Dr. Jelasity Márk bírálói kérdéseire adott válaszok

MTA doktori értekezés szerzője, címe:
Buttyán Levente
Új biztonsági mechanizmusok vezeték nélküli ad hoc és szenzorhálózatokban

Ezúton szeretném hálásan megköszönni Dr. Jelasity Márknak, hogy időt és energiát szánt MTA doktori értekezésem alapos átolvasására és megfogalmazta opponensi véleményét. Köszönöm az értekezéssel kapcsolatos észrevételeit és kérdéseit, melyeket az alábbiakban válaszolok meg:

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?

Az ad hoc hálózatok jelenleg elképzelt alkalmazási területei azokat a területeket ölelik fel, ahol fizikailag nagy kiterjedésű területen kell biztosítani a kommunikáció lehetőségét számos résztvevő számára, ugyanakkor nem feltételezhető kiépített kommunikációs infrastruktúra jelenléte, vagy annak használata valamilyen okból nem kívánatos (pl. drága). Tipikus civil példaként említhető a természeti katasztrófa által sújtott területen végzett mentés, ahol a mentő egységek kommunikációja elengedhetetlen, de a földi infrastruktúra a katasztrófa következtében esetleg megsemmisült. Igaz ugyan, hogy műholdas kommunikáció ebben az esetben is használható, ám ekkor is valós alternatíva lehet egy több ugrásos (multi-hop) vezeték nélküli ad hoc hálózat. Egy másik civil példa a precíziós mezőgazdaság, ahol nagy kiterjedésű megművelt területek vagy nagy területen mozgó állatok megfigyelése a cél, és a megoldás költsége fontos tényező, azaz pl. drága műholdas kommunikáció nem jöhet szóba.

Valószínűnek tartom továbbá katonai alkalmazások létezését (pl. drón rajok kommunikációja), ám erről nincs bővebb információm. A jövőben elképzelhetők űrkommunikációs alkalmazások is, bár ebben az esetben speciális ad hoc hálózatokról van szó, melyeket késleltetés tűrő hálózatoknak (Delay Tolerant Network, vagy DTN) neveznek. Az ad hoc jelleg itt abból fakad, hogy a csomópontok mozognak és közöttük a kapcsolatok folyamatosan változnak, valamint a kapcsolatok relatíve rövid ideig léteznek. Ezekben a hálózatokban tipikusan nem létezik egy teljes útvonal a kommunikációs végpontok között egy adott időpillanatban, ezért az adatokat store-and-forward jelleggel kell továbbítani a cél felé, és ez másfajta útvonalválasztó protokollokat igényel, mint amilyeneket a disszertációmban vizsgáltam. Egy viszonylag friss kapcsolódó cikk pl. a következő:

- T. Le, M. Gerla, Time-Constrained Anycast Routing under Short Contact Duration in Delay Tolerant Networks, Annals of Telecommunications, Vol. 73, pp. 549–558, 2018.

ami az Annals of Telecommunications 2018-as számában jelent meg, mely egy olyan speciális szám volt, amit az ad hoc hálózati technológiák jelenlegi trendjeinek és alkalmazásainak dedikáltak (Emerging Trends and Applications in Ad Hoc Networks). Továbbá a NASA olalán jelenleg is aktívnak látszik a DTN-ekkel kapcsolatos tevékenység[1].

Érdekes módon még okos otthon alkalmazásokban is előfordul az ad hoc (mesh) hálózati technológia használata, pedig ebben a környezetben más megoldás is szóba jöhetne, mert itt az infrastruktúra

[1] https://www.nasa.gov/directorates/heo/scan/engineering/technology/disruption_tolerant_networking

kiépítése nem kivitelezhetetlen. Egy konkrét termék ebben a kontextusban pl. a loxone rádiós eszköze[2] de sok más termék is létezik.

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?

A támadó modellem ebben a fejezetben azt feltételezi, hogy a támadó hozzá juthat néhány legitim csomópont kulcsaihoz:

"We further assume that the adversary has compromised some identifiers, by which we mean that it has compromised the cryptographic keys that are used to authenticate those identifiers. Thus, the adversary can appear as an honest participant under any of these compromised identities."

