyító felek kompromittálódását. Ha egy bizonyító fél kompromittálódik, akkor az összes általa tárolt kulcs a támadó birtokába jut. A felsőbb szintű kulcsokat azonban más bizonyító felek is használják, így részben ők is kompromittálódnak. Pontosabban, azáltal, hogy felsőbb szintű kulcsaik egy része a támadó birtokába jutott, ezek a bizonyító felek alacsonyabb privacy szintet élveznek, mint azok a bizonyító felek, akiknek egyetlen kulcsa sem szivárgott még ki. Sajnos, ha a kulcsfa bináris fa, akkor egyetlen bizonyító fél kompromittálódása az összes bizonyító fél felét érinti!

Ebben a téziscsoportban azzal foglalkozom, hogyan lehet a binárisnál jobb kulcsfát konstruálni, ami minimalizálja a bizonyító felek kompromittálódásából származó privacy veszteséget, míg továbbra is elfogadható szinten tartja a keresésből származó hitelesítési késleltetést. A feladat megoldásához először egy privacy szint mérésére alkalmas metrikát javaslok, mely a jól ismert anonimitás halmaz fogalmára épül. Ezután megmutatom, hogy a kulcsfa paramétereit hogyan kell úgy megválasztani, hogy ezt a metrikát maximalizáljuk, miközben más, a hitelesítés késleltetésére vonatkozó praktikus követelmények továbbra is teljesülnek. A problémát először abban az egyszerű esetben vizsgálom, mikor egy bizonyító fél kompromittálódását engedjük meg, majd a vizsgálatot kiterjesztem az általános esetre, mely tetszőleges számú kompromittált bizonyító felet megenged. Az általános esetben közelítést adok a privacy szint mértékére, és szimuláció segítségével megmutatom, hogy ez a közelítés pontos.

5.1. TÉZIS. *A kulcsfa alapú hitelesítési rendszer által nyújtott privacy szintjének mérésére bevezetem a normalizált átlagos anonimitás halmaz méretet és pontos formulát adok kiszámítására arra az esetre, mikor egyetlen potenciális bizonyító fél kompromittált. Ezt fel-*

használva, egy új algoritmust javaslok az optimális kulcsfa paramétereinek meghatározására, ahol optimális alatt azt értem, hogy az egy kompromittált bizonyító fél esetében számolt normalizált átlagos anonimitás halmaz méret maximális, miközben a legrosszabb hitelesítési késleltetés egy adott küszöb alatt marad.

5.2. TÉZIS. *Általános esetben tetszőleges c számú bizonyító fél lehet kompromittált. A privacy szint mérésére továbbra is az átlagos anonimitás halmaz méretet használom, és ennek értékét az alábbi kifejezéssel közelítem:*

$$\tilde{S} = \sum_{i=1}^{\ell} \sum_{k=1}^{b_i-1} kN_i \binom{b_i-1}{k-1} (1-q_i)^k q_i^{b_i-k} + 1 \cdot p + N \cdot (1-p)^N$$

ahol ℓ a kulcsfa mélysége, $b_1, b_2, \ldots, b_\ell$ az egyes szintek elágazási faktorai, $N = b_1 \cdot b_2 \cdot \ldots \cdot b_\ell$ a fa leveleinek száma, $N_i = \frac{N}{b_1 \cdot b_2 \cdot \ldots \cdot b_i}$ az i szinten elhelyezkedő tetszőleges csúcs alatt található levelek száma, $p = c/N$ annak a valószínűsége, hogy egy véletlen választott levél kompromittált, és $q_i = 1-(1-p)^{N_i}$ annak a valószínűsége, hogy az i szinten elhelyezkedő tetszőleges csúcs alatt található kompromittált levél. Továbbá, szimuláció segítségével megmutatom, hogy ez a közelítés a gyakorlatban pontos.

Az eredmények publikációja

Disszertációm eredményei az alábbi nemzetközi publikációkban jelentek meg.

Nemzetközi folyóiratcikkek:

[J1] G. Ács, L. Buttyán, and I. Vajda. Provably secure on-demand source routing in mobile ad hoc networks. *IEEE Transactions on Mobile Computing (TMC)*, 5(11), November 2006.

[J2] L. Buttyán, L. Czap, and I. Vajda. Detection and recovery from pollution attacks in coding based distributed storage schemes. *IEEE Transactions on Dependable and Secure Computing*, 8(6), November/December 2011.

[J3] M. Félegyházi, J. Hubaux, and L. Buttyán. Nash equilibria of packet forwarding strategies in wireless ad hoc networks. *IEEE Transactions on Mobile Computing*, 5(5), May 2006.

Nemzetközi konferenciacikkek:

[C1] L. Buttyán, L. Czap, and I. Vajda. Securing coding based distributed storage in wireless sensor networks. In *Proceedings of the IEEE Workshop on Wireless and Sensor Network Security (WSNS)*, October 2008.

