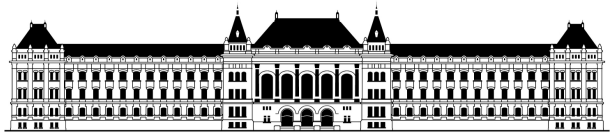


Budapesti Műszaki és Gazdaságtudományi Egyetem
Híradástechnikai Tanszék

Biztonságos adattovábbítás vezetéknélküli multi-hop hálózatokban mobil felhasználók számára

Tézisfüzet

Dóra László

Konzulens:
Buttyán Levente, Ph.D.

Budapest
2011

1. Bevezetés

Ebben a tézisfüzetben, két különböző többugrásos vezetéknélküli hálózat adattovábbítás biztonsági kérdéseivel foglalkozom. Ezen hálózatok a Késleltetés Tűrő Hálózatok és a Vezetéknélküli Mesh Hálózatok.

A Késleltetés Tűrő Hálózat (angol nevén Delay Tolerant Network, továbbiakban DTN) egy olyan infrastruktúra nélküli hálózat, amelyben az üzenetek továbbításáért a résztvevő — általában akkumulátorral működő — végfelhasználók felelnek. Az üzenetek a *store-carry-and-forward* (azaz tárolj-szállíts-és-továbbíts) elvnek megfelelően jutnak célba. Ezzel a módszerrel, az üzenetek akkor is célba tudnak jutni, ha soha sincs online útvonal a forrás és a cél között. Ez úgy lehetséges, hogy a közbülső mobil csomópontok magukkal hordozzák az üzenetet és átadják más közbülső csomópontoknak, ha kapcsolatba kerülnek (pl. egymás közelébe érnek).

Az feladatokat olyan Késleltetés Tűrő Hálózatokban azonosítottam, melyeket tipikusan felhasználók által birtokolt mobil telefonok alkotnak, és helyi információt kell terjeszteni a hálózatban a felhasználók érdeklődési körének megfelelően.

Mivel a vizsgált alkalmazásokban a célpontot mindig a felhasználó érdeklődési köre határozza meg, a csomagokat a résztvevők a dissemination alapú algoritmusok alapján továbbítják. A dissemination alapú algoritmusok esetén a közbülső csomópontok számára nem áll rendelkezésre információ a lehetséges útvonalakról a célpont(ok) felé. Éppen ezért, és mivel maguk a célpontok sem ismertek, minden üzenetet el kell terjeszteni az egész hálózatban. A dissemination alapú algoritmusok alapja az elárasztás, és abban különböznek, hogy miként korlátozzák az üzenetek többszöröződését.

Négy különböző az adattovábbítással kapcsolatos biztonsági feladatot azonosítottam a fent leírt DTN hálózatokban: 1) kooperáció ösztönzése, 2) SPAM üzenetek terjedésének megakadályozása, 3) egyenlőség biztosítása és 4) privacy megóvása.

Egy szokásos Vezetéknélküli Mesh Hálózat mesh routerekből áll (MR), amelyek egy statikus vezetéknélküli ad hoc hálózatként infrastruktúrát biztosítanak a hozzájuk csatlakozó mesh kliensek számára (MC). Mivel a mesh hálózatok többnyire nem különálló hálózatok, ezért a mesh routerek közül néhány egyben a gateway feladatát is ellátja tipikusan a vezetékes Internet irányába. A mesh routerek egy részcsoportja access pointként (AP) is funkcionál, amin keresztül a mesh kliensek a hálózathoz kapcsolódhatnak. Egy mesh router lehet egyszerre gateway és access point is, de az is előfordulhat, hogy egyik feladatot sem látja el.

Olyan Vezetéknélküli Mesh Hálózatokkal foglalkozom, ahol a karbantartásért operátor felel, aki szélessávú Internet elérést biztosít a vele szerződést kötő ügyfeleknek. Az ötlet egyre nagyobb népszerűségnek örvend (lásd pl. Ozone mesh hálózata Párizsban `www.ozone.net` és a Cloud Londonban `www.thecloud.net`).

Ezekben a hálózatokban egy újfajta hozzáállás, hogy a mesh routerek karbantartását több, a hálózati szolgáltatás biztosításáért együttműködő operátor végzi. Ez az együttműködés lehet üzleti szerződés alapú (hasonlóan a roaminghoz a celluláris hálózatoknál). Az ügyfelek egy vagy több operátorral kötnek szerződést, de lehetőségük van, hogy az együttműködő operátorok által üzemeltetett területeken is roamingoljanak, amennyiben szükségessé válik. A hálózati szintű együttműködésnek számos előnye van (pl. a telepítési költségeket lehet leszorítani azzal, hogy egymás eszközeit használhatják az operátorok).

A sávszélesség növelhető azáltal, hogy a mesh routereket több vezetéknélküli interfésszel szereljük fel és azokon keresztül több csatornán kommunikálnak a szomszédaikkal. Ugyanakkor ez a fajta hozzáállás speciális biztonsági tervezést igényel. Ráadásul cél, hogy a felhasználói mobilitást az általam vizsgált WMN támogassa miközben QoS követeléményeknek is megfelel, mivel a MC-ek mozoghatnak QoS érzékeny alkalmazások futtatása közben.

A továbbiakban a fent leírt Vezetéknélküli Mesh Hálózatokra, amely több operátor által

üzemeltetett, több vezetéknélküli csatornát használ több interfészen keresztül és támogatja a QoS érzékeny alkalmazást futtató felhasználók mobilitását, Mulit-WMN-ként hivatkozunk.

Az biztonságos adattovábbítás kérdéskörének három fő csoportját azonosítottam Multi-WMN hálózatokban: 1) MC gyors hitelesítése és hozzáférés védelem a hálózat erőforrásaihoz, 2) vezetéknélküli kapcsolatok védelme beleértve a biztonságos útvonalválasztást, és 3) behatolás és elvárttól eltérő viselkedés felismerése és a hálózat helyreállítása.

2. Kutatási célkitűzések

A DTN-ben alapvető fontosságú, hogy az önző viselkedést megakadályozzuk, mivel az adattovábbítás a végfelhasználók hajlandóságán múlik. A jelenlegi hírnév és elektronikus fizetőeszköz alapú megoldások nem felelnek meg a DTN-es környezet elvárásainak. Alapvető célom javasolni egy olyan elosztott ösztönző mechanizmust, amelynek köszönhetően a csomópontok akkor is tárolják, szállítják, és továbbítják az üzeneteket, ha ők az üzenetre nem kíváncsiak. A mechanizmustól elvárt, hogy növelje a kézbesített csomagok számát, a kézbesítés idejét pedig csökkentse.

A másik probléma, amit vizsgáltam DTN-es környezetben, a felhasználók követhetősége. A vizsgált probléma speciálisan a store-carry-and-forward adattovábbítási elv miatt merül fel. Konkrétan, egy támadó képes lehet profilozni a felhasználókat arra építve, hogy milyen üzeneteket tárolnak, és milyeneket akarnak letölteni másoktól. A profilozás után a csomópontok követhetővé válnak, akkor is ha anonim linkeken kommunikálnak egymással. Célom egy olyan védelmi eljárás tervezése a fent leírt követhetőségi problémára, mely nem veszélyezteti a csomópontok elsődleges célját: az üzenetek gyűjtését.

A Multi-WMN hálózatokat illetően a gyors hitelesítésre és a hozzáférés-védelem biztosítására koncentrálok. Célul tűztem ki, hogy a hitelesítés késleltetését lecsökkentsem, hogy a mobil felhasználók hívásátadása megszakításmentesen menjen végbe az access pointok váltása között. Sok javasolt gyors hitelesítési eljárás olyan megbízhatósági modellre épít, amely nem felel meg a multi-operátor környezet követelményeinek. Ebben a disszertációban célom egy olyan hitelesítő és hozzáférés-védelmet biztosító eljárás tervezése, amely a Multi-WMN hálózatokkal szemben támasztott minden követelménynek megfelel.

A másik vizsgált probléma a Multi-WMN hálózatokban a szabálytalanul viselkedő routerek azonosítása és kikerülése a további forgalmak esetén. Szabálytalanul viselkedő routerek alatt azokat értjük, amelyek hamis információt küldenek magukról az útvonalválasztó algoritmus kontroll üzeneteiben. A feladat megoldása azért is fontos, mivel a szabálytalanul viselkedő routerek rendelkezhetnek érvényes kulcsokkal, amelyekkel hitelesített kontroll üzeneteket küldenek, aminek információját a fogadó fél felhasználhatja. A jelenlegi megoldások azért nem optimálisak, mert azok vagy magas többlet terheléssel járnak, vagy a vezetéknélküli kapcsolatok több csatornás jellegét nem támogatják. Célom egy olyan eljárás tervezése, amely azon szabálytalanul viselkedő routereket azonosítja, amelyek hamis információt küldenek magukról vagy a hozzájuk kapcsolódó kapcsolatokról. Az eljárással szemben elvárt, hogy ne terhelje feleslegesen a hálózatot, ugyanakkor támogassa a több csatornás kommunikációt.