A támadó ezekkel a kulcsokkal nyilván képes a kompromittált csomópontok nevében üzeneteket küldeni. Úgy tűnhet, hogy ilyen feltételek mellett reménytelen a biztonság elérése, ám itt azt próbáltam meg kihasználni, hogy a támadót körülvevő, nem kompromittált csomópontok esetleg észrevehetik azt, ha a támadó hiteles, de nem helytálló útvonalválasztó információt továbbít üzeneteiben. Ezt nem egyszerű elérni, mint ahogy azt az is példázza, hogy több, az irodalomban javasolt "biztonságos" útvonalválasztó protokoll nem volt képes erre. Ugyanakkor, az általam javasolt endairA protokoll bizonyíthatóan biztonságos egy ilyen támadó modellben is.

A kérdés második fele arra vonatkozik, hogy mekkora lehet annak a valószínűsége, hogy egy legitim csomópont kulcsai kompromittálódnak. Ez általában alkalmazás függő. Sok olyan alkalmazás van, ahol a csomópontok publikusan elérhető fizikai lokáción vannak elhelyezve, valamint felügyelet és megfigyelés nélkül működnek. Ilyen alkalmazások lehetnek a mezőgazdasági vagy ökológiai célokra fejlesztett szenzorhálózatok, nagyobb építmények (pl. hidak, alagutak) monitorozását szolgáló szenzorhálózatok, és természetesen számos katonai alkalmazás. Ezekben az alkalmazásokban az a természetes támadó modell, hogy feltesszük azt, hogy ezek a felügyelet nélkül működő csomópontok elérhetők a támadó számára is, aki fizikailag megközelítheti és szétbonthatja őket, és így megszerezheti kulcsaikat, illetve módosíthatja viselkedésüket. Amellett, hogy több alkalmazásban valóban ez a támadó modell a helytálló, intellektuálisan is érdekes ebből kiindulni, mert egy ilyen erős támadó modellben nem triviális a biztonság elérése, pl. pusztán a kommunikációs üzenetek hitelesítésével. Ezért egész disszertációm alapfeltevése ez volt (lásd Introduction fejezet):

"While these types of wireless networks have potentially useful applications, they also represent an interesting challenge in terms of security. The most important challenges include the lack of physical protection and the scarcity of resources. In many applications, such networks are envisioned to be deployed in an environment where the devices simply cannot be protected by physical means. In addition, providing tamper resistance for devices is expensive, and therefore, it is not a viable option in applications where devices must be deployed in large quantities (e.g., sensors), and hence, unit cost must be kept very low. For this reason, we must assume that devices can be compromised, and we must design our security and privacy mechanisms in such a way that they do not fail in the presence of such compromised devices."

[2] https://shop.verdom.hu/loxone-air-base-extension

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?

A plauzibilis útvonal definíciójánál arra törekedtem, hogy figyelembe vegyem a támadó modell természetes következményeit és egyúttal a lehető legpontosabban megfogjam a "létező útvonal" intuícióját. Ahogy fentebb is kifejtettem, a támadó modell erős abban az értelemben, hogy sok mindent megengedett a támadó számára. A biztonság területén általában pesszimista hozzáállást követünk, és erős támadó modelleket használunk, mert ha képesek vagyunk egy protokollról megmutatni, hogy az biztonságos egy feltételezett erős támadó modell mellett, akkor biztonságos lesz egy a gyakorlatban ténylegesen előforduló, esetleg gyengébb támadó modellben is. Itt tehát azt feltételeztem, hogy a támadó rendelkezik néhány kompromittált csomópont kulcsaival (és így használni tudja ezek azonosítóit, akár hitelesített formában is), valamint hogy a támadó által kontrollált kompromittált csomópontok képesek egymás között valós időben információt megosztani. Egyszerűen nem lett volna védhető az a feltételezés, hogy a támadó csomópontok nem tudnak egymásról és nem tudnak információt megosztani egymás között. Ezen erős feltételezések mellett persze nem egyértelmű, hogy mi számít "létező útvonalnak" a gráfban, hiszen ahogy a disszertációban is leírtam, a támadó tetszőlegesen használhatja a kompromittált azonosítókat:

"Essentially, we must take into account that the adversary can always extend any route that passes through an adversarial vertex with any sequence of compromised identifiers. This is a fact that our definition of security must tolerate, since otherwise we cannot hope that any routing protocol will satisfy it."