[C2] L. Buttyán, L. Dóra, and I. Vajda. Statistical wormhole detection in sensor networks. In *Proceedings of the European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS)*. Springer, July 2005.

[C3] L. Buttyán, T. Holczer, and I. Vajda. Optimal key-trees for tree-based private authentication. In *Proceedings of the International Workshop on Privacy Enhancing Technologies (PET 2006)*. Springer, June 2006.

[C4] L. Buttyán and I. Vajda. Towards provable security for ad hoc routing protocols. In *Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN)*, October 2004.

[C5] S. Capkun, L. Buttyán, and J. Hubaux. SECTOR: Secure tracking of node encounters in multi-hop wireless networks. In *Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN)*, October 2003.

[C6] M. Félegyházi, L. Buttyán, and J. Hubaux. Equilibrium analysis of packet forwarding strategies in wireless ad hoc networks – the static case. In *Proceedings of the International Conference on Personal Wireless Communication (PWC'03)*, September 2003.

A kutatás hatása

A disszertáció eredményei 2003 és 2011 között születtek. Abban az időszakban a vezeték nélküli ad hoc és szenzorhálózatok aktívan kutatott tématerületek voltak, és a biztonság és privacy kérdése ezekben a hálózatokban fontos kutatási problémának számított. Azóta eltelt jópár év, és mostmár látható, hogy az ad hoc hálózatok nem valósultak meg abban a formában, ahogy akkor a kutatók elképzelték azt. Ugyanakkor, a szenzor-technológia folyamatosan fejlődött és mára elérte azt az érettségi szintet, mely lehetővé teszi gyakorlati alkalmazását a kutatólaboratóriumok falain kívül is. Számos olyan alkalmazás van, melyekben szenzorok gyűjtenek adatot nagy mennyiségben a környezetből, emberi építményekből (pl. épületekből, hidakról, alagutakból), vagy élő szervezetekből, beleértve az emberi testet is. Korunk okos épületei, okos autói, és okos városai az „okosságot" abból nyerik, hogy az érzékelés, az adatfeldolgozás és a kommunikáció kombinációjának segítségével tudatában vannak a környezetüknek és reagálni tudnak annak változásaira, és ez minden intelligens rendszer fő jellemzője. Ma már nem a szenzorhálózatok terminológiát használjuk ezekre a rendszerekre, hanem inkább a *kiber-fizikai rendszerek* és a *dolgok* vagy *tárgyak Internetje* (Internet of Things - IoT) kifejezések terjedtek el. Ám érdemes fejben tartani, hogy ezek megvalósulását az ad hoc és szenzorhálózatok területén végzett kutatások alapozták meg. És mivel a különböző intelligens beágyazott rendszerek egyre fokozottabban gyűjtenek adatot rólunk és irányítják mindennapi életünket, a biztonság és a privacy kérdése fontosabbá vált mint bármikor korábban. Ebben a kontextusban tehát a disszertáció eredményeit továbbra is fontosnak tekinthetjük.

Az itt bemutatott eredményeim közvetlen hatással voltak más kutatók munkájára is: a bizonyíthatóan biztonságos útvonalválasztó protokollok elemzésével és tervezésével kapcsolatos munkát Ács Gergely folytatta és egészítette ki új definíciókkal és bizonyításokkal más típusú ad hoc és szenzorhálózati útvonalválasztó protokollra [2, 3, 4, 1]; a statikus ad hoc hálózatokban spontán kialakuló kooperáció vizsgálatát Félegyházi Márk egészítette ki a dinamikus esettel [19]; a kódolásra épülő elosztott adattároló rendszerek szennyezéses támadásokkal szembeni védelmét szolgáló algoritmusok teljesítményét Czap László javította később különböző optimalizációkkal [10]; a szimmetrikus kulcsú, privacy megőrző hitelesítés területén végzett kutatásokat Holczer Tamás egészítette ki újabb, nem kulcsfákra épülő megoldásokkal [6]; és végül az itt javasolt decentralizált féregjárat detektáló algoritmus alapjául szolgáló távolságbecslést (distance bounding) Srdjan Capkun alkalmazta később sikerrel biztonságos helymeghatározó algoritmusokban [13, 14].

Hivatkozások

[1] G. Ács. Secure routing in multi-hop wireless networks. PhD thesis, Budapest University of Technology and Economics, 2009.

[2] G. Ács, L. Buttyán, and I. Vajda. Provable security of on-demand distance vector routing in wireless ad hoc networks. In *Proceedings of the European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS)*, Visegrad, Hungary, July 2005.

[3] G. Ács, L. Buttyán, and I. Vajda. Modelling adversaries and security objectives for routing protocols in wireless sensor networks. In *Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN)*, October 2006.

[4] G. Ács, L. Buttyán, and I. Vajda. The security proof of a link-state routing protocol for wireless sensor networks. In *Proceedings of the IEEE Workshop on Wireless and Sensor Networks Security (WSNS)*, October 2007.