3. Kutatási módszerek

A munka legelején összeállítottam egy listát az eljárással szemben támasztott követelményekről. A már létező megoldásokat a követelménylista figyelembevételével tekintettem át. Ha egyik eljárás sem elégítette ki az összes követelményt, egy új megoldást javasoltam, amelyet addig terveztem, amíg az összes követelménynek meg nem felelt.

Formális módszereket alkalmaztam, szimulációt vagy valós implementációt készítettem annak bizonyítására, hogy a javasolt eljárás az elvárt módon működik a neki szánt környezetben. Ha

nem készült valós implementáció, a problémát egy modellben helyeztem el (beleértve a támadó modellt is), amely modell valószínűségi és játékelméleti alapokon nyugszik.

A javasolt módszerek hatékonyságának mérésére különböző metrikákat vezettem be, amelyek lehetővé tették a javaslatot már létező eljárásokkal vagy a legjobb és legrosszabb esetekkel való összehasonlításra. A metrikák tulajdonságainak felderítésére Markov modellt és valószínűség számítást használtam.

Vizsgálataim mégis a modellek komplexitása miatt többnyire átfogó szimulációra építenek. Az eredmények kiértékelését több szimulációs futtatás eredményeinek átlaga és tapasztalati szórása vagy konfidencia intervalluma alapján végeztem. Valós mobilitást a SUMO mobilitási környezettel [SUM10] helyettesítettem, amelynek az eredményét C++ vagy Matlab alapú szimulátorban használtam fel.

4. Új eredmények

4.1. Barter a kooperatív adattovábbítás ösztönzésére Késleltetés Tűrő Hálózatokban

1. TÉZISCSOPORT:. *A kooperatív adattovábbítás ösztönzésére barter alapú üzenetcsere eljárást javasolok Késleltetés Tűrő Hálózatok számára. Szimuláció segítségével megmutatom, hogy a javasolt eljárás valóban ösztönzi a csomópontokat az üzenetek továbbítására, amely gyorsabb és nagyobb arányú kézbesítést eredményez. [C4] [J2]*

A [PVS07] cikkben azonosított problémák motiváltak, hogy egy olyan ösztönző eljárást javasoljak, melynek köszönhetően a felhasználók akkor is továbbítják egymás üzeneteit, amikor az üzenet tartalma számukra érdektelen. A javasolt eljárás a *barter* mechanizmus köré épül: a felhasználók az üzenetekkel kereskednek, és csak akkor tudnak letölteni egy üzenetet a másiktól, amennyiben ők is képesek adni egy újat viszont. Ettől azt várom, hogy a felhasználók akkor is letöltenek üzenetet, ha nem érdekli őket a tartalma, hogy később egy olyanra tudják cserélni, ami már érdekes. Ezáltal az üzenetek gyorsabban terjednek a hálózatban.

1.1. TÉZIS:. *Az önzőség Késleltetés Tűrő Hálózatokra gyakorolt hatásainak vizsgálatára modelleztem a hálózatot és a benne szereplő résztvevőket, valamint szimulációt futtattam. A bartert, mint üzenetcsere eljárást alkalmaztam, ami egy olyan rendszert eredményezett, amely nem kíván központi egységet, mint az elektronikus fizetésen alapuló megoldások, és amely nem várja a szereplőktől, hogy megfigyeljék egymást, mint ahogy a hírnév alapú eljárások. Játékelmélet segítségével megmutattam, hogy a szimulációs paraméterek széles tartományában a Nash Egyensúlyi stratégia azt diktálja a felhasználók számára, hogy akkor is gyűjtsenek és terjesszenek üzeneteket, ha az üzenet tartalma számukra érdektelen. Ez azt jelenti, hogy a barter alapú megoldás valóban csökkenti az önzőség hátrányos hatásait [C4] [J2]*

A modellünkben a felhasználó és eszköze együttesen alkotja a *mobil csomópont*ot. Az üzeneteket speciális, ún. *üzenet csomópont*ok generálják.

Mindegyik üzenet vagy elsődleges vagy másodlagos egy mobil csomópont számára. Elsődleges, ha az adott csomópontot érdekli az üzenet tartalma, és másodlagos, ha nem.

Egy üzenetet két alapvető tulajdonságával jellemzem: az egyik a *popularitás* (ζ), a második pedig az *érték csökkenés karakterisztika* (δ). A popularitás azt írja le, hogy egy véletlenül választott mobil csomópont milyen valószínűséggel érdeklődik az adott üzenet tartalma iránt. Az érték

csökkenés karakterisztika meghatározza, hogy hogyan változik az üzenetek értéke az időben. A másodlagos üzeneteknek nincs közvetlen értéke a csomópontok számára.

A modellben, a mobil csomópontok nem tudnak akármennyi üzenetet kicserélni egymással, csak időszeletenként egyet. Ez a csere *implicit költség*e, mivel egyáltalán nem garantált, hogy a csomópontok minden üzenetet le tudnak tölteni egymástól, amit akarnak. A modellben nincs egyéb költség, ugyanakkor a mobil csomópontok kitörölnek minden olyan üzenetet, aminek az értéke D küszöbszint alá esik.

Ahogy az 1. képleten látható, az i. csomópont *goodput*ja a t-edik időszeletben ($0 \leq G_i(t) \leq 1$) az elsődleges üzenetek megszerzéskori értékének összege ($v_i(\tau)$) normalizálva az ideális esetben megszerezhető maximális értékkel ($|M_i^P(t)|$).

$$G_i(t) = \frac{\sum_{\tau=0}^{t} v_i(\tau)}{|M_i^P(t)|} \tag{1}$$

$v_i(\tau)$ számítását az érték csökkenés függvényéből számolhatjuk a következőképp: $v_i(t) = \delta(t - T_{m_i^t})$, ahol m_i^t az üzenet, amit i csomópont töltött le a t. időszeletben, T_m az m üzenet generálásának időszelete.

A goodput ugyan időben változhat, de konvergál egy határértékéhez, amint ezt az 1.3. tézisben bebizonyítom. Tehát a továbbiakban a goodputot a határértékében vizsgálom és G_i-ként jelölöm minden i csomópont esetén.

$$G_i = \lim_{t \to \infty} G_i(t) \tag{2}$$

A javaslatom szerint a mobil csomópontok közötti adattovábbítás ösztönözhető a *barter* elv segítségével. A mobil csomópontok egyenlő számú üzenetet cserélnek ki egyesével az általuk meghatározott sorrendben. A modellben a sorrendet az üzenetek érték csökkenés karakterisztikája határozza meg.

Ahogy már említettem, a másodlagos üzeneteknek nincsen közvetlen haszna a csomópontok számára, ugyanakkor megéri letölteni azokat, hogy később elsődleges üzenetre lehessen cserélni. Ennek megfelelően a másodlagos üzenetek értéke csupán a letöltés sorrendjének meghatározásakor kerül számításba. Mobil csomópontok számára, a másodlagos üzenet értéke t időszelettel a generálás után $SP \cdot \delta(t)$. SP a *másodlagos/elsődleges arányszám* (secondary/primary ratio). Fontos megjegyezni, hogy ha $SP_u = 0$, akkor az u csomópont nem tölt le egyáltalán másodlagos üzenetet.

A barter alapú eljárást játékként elemeztem, hogy a mobil csomópontok viselkedését megvizsgálhassam. Definiáltam egy nem kooperatív játékot $G = [P, \{S_i\}, \{\pi_i\}]$, amit *barter játék*nak neveztem. P a játékosok halmaza, S_i az i. játékos stratégiai tere, és π_i az i. játékos kifizetése. A pontosság kedvéért π_i egy egyszerűsített jelölése a $\pi_i(s_0, s_1, ..., s_{|P|-1})$-nek, mivel minden játékos kifizetése függ a saját és többi játékos stratégiájától.

A barter játékban, a játékosok (P) a mobil csomópontok (éppen ezért a továbbiakban ugyanazt a jelölést használom a játékosokra, mint a mobil csomópontokra). A stratégiai tere minden játékosnak a másodlagos/elsődleges arányszám ($SP_i \in S_i = [0, 1]$). Feltételezzem, hogy a játékosok a stratégiájukat nem változtatják meg a játék során, viszont úgy választják meg azt, hogy minél nagyobb goodputot érjenek el. Éppen ezért a játékosok kifizetése a határértékben vett goodput ($\pi_i = G_i$).

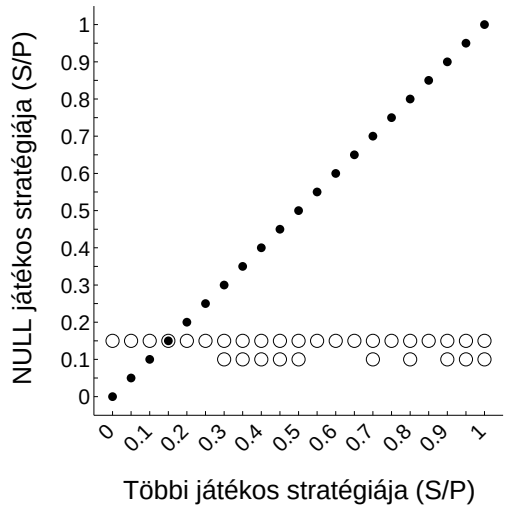
Jól látható, hogy a barter játék egy szimmetrikus játék, mivel minden játékosnak azonos a stratégiai tere ($S_0 = S_1 = ... = S$) és azonos a kifizetés függvénye is ($\pi_i = \pi_j, i, j \in P$). Egy G szimmetrikus játék egyszerűsített jelölése $[P, S, \pi()]$.