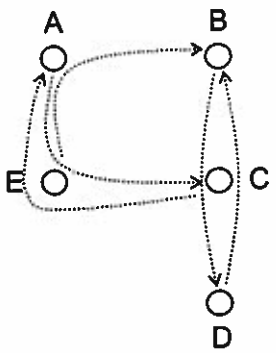
A plauzibilis útvonal fogalma tehát azt próbálja megfogni, hogy mi az ami egyáltalán hihető, hogy helyes útvonal, akkor ha a támadó a fenti képességekkel rendelkezik és tetszőlegesen kiegészíthet rajta áthaladó útvonalakat az által birtokolt és kontrollált azonosítókkal. A plauzibilis útvonal fogalma így valóban megengedő lett, mert szándékosan tolerálja azokat a támadásokat, amiket lehetetlen kivédeni az adott modellben. Azt gondolom azonban, hogy nem "túlságosan" megengedő, mert csak azt tolerálja, ami elkerülhetetlen. Nem gondolom, hogy a plauzibilis útvonal fogalma az adott támadó modell mellett tovább szigorítható.

Hogy következik-e ebből az, hogy a biztonságos útvonalválasztás lényegében lehetetlen? Nos, abban az értelemben igen, hogy még ha garantáljuk is, hogy a protokollunk csak plauzibilis utakat adhat vissza, ezek nem feltétlen lesznek a valóságban létező utak a tényleges hálózatot reprezentáló gráfban. Ugyanakkor, erősebbnek tartok egy olyan protokollt, ami bizonyíthatóan csak plauzibilis utakat ad vissza (mint pl. a disszertációban javasolt endairA), mint egy olyan protokollt, ami nem plauzibilis (azaz még a támadó modell mellett sem hihető) útvonalat is visszaadhat. Ebből kifolyólag, továbbra is látom értelmét a disszertációban bemutatott, biztonságos útvonalválasztással kapcsolatos fogalmaknak és eredményeknek.

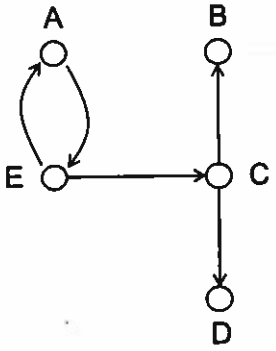
4. A hálózatban a 2.3 tézis szerint létezhet egy racionálisan kooperáló részhalmaz. Lehet ezt jellemezni valami strukturális módon (pl. maximális erősen összefüggő függőségi részgráf)? Illetve, vajon Nash egyensúly-e az az eset, amikor a 2.1 tétel szerint nem-kooperáló csúcsokon kívüli csúcsok TFT stratégiát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

Az első kérdésre a választ a disszertációm 40-41. oldalán leírt iteratív algoritmus működésének vizsgálatából nyerhetjük. Itt azt vizsgáltam, hogy mi történik akkor, mikor a 2.1 tétel feltételét kielégítő csomópontok defektálni kezdenek. Ezen csomópontok nem-reaktív viselkedése nem-reaktívvá tehet olyan függőségi hurkokat, melyek eddig reaktívak voltak. Ha ezáltal egy csomópontnak nem marad

reaktív függőségi hurka, akkor ő is defektálni kezd a 2.2 tétel következtében, és így a defektálás lavina hatás szerűen terjedhet a függőségi gráfban. Ha azonban a defektív hatás nem kebelezi be az egész gráfot, akkor marad olyan részhalmaza a csomópontoknak, akik számára a kooperáció legalábbis nincs kizárva. A kérdés tehát az, hogy mi a feltétele annak, hogy a defektív hatás ne tudja bekebelezni az egész függőségi gráfot. Mivel a hatás az irányított élek mentén terjed, ezért egy elégséges feltétel lehet egy olyan teljesen különálló komponens a függőségi gráfban, amiben a kooperáció feltételei adottak, vagy egy olyan részgráf létezése a függőségi gráfban, melyből csak kifelé mutató élek vannak, és melyben a kooperáció feltételei adottak. Példaként tekintsük az alábbi szcenáriót és hozzá tartozó függőségi gráfot:



(a) kommunikációs kapcsolatok



(b) függőségi gráf

Itt B, C, és D csomópontoknak egyáltalán nincs függőségi hurka, tehát a 2.1 tétel szerint, az ő legjobb stratégiájuk a defektálás. A defektív viselkedés azonban nem terjed át az A és E csomópontokra, mert az A és E csomópontokat tartalmazó részgráfba nem mutat él a B, C, és D csomópontokat tartalmazó részgráfból.

A fentiek folyománya, hogy a második kérdésre a válasz pozitív, azaz lehet az Nash egyensúly, hogy minden olyan csomópont, amelyiknek nincs reaktív függőségi hurka defektál, míg minden más (azaz reaktív függőségi hurokkal rendelkező) csomópont TFT stratégiát játszik. A fenti ábra erre is jó példa. Tudjuk, hogy a B, C, és D csomópontok a 2.1 tétel miatt defektálnak, ugyanakkor A és E csomópontok játszhatnak TFT-t, és ez számukra kedvező lehet, mivel egymás viselkedésétől közvetlenül függenek. Vegyük észre, hogy E csomópont viselkedésétől függ C csomópont haszna, míg fordítva nem így van, ezért E defektálhatna C-vel szemben. Ám a modellemben a csomópontok egy kooperációs szintet választanak és azt alkalmazzák minden útvonalon, nem tesznek különbséget az útvonalak között. Ezért ha E defektálna, az negatívan érintené A-t is, aki szintén függ E-től. Ha erre válaszul A is defektál, akkor ez visszahat E-re. Tehát E-nek megérheti magas kooperációs szintet választani A miatt, és ezzel, mintegy mellékhatásként, C forgalmát is továbbítani, feltéve, hogy C forgalmának továbbítási költsége nem magasabb, mint E abból származó haszna, hogy A továbbítja forgalmát. Utóbbi mondat azt is illusztrálja, hogy bár lehet az Nash egyensúly, hogy minden olyan csomópont TFT-t játszik, ami a 2.1 és 2.2 tételek miatt nem defektál, ám nem biztos, hogy ez mindig bekövetkezik, mert más feltételeknek a teljesülése is szükséges ehhez.

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.

A [79]-ben javasolt módszer szerintem is jól használható, ahogy ezt a szerzők a cikkükben be is mutatják. A módszer hátrányának tekinthető, hogy a csomópontoknak távolságbecslést kell végrehajtaniuk minden szomszédos pár között. Ez azonban nem jelent túlságosan nagy kihívást, és könnyen beépíthető a szomszédsági viszony felderítésére szolgáló (neighbor discovery) protokollba. A disszertációban javasolt módszerem minimális előnye [79]-cel szemben, hogy nincs szükség távolságbecslésre a csomópontok között, mert a javasolt módszer csak magát a szomszédsági relációt használja fel.

A féregjárat detekcióra tudomásom szerint a decentralizált megoldások terjedtek jobban el, melyek vagy biztonságos helymeghatározásra vagy distance bounding technikákra vagy ezek kombinációjára épülnek. A disszertációban javasolt distance bounding ötletet használva például társszerzőm, Srdjan Capkun később több olyan megoldást is javasolt, ami biztonságos helymeghatározást tesz lehetővé, és ez a féregjárat detekció problémáját is megoldja:

- S. Capkun, JP. Hubaux, Secure positioning of wireless devices with application to sensor networks, 24th Annual Joint Conference of the IEEE Computer and Communications Societies, 2005.
- S. Capkun, JP. Hubaux, Secure positioning in wireless networks, IEEE Journal on Selected Areas in Communications 24(2), pp. 221-232, 2006.
- D. Basin, S. Capkun, P. Schaller, Formal Reasoning about Physical Properties of Security Protocols, ACM Transactions on Information and System Security, September 2011.
- Ranganathan, S. Capkun, Are We Really Close? Verifying Proximity in Wireless Systems, IEEE Security & Privacy 15(3), 2017.