[5] Rudolf Ahlswede, Ning Cai, Shuo-Yen Robert Li, and Raymond W. Yeung. Network information flow. *IEEE Transactions on Information Theory*, 46(4):1204–1216, July 2000.

[6] G. Avoine, L. Buttyán, T. Holczer, and I. Vajda. Group-based private authentication. In *Proceedings of the IEEE Workshop on Trust, Security, and Privacy for Ubiquitous Computing (TSPUC)*, June 2007.

[7] C. Boyd and A. Mathuria. *Protocols for Authentication and Key Establishment.* Springer-Verlag, 2003.

[8] S. Buchegger and J-Y. Le Boudec. Performance analysis of the CONFIDANT protocol. In *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, June 2002.

[9] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM Transactions on Computer Systems*, 8(1):18–36, February 1990.

[10] L. Buttyán, L. Czap, and I. Vajda. Pollution attack defense for coding based sensor storage. In *Proceedings of the IEEE Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC)*, June 2010.

[11] L. Buttyán and J.-P. Hubaux. Enforcing service availability in mobile ad hoc WANs. In *Proceedings of the 1st ACM/IEEE International Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc)*, August 2000.

[12] L. Buttyán and J.-P. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. *ACM/Kluwer Mobile Networks and Applications (MONET)*, 8(5), October 2003.

[13] S. Capkun and J-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *Proceedings of IEEE INFOCOM*, 2005.

[14] S. Capkun and J-P. Hubaux. Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications (JSAC)*, February 2006.

[15] A. G. Dimakis, V. Prabhakaran, and K. Ramchandran. Distributed data storage in sensor networks using decentralized erasure codes. In *Proceedings of the Asilomar Conference on Signals, Systems, and Computers*, Pacific Grove, CA, USA, November 2004.

[16] A. G. Dimakis, V. Prabhakaran, and K. Ramchandran. Ubiquitous access to distributed data in large-scale sensor networks through decentralized erasure codes. In *IPSN '05: Proceedings of the 4th international symposium on Information processing in sensor networks*, page 15, Piscataway, NJ, USA, 2005. IEEE Press.

[17] A. G. Dimakis, V. Prabhakaran, and K. Ramchandran. Decentralized erasure codes for distributed networked storage. *IEEE/ACM Transactions on Networking*, 14(SI):2809–2816, 2006.

[18] A. G. Dimakis, V. Prabhakaran, and K. Ramchandran. Distributed foutain codes for networked storage. In *Proceedings of the IEEE Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Toulouse, France, 2006.

[19] M. Félegyházi, J-P. Hubaux, and L. Buttyán. Equilibrium analysis of packet forwarding strategies in wireless ad hoc networks – the dynamic case. In *Proceedings of the Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, March 2004.

[20] Christina Fragouli, Jean-Yves Le Boudec, and Jörg Widmer. Network coding: an instant primer. *SIGCOMM Comput. Commun. Rev.*, 36(1):63–68, 2006.

[21] Tracey Ho, Ralf Kötter, Muriel Medard, David R. Karger, and Michelle Effros. The benefits of coding over routing in a randomized setting. In *Information Theory Symposium (ISIT). IEEE*, June 2003.

[22] Y.-C. Hu and A. Perrig. A survey of secure wireless ad hoc routing. *IEEE Security and Privacy Magazine*, 2(3):28–39, May/June 2004.

[23] Y.-C. Hu, A. Perrig, and D. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In *Proceedings of the ACM Conference on Mobile Computing and Networking (Mobicom)*, 2002.

[24] S. Y. R. Li, R. W. Yeung, and Ning Cai. Linear network coding. *Information Theory, IEEE Transactions on*, 49(2):371–381, 2003.

[25] S. Marti, T.J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom)*, August 2000.

[26] P. Michiardi and R. Molva. Core: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks. In *Proceedings of the International Conference on Communication and Multimedia Security*, September 2002.

[27] D. Molnar and D. Wagner. Privacy and security in library RFID: issues, practices, and architectures. In *Proceedings of the ACM Conference on Computer and Communications Security*, 2004.

[28] P. Papadimitratos and Z. Haas. Secure routing for mobile ad hoc networks. In *Proceedings of SCS Communication Networks and Distributed Systems Modelling Simulation Conference (CNDS)*, 2002.

[29] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao. Cooperation in wireless ad hoc networks. In *Proceedings of IEEE INFOCOM'03*, March-April 2003.

[30] A. Urpi, M. Bonuccelli, and S. Giordano. Modeling cooperation in mobile ad hoc networks: A formal description of selfishness. In *Proceedings of WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, March 2003.

[31] S. Zhong, Y. R. Yang, and J. Chen. Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks. In *Proceedings of IEEE INFOCOM'03*, March-April 2003.