A barter alapú eljárás vizsgálata során a Nash Egyensúlyt [FT91] keressük. Azzal az egyszerűsítéssel élek, hogy csak a tiszta, szimmetrikus Nash Egyensúlyi stratégiákat találjuk meg.

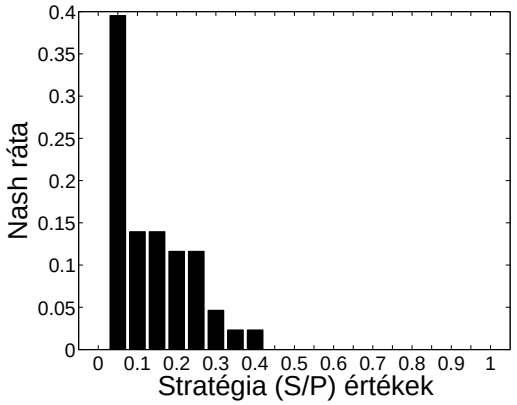
Egy szimmetrikus játékban $\{s^*\}$ egy Nash Egyensúly, ha a következő képlet igaz mindegyik i játékosra ($i \in P$):

$$s_i^* = \arg\max_{s_i \in S} \pi(s_0^*, s_1^*, \dots, s_i, \dots), \text{where } s_u^* = s_v^* \forall u, v \in P/\{i\} \tag{3}$$

A képletből következik, hogy könnyű ellenőrizni, hogy egy adott stratégia profil ($\{s'\}$) Nash Egyensúly-e. Bármely i játékosra ($i \in P$) nézve — az általánosság elvesztése nélkül legyen ez a játékos $i = 0$, és nevezzük *NULL játékos*nak —, ha az i játékosnak megéri más stratégiát választani, $\{s'\}$ nem Nash Egyensúlyi stratégia. Ugyanakkor, ha s' a legjobb választás i játékos számára, akkor s' lesz a legjobb választás a többiek számára is, hiszen a kifizetés függvény minden játékos számára azonos a játék szimmetriája miatt. Tehát, a szimmetrikus tiszta Nash Egyensúlyi stratégia megtalálásához elegendő egy két dimenziós teret vizsgálni, ami független a játékosok számától.



1. ábra. **Nash Egyensúly a barter játékban**

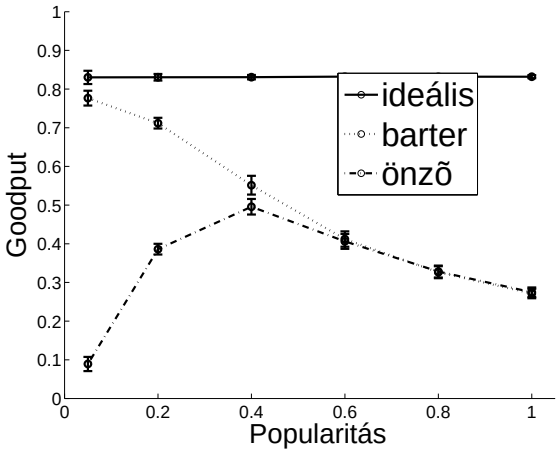


2. ábra. **Nash Egyensúly értékeinek hisztogramja**

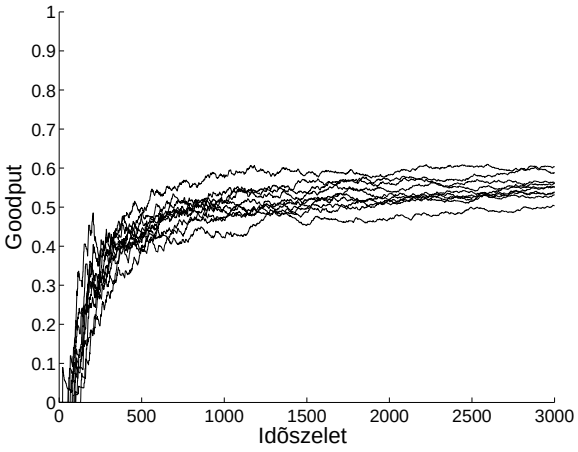
A modell komplexitása miatt analitikus helyett szimulációs eszközöket használtam. A szimulációs környezetet C++-ban készítettem, ahol 300 mobil csomópont mozgott diszkrét időszeletekben az alábbi két mobilitás modellnek megfelelően: Restricted Random Waypoint [BGLB02] és Simulation of Urban MObility [SUM10] modell.

Az 1. ábrán, ahol NULL játékos legjobb válaszát ábrázoljuk egy reprezentatív szcenárióban, a függőleges tengelyen a NULL játékos stratégiai tere látható, míg a vízszintes tengelyen a többi játékosé. A jelölt Nash Egyensúlyi stratégiák azok, amelyek mind a NULL játékos, mind a többi játékos esetén megegyeznek (ezeket fekete ponttal jelöltük). A NULL játékos legjobb válaszát a többi játékos stratégiájára fekete körökkel jelenítettük meg. A Nash Egyensúlyt azok az $\{s\}$ stratégiák jelentik, ahol a jelöltek egybeesnek a NULL játékos legjobb válaszával.

A 2. ábrán a Nash Egyensúly értékeinek hisztogramja látható minden szimulációt figyelembe véve. Az ábra azt mutatja, hogy a szimulált esetekben azok a stratégiák a legelőnyösebbek — azaz a barter játék Nash Egyensúlya —, amelyekben a másodlagos/elsődleges arányszám alacsony, de nem 0. Tehát, a barter alapú eljárás segítségével hasznos mások üzeneteit továbbítani ($s \neq 0$).



3. ábra. **Goodput értéke ideális, önző és barter alapú hálózat esetén**



4. ábra. **A goodput konvergálása néhány véletlenül kiválasztott csomópont esetében**

1.2. TÉZIS:. *Szimuláció segítségével megmutatom azt, hogy a barter mechanizmus a mobil csomópontok ösztönzése által teljesíti az eredeti elvárást, miszerint az üzenetek nagyobb arányban és gyorsabban jutnak el az érdeklődőkhöz azokban az esetekben, amikor az önzőség a fő oka a lassú üzenet-terjedésnek. Továbbá megmutatom, hogy bizonyos esetekben a goodput megközelítheti a rendszeren belül ideálisnak tekinthető esetet. Mindezt három eset összehasonlításával teszem meg: 1) amikor minden felhasználó Nash Egyensúlyban lévő stratégiát választja a barter alapú eljárás kényszerítő hatása mellett, 2) amikor minden felhasználó önző módon csak az őt érdeklődő üzeneteket továbbítja barter nélküli rendszerben, valamint 3) amikor minden felhasználó minden üzenetet mindenféle megkötés nélkül azonnal továbbít. [C4] [J2]*

A 3. ábrán a hálózat goodputját ábrázolom különböző popularitási értékek függvényében három különböző szcenárióban. A folytonos vonallal jelölt függvény egy ideális értéket határoz meg a goodputra tapasztalati úton, ami mögött az áll, hogy minden csomópont minden üzenetet (elsődlegest és másodlagost egyaránt) azonnal letölt egyetlen időszeletben. A ponttal és vonallal jelölt függvényen azt ábrázolom, amikor a csomópontok önző módon viselkednek, és semmilyen mechanizmus nem ösztönzi őket, hogy kooperáljanak, tehát csak elsődleges üzenetek terjesztenek. Végül a ponttal ábrázol függvény a barter alapú eljárás hatékonyságát mutatja, ahol a csomópontok a barter játék Nash Egyensúlyi stratégiáját követik. Mindegyik szimulációban az üzenetek azonos popularitási értékkel rendelkeznek. A függvények szimulált pontjaiban feltüntetem a 95%-os konfidencia intervallumot is.

Ahogy az ábráról leolvasható, a barter alapú eljárás látványosan növelte a hálózat goodputját, ahol az üzenetek popularitása alacsony volt. Ráadásul ezekben az esetekben a goodput megközelítette az ideális eset értékét. Ugyanakkor a barter alapú eljárás nem csökkentette a goodputot azokhoz az esetekhez képest sem, amikor nem ösztönözte semmi a csomópontokat, de a magas popularitás érték miatt amúgy is terjesztették az üzeneteket. A popularitás növelésével a goodput a barter esetén csökken, mert a vizsgált esetekben a letölthető üzenetek száma eléri a rendszer adta határokat, míg a elsődleges üzenetek aránya könnyen tud növekedni.