A decentralizált megoldások nagy előnye, hogy nemcsak a szenzorhálózatok kontextusában alkalmazhatók (ahol feltételezhető egy központi entitás, üzemeltető létezése), hanem olyan más gyakorlati esetekben is, melyekben a féregjárat támadás reális, valós problémaként jelentkezik. Erre példaként említhető a fizikai közelség bizonyítására épülő hozzáférésvédelem, pl. olyan rendszerek, melyekben proximity kártyákat vagy RFID alapú badge-eket használnak a fizikai hozzáférés szabályozására:

- A. Francillon, B. Danev, S. Capkun, Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars, Network and Distributed Systems Symposium, 2011.

Az ilyen rendszerekben csak a distance bounding vagy a biztonságos helymeghatározás használható a féregjárat (replay attack) detektálására. A gyakorlati megvalósíthatóságot és használhatóságot bizonyítja, hogy Srdjan Capkun egy sikeres spin-off vállalkozást[3] is létrehozott, mely a distance bounding ötletre épülve nyújt megoldást a biztonságos hozzáférésvédelem és helymeghatározás problémákra.

[3] https://www.3db-access.com/

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.

Tulajdonképpen a disszertációban szereplő jelenleg javasolt megoldás is alkalmazható úgy, hogy nagyobb, több levelet tartalmazó fával tervezünk, mint amennyi hitelesítendő eszközünk (pl. RFID tag-ünk) van valójában. A gyakorlatban egy ilyen rendszer üzemeltetése ezt úgyis megkívánja, hiszen kizárt, hogy a használatban levő eszközök száma ne változna az idő során, és célszerű már eleve nagyobb fával tervezni, hogy a később dinamikusan növekvő eszközszámot tolerálni tudjuk a rendszer (kulcsfa) teljes áttervezése nélkül. Tehát N valójában lehet a maximálisan elképzelhető eszközök száma. Továbbá N általában nem lesz prím, mivel az eszközök tipikusan valamilyen n bithosszúságú azonosítót használnak, így a lehetséges azonosítók száma N = 2^n lesz, és erre jól alkalmazható a disszertációban javasolt kulcsfa konstrukciós algoritmus. Az, hogy a disszertációban nem kötöttem meg, hogy N csak 2 hatványa lehet valójában általánosabbá teszi az eredményt, bár a gyakorlatban szinte kizárólag csak a kettőhatvány méretű rendszer jön számításba.

Azonban, ahogy erre az opponensi kérdés is rávilágít, ha nincs minden levél használatban, akkor a privacy mértéke függ attól, hogy mennyi tudása van a támadónak arról, hogy mely levelek "üresek" és melyek nem. A privacy mértéke ugyanis az eszköz-kompromittálódás eredményeként kialakuló anonimitás halmazok méretétől függ, és ha pl. a támadó pontosan tudja, hogy mely levelek "üresek", akkor ezeket a leveleket eleve kizárhatja az anonimitás halmazokból, csökkentve azok méretét, és ezzel az egész rendszerre jellemző mérőszámot is. Ez ellen úgy védekezhetünk, hogy a használt azonosítókat nem szisztematikusan, hanem véletlenszerűen allokáljuk az eszközök számára, így a támadó nem tudja biztosan, hogy mely levelek maradnak "üresek" a fában. Tovább növeli a támadó bizonytalanságát a gyakorlatban, hogy valószínűleg azt sem tudja biztosan, hogy mennyi levél van egyáltalán használatban, hiszen ez eleve folyamatosan változhat. Ezekkel a kiegészítésekkel, a gyakorlatban továbbra is megfelelő mértékű privacy-t biztosíthat egy jól tervezett kulcsfa.

A másik aspektus a hitelesítési késleltetés, ám ezt alapvetően nem a levelek száma, hanem a fa struktúrája (az elágazási faktorok értéke) határozza meg. Ha a maximális eszközszámra tervezzük a kulcsfát, és az biztosítja a hitelesítési késleltetés megfelelően alacsony értékét, akkor ezt a késleltetést akkor sem haladjuk meg, ha nem használjuk fel a fa összes levelét.

Budapest, 2021. március 19.

.....

Buttyán Levente