1.3. TÉZIS:. *A hálózat vizsgálata mind az 1.1. és az 1.2. tézisben a goodput metrikára épít, amely egyszerre tükrözi a csomagok kézbesítési arányát és idejét. Mivel a goodput értékét szimulációval határoztam meg, kritikus, hogy azt a határértékben vizsgáljuk. Markov modellt használva megmutattam, hogy a goodput értéke exponenciálisan konvergál a határértékhez. Tehát a goodput értéke nem változna lényegesen hosszabb szimuláció esetében sem, mint amit empírikus úton határoztam meg. [J2]*

Annak bizonyítására, hogy a goodput konvergál a határértékéhez ahogy a 4. ábra mutatja, a bemutatott rendszert véges állapotú Markov modellbe helyeztem. A Markov modell egy állapota t időpontban a következőképp írható le:

$$\begin{aligned} s(t) = \{&B_1(t), B_2(t), \ldots, B_N(t), \\ &Z_1(t), Z_2(t), \ldots, Z_N(t), \\ &H_1(t), H_2(t), \ldots, H_N(t)\} \end{aligned} \tag{4}$$

ahol

- N a mobil csomópontok száma
- $B_i(t) = [m_{i_1}, m_{i_2}, \ldots]$ az i mobil csomópont buffere, ahol az üzeneteket tárolja. A buffer mérete 2^l, ahol l az üzenet maximális hossza.
- $Z_i(t) \in \{*, m\}$ az i üzenet csomópont bufferében tárolt üzenet i, ahol $*$ azt az esetet jelöli, amikor t időpontban semmilyen üzenetet nem tárol, különben m a generált üzenetet jelöli, amely az üzenetek egy véges halmazából kerül ki.
- $H_i(t)$ az i csomópont pozícióját határozza meg az F területen, amelyen a mobil csomópontok mozognak.

Az állapottér leírható egy determinisztikus leképzéssel, ahogy a következő képlet mutatja:

$$\begin{aligned} s(t+1) = \mathfrak{f}[&s(t), \\ &r_1(t+1), r_2(t+1), \ldots, r_N(t+1), \\ &r'_1(t+1), r'_2(t+1), \ldots, r'_n(t+1), \\ &r''_1(t+1), r''_2(t+1), \ldots, r''_M(t+1)] \end{aligned} \tag{5}$$

ahol $r_i(t+1)$, $r'_j(t+1)$ és $r''_k(t+1)$ véletlen számok, amelyek rendre meghatározzák az i csomópont következő lépését, a j üzenet csomópont üzenet generálását, valamint a csomópontok párosítását a k. helyen. A véletlen számok egymástól és időtől függetlenül generálódnak.

Könnyű látni, hogy az állapotátmeneti leképzés időfüggetlen. Az állapot változók sorozata $S(0), S(1), \ldots, S(t), \ldots$ diszkrét idejű homogén Markov láncot alkotnak. A Markov folyam állapotátmeneti mátrixa levezethető a 4. és az 5. képletből. Az állapotátmeneti mátrix P_{ij} eleme meghatározza annak a valószínűségét, hogy a rendszer az i állapotból a j állapotba kerül.

A Markov-lánc *ergodikus*, ha $\lim_{n\to\infty} P_{ik}^{(n)} = P_k$ határérték minden k-ra létezik, és a határérték független i-től és $\sum_{k=1}^{\infty} P_k = 1$.

Ahogy a Markov-láncok klasszikus elmélete állítja, egy véges állapotú homogén Markov-lánc ergodikus, ha irreducibilis és aperiodikus. Azaz létezik t időszelet és j állapot, hogy j állapot tetszőleges i kezdeti állapotból pozitív valószínűséggel elérhető legyen t időszeleten belül. A P_j határérték eloszláshoz való konvergencia exponenciális, ami a következőt jelenti: $P_{ij}^{(t)}$ jelentse a

valószínűséget, hogy a Markov-lánc i állapotból j állapotba t időszeleten keresztül jut el, ezen kívül a stacionárius valószínűsége a j állapotnak legyen P_j, ekkor a $|P_{ij}^{(t)} - P_j|$ különbség exponenciálisan csökken, amikor t tart végtelenbe (Markov elmélete). Ekkor létezik j-től független exponenciális határ a $|P_{ij}^{(t)} - P_j|$ különbségre.

A modellben az ergodikus tulajdonságot a következőképp bizonyítom: Feltételezzük, hogy a rendszer tetszőleges állapotban van. Kiválasztunk egy k állapotot, amelyben az első csomópont egy friss üzenettel rendelkezik, a többieknek pedig üres a buffere. A k állapot bármely másik állapotból a következőképp érhető el: Először minden csomópont buffere kiürül oly módon, hogy a mobil csomópontok úgy mozognak vagy állnak egy fix ponton, hogy közben nem találkoznak üzenet csomóponttal. Ahogy az idő telik, a régi üzeneteket a mobil csomópontok eldobálják. Ezután az első node közel kerül egy üzenet csomóponthoz, amelyik éppen generál egy üzenetet, és azt a csomópont átveszi.

Ahogy fent megmutattam, a rendszer ergodikus, tehát a stacionárius állapotban lévő eloszláshoz exponenciális gyorsasággal közeledik.

Ugyanakkor az 1. képletet vizsgálva jól látható, hogy a goodput értékét nem csak a stacionárius állapotú viselkedés határozza meg, hanem a tranziens állapoté is. Viszont a Markov-láncok ergodicitásából következik, hogy a tranziens állapot hatása exponenciális gyorsasággal tűnik el és elhanyagolhatóvá válik, ahogy az idő tart a végtelenbe. Empírikus megfigyelés alapján úgy látom, hogy a goodput értéke 3000 időszelet után lényegesen nem változik a későbbiekben.

4.2. Hide-and-Lie a privacy fokozásáért Késleltetés Tűrő Hálózatokban

2. TÉZISCSOPORT:. *A felhasználók követhetőségének megakadályozására dissemination alapú Késleltetés Tűrő Hálózatokban egy ún. Hide-and-lie metódust javasoltam. Ez az eljárás olyan támadások ellen nyújt védelmet, amelyben a támadó profilt épít a felhasználókról az alapján, hogy milyen információt akarnak letölteni és milyen információt tudnak megosztani a többiekkel. Ez a fajta támadás követhetővé teszi a felhasználókat akkor is, ha a többiekkel anonim kapcsolatokon keresztül kommunikálnak. [C6]*

A csomópontok közötti kommunikáció információt szivárogtathat ki a felhasználók érdeklődéséről. Ebben a téziscsoportban olyan támadásokkal foglalkozom, amelyek az ilyen kiszivárogtatott információra építenek.

2.1. TÉZIS:. *Az 1. téziscsoportban bemutatott modellt alkalmazva alkottam meg a támadó modellt, melyben több specifikus támadási algoritmust is kidolgoztam Késleltetés Tűrő Hálózatokban. Szimuláció segítségével megmutattam, hogy a vizsgált modellben a csomópontok nagy valószínűséggel követhetők, ha semmilyen védelmi mechanizmust nem alkalmaznak. Analitikusan felsőbecslést adtam az érdeklődési kör alapú támadó sikerességére. [C6]*

Az egyszerűség kedvéért azt feltételezzem, hogy minden üzenetet be lehet sorolni a C számú kategória egyikébe. Egy friss üzenet $\frac{1}{C}$ valószínűséggel tartozik egy adott kategóriába. Minden csomópont ε valószínűséggel érdeklődik egy adott kategória üzenetei iránt. Szintén az egyszerűség kedvéért minden csomópont számára a ε értéke azonos a vizsgált szcenárióban.

Azt feltételezzem, hogy egy támadó a következő felhasználói profilt tudja megbecsülni u csomópont esetén a t időpontban:

$$UP_u(t) = (EIP_u(t), CHM_u(t), IDL_u(t)) \tag{6}$$

ahol UP a következő hármasból áll:

- Becsült Érdeklődési Profil (EIP) egy bináris vektor. A vektor k. eleme 1, ha az u felhasználó érdeklődést mutat a k kategória iránt.
- Felajánlott Üzenetek Kategória Hisztogramja (CHM) azt mutatja, hogy mennyi az u felhasználónál tárolt üzenet tartozik egy adott kategóriába.
- IDL a felajánlott üzenetek egyedi azonosítói.

A támadó a támadó modell szerint a következőképp viselkedik:

1. A támadó azonosítja a célpontot (u_T) N számú csomópont közül.
2. A támadó megbecsüli a célpont felhasználói profilját: $UP_{u_T}(t_0)$. Az az időszelet, amikor ez történik a referencia időpont, és t_0-ként jelölöm.
3. τ időszelettel később ($t_1 = t_0 + \tau$), a támadó megbecsüli minden felhasználó profilját $UP_{u_i}(t_1), i \in [1..N]$, és kiszámítja a távolságot u_i és u_T profilja között. τ a támadás késleltetését jelöli.
4. A támadó azt a csomópontot választja, amelyiknek a profilja a legjobban hasonlít a célpontra. Ha több azonos közelségű van, akkor véletlenszerűen választ egyet közülük. A támadás akkor sikeres, ha a kiválasztott csomópont éppen az u_T célpont.

A fent vázolt sikervalószínűség jó privacy metrikának tekinthető, mivel ez az, ami a legtöbbet elárul a támadás várható kimeneteléről.

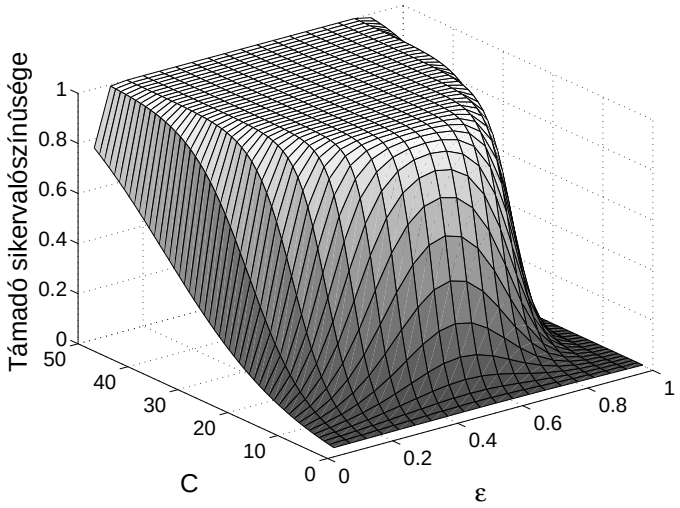
A begyűjtött felhasználói profilok összehasonlítására ún. támadófüggvényeket definiáltam, amit $\mathcal{A}$-val jelölök. Az $\mathcal{A}$ bemenete $N+1$ felhasználói profilból áll, a kimenet pedig a kiválasztott csomópont ID-je:

$$\mathcal{A} : (UP_{u_T}(t_0), UP_{u_i}(t_1), i \in [1..N]) \rightarrow j, j \in [1..N] \tag{7}$$

A támadás akkor és csak akkor sikeres, ha $j = T$.

Világos, hogy a legegyszerűbb támadó számára is elérhető a $\frac{1}{N}$ sikervalószínűség egyszerű találgatással. Kifinomultabb támadófüggvényekkel nagyobb sikervalószínűség is elérhető. A következőkben négy támadófüggvényt mutatok be:

- **Előszűrt üzenet ID alapú támadásfüggvény:** A támadó először is kiszűri azokat a csomópontokat, amelyiknek a EIP-je eltér a célpontétól csak azokat hagyva a listában, akiknek a $EIP_u(t_1)$ azonos $EIP_{u_T}(t_0)$-val. A maradék listából azok maradnak bent, akiknek a $IDL_u(t_1)$ a legközelebb áll a $IDL_{u_T}(t_0)$-hez. Távolság alatt azon halmazok metszeteinek méretét értem, amely a célpont és egy adott jelölt csomópontok üzeneteinek ID listájából áll.
- **Szűretlen üzenet ID alapú támadásfüggvény** esetén kizárólag a $IDL_{u_T}(t_0)$ és $IDL_u(t_1)$ metszetének mérete alapján választja ki a jelölt csomópontot
- **Kategória Hisztogram alapú támadásfüggvény** azt a u csomópontot választja ki, amelyik esetén a $CHM_u(t_1)$ leginkább hasonlít $CHM_{u_T}(t_0)$-re. Két hisztogram hasonlóságát a χ^2–teszt segítségével határozza meg a támadó.
- **Kiemelkedő Kategória alapú támadásfüggvény** arra épít, hogy azon kategóriákhoz, melyek a felhasználó érdeklődési körébe tartoznak, több üzenet tartozik (felül reprezentáltak), mint azokhoz, amelyek nem tartoznak az érdeklődési körébe (alul reprezentáltak). Az érdeklődési körbe tartozó kategóriák felfedéséhez két klaszterre bontja a támadó a C



5. ábra. **Analitikusan meghatározott felső becslés az ideális IP alapú támadó sikervalószínűségére**

kategóriát a k-átlag klaszterező algoritmust futtatva [Har75] a CHM-ek felett. A klaszterezés eredménye egy C hosszú bináris vektor, ahol 1-es áll ahol a kategória kiemelkedően sok üzenettel rendelkezik. Két bináris vektor hasonlóságát a vektorok Hamming távolsága határozza meg.

Még ha egy $\mathcal{A}_{IP\text{ ideal}}$ ideális IP alapú támadó meg tud különböztetni két csomópontot egymástól, ha különbözőek az IP-k, annak a valószínűsége, hogy két csomópontnak azonos az IP-je nem elhanyagolható. Az ideális IP alapú támadó sikervalószínűsége tekinthető egyfajta felső becslésnek minden IP alapú támadó (pl. Kiemelkedő Kategória alapú támadásfüggvény) sikervalószínűségére nézve. Ez az érték analitikus eszközökkel meghatározható.

Az ideális IP alapú támadó sikervalószínűsége meghatározható az azonos IP-k várható számával. A sikervalószínűség kiszámításához először két IP egyenlőségének valószínűségét számíthatjuk ki a következőképp:

$$\begin{aligned} p &= \frac{\sum_{w=1}^{C} \binom{C}{w} \left(\varepsilon^2\right)^w \left((1-\varepsilon)^2\right)^{C-w}}{\left(1-(1-\varepsilon)^C\right)^2} \\ &= \frac{\left(\varepsilon^2 + (1-\varepsilon)^2\right)^C - (1-\varepsilon)^{2C}}{\left(1-(1-\varepsilon)^C\right)^2} \end{aligned} \tag{8}$$

ahol w az IP súlya, ami 1 és C közötti értéket vehet fel (mivel minden résztvevő csomópontot legalább egy kategória érdekeli).

Az $\mathcal{A}_{IP\text{ ideal}}$ sikervalószínűsége reciproka az azonos IP-vel rendelkező csomópontok átlagos számával.

$$\begin{aligned} &\Pr(\mathcal{A}_{IP\text{ ideal}}(UP_{u_T}(t_0), UP_{u_1}(t_1), \ldots, UP_{u_N}(t_1)) = u_T) \\ &\simeq \frac{1}{1+p\,(N-1)} \end{aligned} \tag{9}$$

A fent bemutatott támadófüggvények hatékonyságának vizsgálatára különböző paraméterekkel (C és ε) szimulációkat is futtattam. A bemutatott eredményeket minden paraméterre 100 szimulációs futtatásból számítottam.

A 6. ábrán a $\lambda = 0$ eseteket elemezve látható különböző támadók sikervalószínűsége a vizsgált szcenáriókban, amikor nincs semmilyen védekezés. Ahogy az 5. ábra is mutatja az ideális IP alapú támadás sikeressége nagyban függ a kategóriák számától (C) és annak valószínűségétől, hogy egy csomópont érdeklődik egy adott kategóriához tartozó üzenetek iránt (ε). Ahogy az ábráról leolvasható a kategóriák nagy számával az ideális támadó sikeressége is nő. Azonban a kategóriák alacsony száma esetén a sikervalószínűség nagyban függ a ε értékétől. A ε minél közelebb van 0.5-höz, annál jobban nő a támadás sikerének valószínűsége. Mindez azzal magyarázható, hogy minél nagyobb teret engednek a rendszer paraméterei a változatosságnak, annál kisebb az esélye annak, hogy két csomópont azonos IP-vel rendelkezik.

2.2. TÉZIS:. *Javasolok egy általános védelmi mechanizmust a 2.1. tézisben leírt támadások ellen, amit Hide-and-lie-nak hívok. Szimuláció segítségével megmutatom, hogy a támadók sikervalószínűsége akár az egyszerű találgatás szintjére csökkenthető miközben a csomópontok goodputja nem változik lényegesen, sőt, néhány szcenárióban még növekedik is. [C6]*

A felhasználói profil módosításával a csomópontok félre tudják vezetni a támadókat. Az IP módosításán keresztül két egyszerű eljárás segítségével ez megtehető. Az egyik ilyen eljárás az érdeklődési körbe eső néhány kategóriát *elrejteni* (hide), amikor a csomópont azt állítja, hogy nem érdeklik azok az üzenetek. Valamint a másik ilyen eljárás, amit egy csomópont alkalmazni tud, azt *hazudni* (lie), hogy néhány érdektelen kategória számára érdekes. A két eljárás együttes alkalmazását nevezem *Hide-and-Lie Stratégiának* (HLS). Az átmenetileg módosított IP-t nevezem Átmeneti Érdeklődési Profilnak (EIP), vagy ugyanezt EIP-nek a támadó szempontjából. Ahogy a neve is mutatja a EIP átmeneti, és akár minden időszeletben újat lehet generálni.

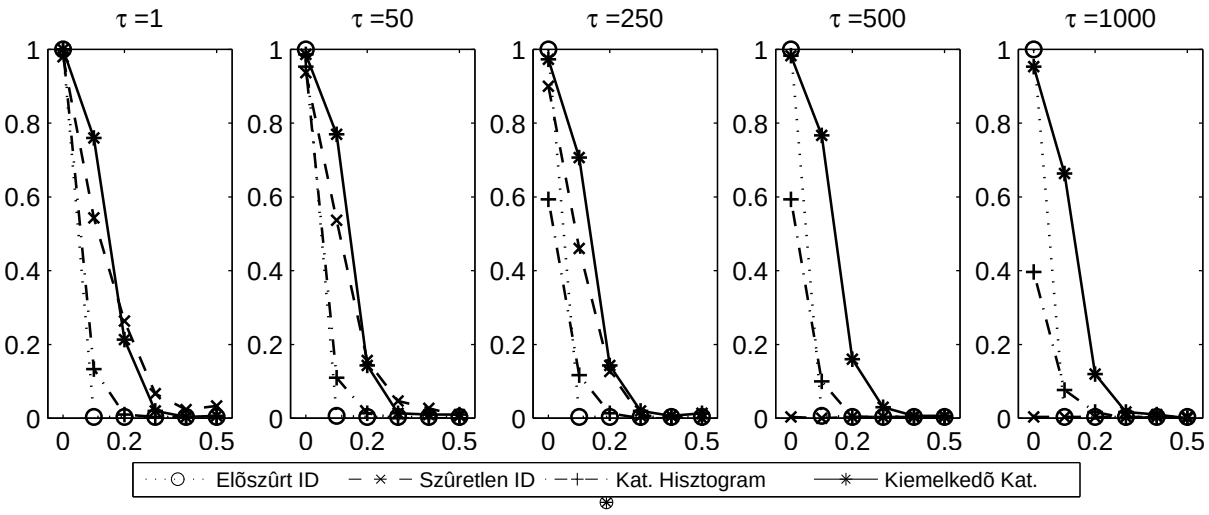
Természetesen, a letölteni kívánt és felajánlott üzeneteket az üzenetcsere folyamán szinkronizálni kell a EIP-vel: 1) az elrejtett kategóriákhoz tartozó üzeneteket is el kell rejteni, és nem szabad ilyen üzenetet letölteni sem a másik féltől, valamint 2) amikor egy csomópont azt hazudja egy kategóriáról, hogy érdekli, akkor az ahhoz tartozó üzeneteket fel is ajánlja és le is tölti a másik féltől.

A EIP az eredeti IP-ból generálható oly módon, hogy λ valószínűséggel invertálunk egy adott kategória iránt mutatott érdeklődést. Ezt azt jelenti, hogy olyan kategória iránt mutatunk érdeklődést, ami egyébként nem érdekelt és fordítva. A λ paraméter az ún. Hide-and-Lie stratégia érték.

A korábban vázolt támadófüggvények sikervalószínűségét ábrázolom a 6. ábrán különböző Hide-and-Lie stratégia értékek és különböző időpontokban elvégzett támadások függvényében. A könnyebb érthetőség kedvéért az utóbbi paraméter szerint különválasztottam az ábrákat.

Az Előszűrt üzenet ID alapú támadófüggvény a leghatékonyabb, amikor nincs védelmi mechanizmus $\lambda = 0$, ugyanakkor bármelyik másik esetben, a függvény képtelen különbséget tenni a célpont és a többi csomópont között, mivel már egy kategória megváltoztatása az EIP-ben félrevezeti a támadót. A Szűretlen üzenet ID alapú támadófüggvény sikervalószínűsége alacsonyabb ugyan $\lambda = 0$ esetén, viszont lényegesen jobb az előző támadófüggvényhez képest, amikor $\lambda > 0$. Ugyanakkor a Szűretlen üzenet ID alapú támadófüggvény nagyon érzékeny a támadás idejére. A Kategória Hisztogram alapú támadófüggvény kevésbé érzékeny erre, viszont ez nehezen tolerálja, hogy a EIP megváltoztatásával minden a változtatott kategóriához tartozó üzenet eltűnik vagy megjelenik a listában. A támadás idejére legkevésbé érzékeny algoritmus a Kiemelkedő Kategória alapú támadásfüggvény. Igaz, ez a függvény sem képes megkülönböztetni a csomópontokat, ha a $\lambda = 0.5$, mert ilyenkor nincsenek felül és alul reprezentált kategóriák.

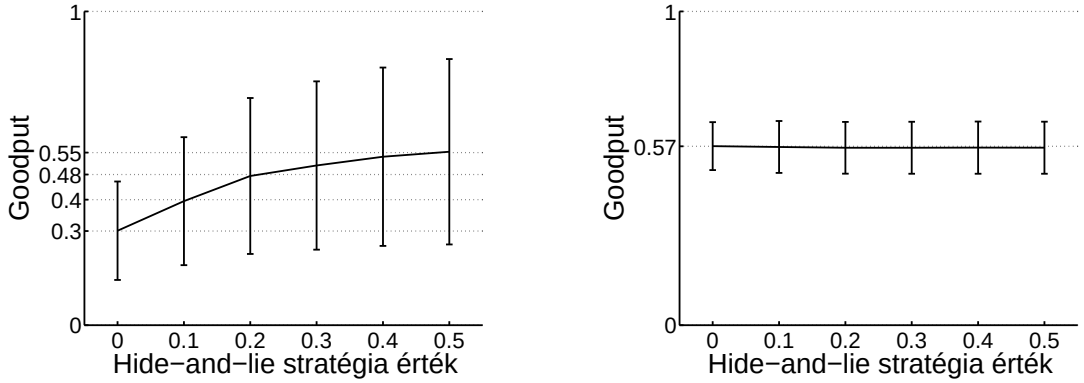
Mindegyik támadófüggvényről elmondható, hogy a csomópontok magas Hide-and-Lie stratégiával védekeznek a támadások ellen, egyik vizsgált támadófüggvény sem tudja megkülönböztetni



6. ábra. $\mathcal{A}$**-k sikervalószínűsége a Hide-and-Lie stratégia értékek** (λ) **függvényében**

a célpontot a többi csomóponttól jobban, mint a naiv támadó, aki csak véletlenszerűen választ ki egy csomópontot.

A védelmi mechanizmus hatását vizsgálandó, definiáltam a goodputot, hasonlóan, mint az 1. képletben az 1. téziscsoportban. A 7. ábrán az átlagos goodputot ábrázolom minden csomópontra nézve a Hide-and-lie stratégia függvényében két különböző szcenárióban. Az ábrán a tapasztalati szórást is feltüntettem. Fontos azonban kiemelni, hogy ez a két ábra nem reprezentatív, még ha az 7(a). ábrán egy érdekes hatás figyelhető is meg. Mégpedig a λ növelésével nem csökken, hanem nő a goodput. Ezzel szemben a 7(b). ábra azt mutatja, hogy a Hide-and-Lie stratégia megválasztásának nincs hatása az üzenetek kézbesítésére.



(a) 1. szcenário (b) 2. szcenário

7. ábra. **Átlagos goodput tapasztalati szórás feltüntetésével**

4.3. Gyors hitelesítési eljárások több operátor által üzemeltetett Vezetéknélküli Mesh Hálózatokban

3. TÉZISCSOPORT:. *Két tanúsítvány alapú hitelesítési és hozzáférés védelmi eljárást javasoltam több operátor által üzemeltetett Vezetéknélküli Mesh Hálózatok számára, ami olyan speciális követelményeket támaszt a hitelesítő protokollokkal szemben, amelyet a jelenlegi megoldások nem tudnak kielégíteni. A hitelesítés idejének csökkentésére egy ún. gyenge kulcsú eljárást javaslok korlátozott kapacitású eszközök számára. [C3] [J1] [J3] [B1]*

Ebben a téziscsoportban két tanúsítvány alapú hitelesítő protokollt javaslok Multi-WMN hálózatokban. Először is a tanúsítvány alapú hitelesítő protokoll architektúrája kerül bemutatásra. Utána néhány klasszikus kripto-primitív sebességét vizsgálom meg. Majd a nonce és időbélyeg alapú eljárás bemutatása után meghatározom, hogy milyen publikus kulcsú algoritmust mekkora kulcsmérettel érdemes használni azért, hogy teljesítsék az általános biztonsági követelményeket úgy, hogy közben biztosítva legyen a rövid hitelesítési késleltetés a hívásátadás során. A hitelesítés késleltetését valós környezetben is vizsgálom.

3.1. TÉZIS:. *Egy publikus kulcsú nonce alapú hitelesítő és hozzáférés védelmi eljárást javasoltam. Valós környezetben elvégzett mérések alapján megmutattam, hogy a hitelesítés késleltetése még a QoS érzékeny alkalmazások számára is tolerálható egy tipikus környezetben, ahol a mesh kliens erős számításkapacitással rendelkezik, míg az access point gyenge számításkapacitással. Informálisan azt is megmutattam, hogy az általam javasolt megoldás megfelel a több operátor által üzemeltetett Vezetéknélküli Mesh Hálózatok követelményeinek. [J3]*

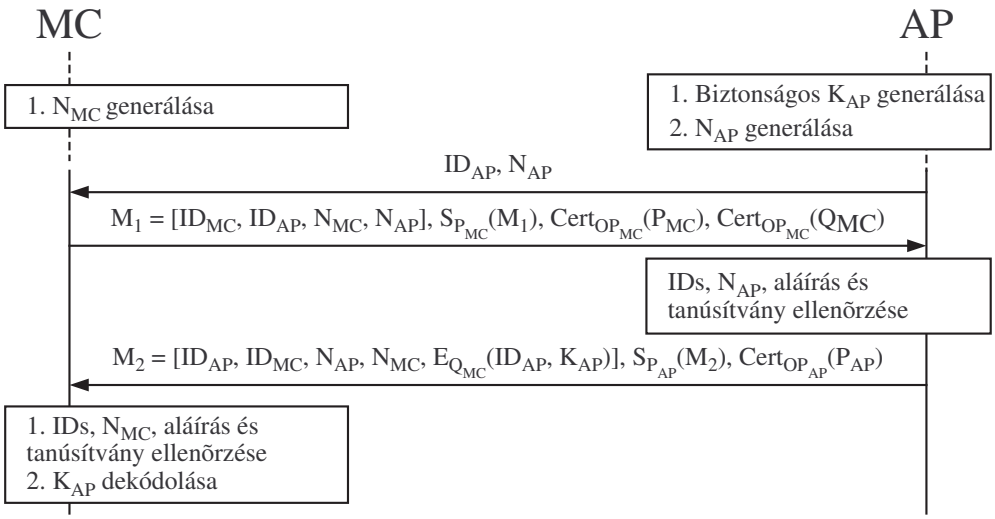
Az általam javasolt tanúsítvány alapú hitelesítési sémában mindegyik operátor saját tanúsítvány központot (CA) üzemeltetet. Ezek a CA-k felelnek azért, hogy tanúsítványt bocsássanak ki saját access point-jaik és előfizetőik számára. A CA feladata ezen kívül a visszavonási listák (CRL) karbantartása is.

Azon operátorok, akik együttműködnek (O_1 and O_2) ún. kereszt-tanúsítványt bocsátanak ki egymás CA-i számára. Ennek köszönhetően a résztvevők (előfizetők vagy access pointok) tanúsítvány alapú hitelesítést és kulcsmegegyezést tudnak végrehajtani akkor is, ha különböző operátorhoz tartoznak.

A 8. ábra azt mutatja be, hogy működik az általam javasolt nonce alapú hitelesítő eljárás. ID_X, N_X és K_X jelöli sorrendben X ID-ját, X által generált nonce-ot és X által generál kulcsot (X lehet AP vagy MC). $S_{P_X}(M)$ jelöli az M üzenet X privát kulcsával kiszámított digitális aláírását, és $E_{Q_X}(M)$ jelöli az X publikus kulcsával kódolt rejtjelezett M üzenetet. $Cert_{OP_X(P_X)}$ jelöli az X operátora által kibocsátott tanúsítványt, mely összerendeli X-et a publikus kulcsával.

A digitális aláírást és rejtelezést illetően érdemes minél több számításigényes műveletet az MC-re hárítani a következő okok miatt: 1) Általában azon MC-k, amelyek számára fontos a megszakításmentes hívásátadás, jóval nagyobb számítási kapacitással bírnak, mint az AP-k, mert fel vannak készítve mediafolyamok kezelésére is. Ezzel szemben az AP-k esetén fontos tervezési szempont, hogy olcsók legyenek, ezért azok számítási kapacitása korlátozott. 2) A DoS ellenállóság növelhető, amennyiben az MC végez több számítást, mivel egy támadónak több műveletet kell végrehajtania a sikeres támadáshoz.

Éppen ezért azt használtam ki, hogy némely publikus kulcsú művelet számításigénye aszimmetrikus. Amikor az MC rendelkezik nagyobb teljesítménnyel, mint az AP, az MC RSA-t használ digitális aláírás elvégzésére, míg, az AP DSA-t. Ezekben az esetekben az összes nagy számítás-



8. ábra. **Nonce alapú hitelesítési eljárás**

igényű feladatot (privátkulcsú művelet RSA esetén és digitális aláírás ellenőrzése DSA esetén) az MC végez el, míg a gyors műveleteket az AP.

A K_{AP} bizalmasságának fenntartása érdekében minimum 1024 bit hosszú RSA kulcs használatát javaslok. Mivel az MC publikus kulcsai hosszú életűek, ezért annak is 1024 bit hosszúnak kell lennie legalább. Az AP-k publikus kulcsait gyakran változtatják (pl. naponta), mégis 1024 bit hosszú kulcsot javaslok.

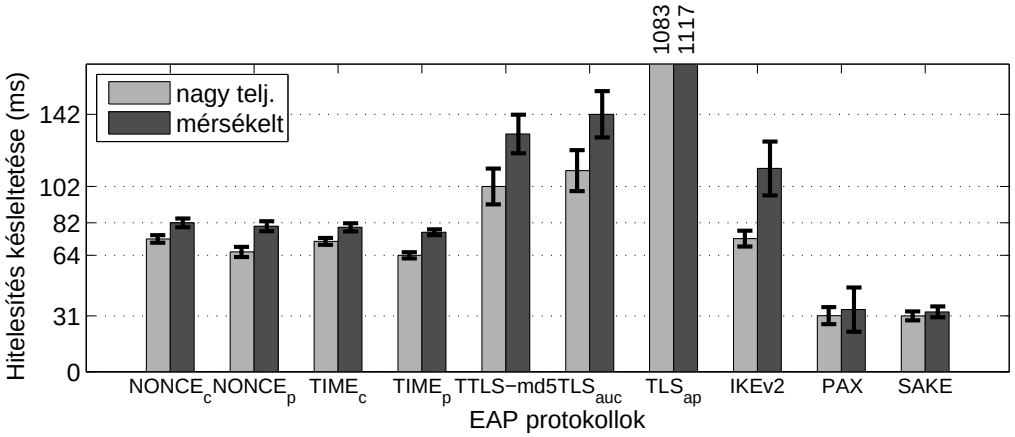
A vizsgálatokhoz elkészítettem egy proof-of-concept implementációt. A hitelesítési üzeneteket EAP (Extensible Authentication Protocol) formátumba ágyaztam [ABV+04]. Az EAP üzenetek EAPOL üzenetekbe vannak ágyazva, amelyet a IEEE 802.11i [IEE04] és a IEEE 802.11r [IEE08] (jelenlegi Wi-fi hitelesítést standardizáló dokumentumok) hivatkozó IEEE 802.1X [IEE01] definiál. Az IEEE 802.11i-ben definiált Pairwise Master Key, amely a hozzáférés-védelmet biztosítja, a következőképp számítódik: $K_{conn} = Hash(K_{AP}, N_{MC})$, ahol $Hash()$ egy egyirányú függvény.

A hitelesítés késleltetését különböző elrendezésekben vizsgáltam. Mindegyik esetben az AP egy MikroTik Routerboard 133 típusú eszköz volt 175 MHz MIPS32 processzorral. Annak vizsgálatára, hogy az MC teljesítménye miként befolyásolja a hitelesítés késleltetését három különböző MC-t használtam: 1) nagy teljesítményűt 1.86 GHz-es 32 bit-es processzorral, 2) mérsékelt teljesítményűt 800 MHz-es 32 bit-es processzorral és 3) alacsony teljesítményűt egy másik MikroTik routerrel.

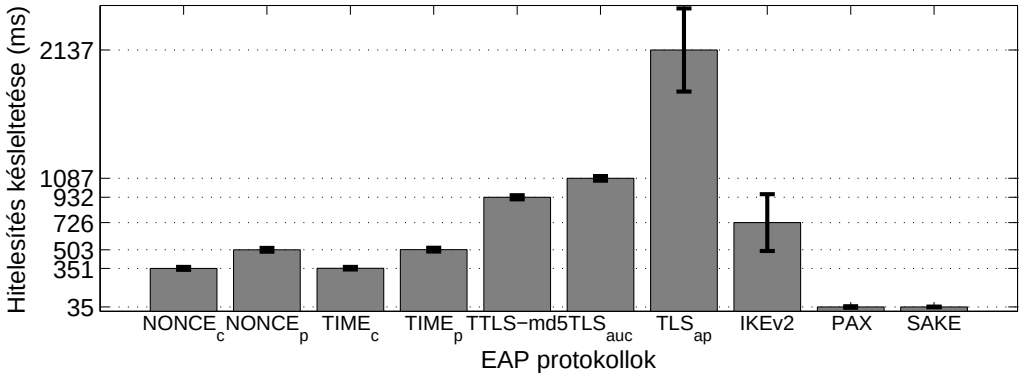
A saját megoldásomat jelenleg elterjed hitelesítő szervert (AP) igénylő megoldásokkal (pl. EAP-TLS, EAP-TTLS) hasonlítottam össze. Ezen esetek vizsgálatához, hostapd-t, mint különálló RADIUS szervert telepítettem egy nagy teljesítménnyel rendelkező PC-re. Ezekben az esetekben az AP-t közvetlen linkkel kapcsoltam össze az AS-sel így minimalizálva az AS és AP közötti kommunikáció késleltetését.

Összesen tíz külön hitelesítési eljárást három különböző teljesítményű MC eszközzel vizsgáltam. Minden mérést 100-szor végeztem el, és kiszámoltam a hitelesítés átlagos késleltetését, valamint a tapasztalati szórását. Az eredmények a 9. ábrán láthatóak. A horizontális tengelyen a különböző protokollokat tüntettem fel, míg a vertikális tengelyen a hitelesítés késleltetése olvasható le. Különböző elrendezések különböző színű oszlopokon jelennek meg.

Ahogy az leolvasható az ábráról a nonce alapú hitelesítési eljárás, amit NONCE_p-vel jelölök, nagy mértékben csökkentette a hitelesítés késleltetését összehasonlítva az ugyanolyan biztonságú publikus kulcsot használó központosított eljárásokkal (TTLS-md5, TLS_{auc} és IKEv2). Ezekben



(a) Nagy és mérsékelt teljesítményű MC



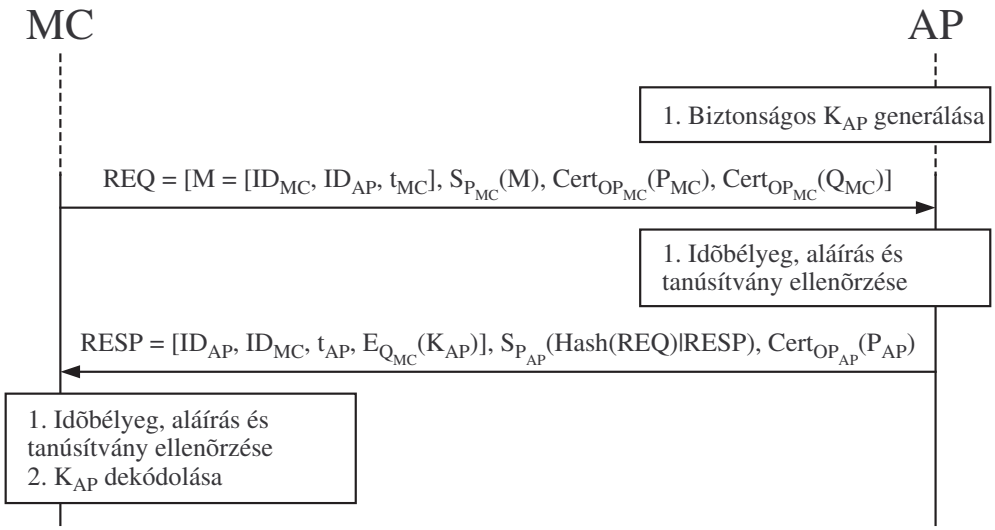
(b) Alacsony teljesítményű MC

9. ábra. **Hitelesítések átlagos késleltetései feltüntetve a tapasztali szórást**

az eljárásokban az AS egy nagy teljesítményű eszköz szemben az én megoldásommal, ahol az AP egy korlátozott számítási kapacitással bíró eszköz. Ráadásul abban az esetben (TLS_{ap}), amikor az AS ugyanolyan gyenge teljesítményű, mint az AP, a hitelesítés késleltetése egy nagyságrenddel nagyobb. A szimmetrikus kriptográfiát alkalmazó eljárások (PAX és SAKE) ugyan 30–40 ms alatt lefutottak (figyelmen kívül hagyva a kommunikációs késleltetést valós környezetben), azonban ezek a megoldások nem elégítik ki maradéktalanul a Multi-WMN követelményeit.

A megoldásom kielégít minden általános követelményt, amit a QoS-t biztosító Vezetéknélküli Mesh Hálózatok követelnek, amit a következő érvek támasztanak alá. Mind a mesh kliens, mind az access point ellenőrzi a másik fél hitelességét, valamint a protokoll mindkét fél számára biztosít implicit kulcshitelességet és kulcsfrissességet. A megoldás DoS ellenálló, mivel nincs egy központi elem, aminek megtámadása a teljes hálózat lassulásához vagy lebénulásához vezetne. Ahogy az eredmények mutatják, a javasolt protokollban sikerült annyira lecsökkenteni a hitelesítés késleltetését, hogy a megszakításmentes hívásátadás lehetségessé váljon annak ellenére, hogy a megoldás publikus kulcsú kriptográfiára épít .

Ugyanakkor a megoldás olyan követelményeknek is megfelel, amit az követel meg, hogy több operátor üzemelteti a hálózatot. Nincs olyan kiemelt entitás, amiben mindegyik operátoroknak meg kell bíznia. A kapcsolat kulcsok nem fednek fel hosszabb távú kulcsokat, és függetlenek korábbi és későbbi kulcsoktól egyaránt. Ezeknek a tulajdonságoknak köszönhetően az operátorok megvédik magukat és előfizetőiket a rosszul beállított access pointok okozta sérülékenységektől, legalábbis korlátozzák a hiba terjedését.



10. ábra. **Időpecsét alapú hitelesítő eljárás**

Az EAP standardnak megfelelően implementáltam a megoldást, amely megfelel az IEEE 802.11i és a IEEE 802.11r követelményeinek. Éppen ezért a hitelesítő eljárás használható inter- és intra-domain hívásátadásra is.

3.2. TÉZIS:. *Egy publikus kulcsú időpecsét alapú hitelesítő és hozzáférés védelmi eljárást javasoltam. Valós környezetben elvégzett mérések alapján megmutattam, hogy a hitelesítés késleltetése még a QoS érzékeny alkalmazások számára is tolerálható egy tipikus környezetben, ahol a mesh kliens erős számításkapacitással rendelkezik, míg az access point gyenge számításkapacitással. Informálisan azt is megmutattam, hogy az általam javasolt megoldás megfelel a több operátor által üzemeltetett Vezetéknélküli Mesh Hálózatok követelményeinek. [C3] [J3]*

Általánosan elmondható, hogy az időpecsét alapú eljárások a nonce alapú eljárásokkal szemben kevesebb véletlen számot igényelnek, és a kölcsönös hitelesítés két üzenet segítségével is elvégezhető szemben a nonce három üzenetével. Viszont az időpecsét alapú eljárások megkövetelik az órák szinkronizáltságát. Ugyanakkor a tanúsítvány alapú eljárások eleve megkövetelik ezt, ezért nem kell újabb követelményt teljesíteni.

A javasolt időpecsét alapú hitelesítő séma a 10. ábrán kerül bemutatásra. A jelölések azonosak a 8. ábrán ismertetettekkel. Az egyetlen új jelölés csupán a t_X, ami az X által küldött időpecsétet jelöli (továbbra is X lehet AP vagy MC). A Pariwise Master Key úgy számítódik, hogy $Hash(K_{AP}, t_{MC})$.

Mind az architektúra, mind az aszimmetrikus kriptográfiai primitívek használata megegyezik a nonce alapú eljárásnál bemutatottakkal. Éppen ezért a 3.1 tézisben tett állítások érvényesek erre a tézisre is. A 9. ábrán TIME_p-vel jelöltem az időpecsét alapú eljárást. A késleltetés is nagyon hasonló a nonce alapú hitelesítő eljárásához.

3.3. TÉZIS:. *Javasoltam a 3.1 és 3.2 tézisben már ismertetett protokollok egy variánsát, hogy a korlátozott mesh kliensek rövidebb (gyenge) kulcsot használhassanak. Megmutattam, hogy 30%-os késleltetés csökkentés érhető el korlátozott mesh kliens esetén. Azt is megmutattam, hogy a gyenge kulcsú eljárás akkor nyereséges, amikor a publikus kulcsú műveletek gyorsítása nagyobb mértékű, mint a hosszabb tanúsítvány lánc ellenőrzése okozta többlet. [C3] [J3]*

Mivel a gyengébb teljesítményű MC nem képes végrehajtani az összes nagy számítási kapacitást igénylő műveletet úgy, hogy ne okozzon tolerálhatatlan késleltetést, egy újfajta eljárást vezettem be a késleltetés csökkentésére annak árán, hogy mindkét félnek előszámításokat kell végezni a hívásátadás előtt.

A gyorsítás arra épül, hogy rövidebb kulcsokkal a digitális aláírás gyorsabban elvégezhető. Mivel a rövidebb kulcsok gyengébbek, ezért az ezekhez tartozó tanúsítványok élettartama is rendkívül rövid, olyannyira, hogy biztosan lejárnak mielőtt valaki feltörné azokat.

A gyenge kulcsokat és a hozzá tartozó tanúsítványokat a résztvevők generálják a hívásatadást megelőzően. Lényegében az MC-k és AP-k maguk bocsátják ki a tanúsítványokat. Először generálnak egy gyenge kulcspárt, majd a saját ID-jüket a tanúsítvány neveként beállítják, valamint meghatározzák a tanúsítvány lejárati idejét. Végül ellátják a tanúsítványt digitális aláírással, amelyet egy olyan privát kulccsal generálnak, amihez tartozó tanúsítványt a operátor adott ki gyenge kulcsok aláírására. Éppen ezért bárki, aki ismeri a CA publikus kulcsát ellenőrzni tudja a gyenge kulcs hitelességét.

Mivel a tanúsítványok rendkívül rövid életűek, nem szükséges hozzá CRL-t fenntartani. A gyenge kulcsok tanúsítványát RSA-val generált digitális aláírással látják el, ezért annak ellenőrzése rendkívül gyorsan végrehajtható.

512 bites kulcsot javasolok rövid kulcsok használatára, amely a legjobb kompromisszumot jelenti manapság az érvényességi idő és számítási igény tekintetében. Hasonlóan a korábbi esetekhez, az MC RSA-t az AP DSA-t használ digitális aláírás generálására.

Fontos megjegyezni, hogy az időszinkronizálást biztonságos módon kell elvégezni, különben egy támadó el tudja érni, hogy az MC vagy az AP egy már korábban feltört kulcshoz tartozó tanúsítványt érvényesnek fogadjon el. Az biztonságos időszinkronizálás további vizsgálatától eltekintek.

Ahogy a 9(b). ábráról leolvasható, a gyenge kulcsú eljárás (NONCE_c-ként és TIME_c-ként jelölve sorrendben a nonce és időpecsét alapú hitelesítő eljárásokat) szignifikáns javulást mutat alacsony teljesítményű MC esetén a nagyobb teljesítményű MC-kre tervezett metódushoz képest. Átlagosan körülbelül 30%-os javulást lehetett elérni a vizsgált eszközökön. Ugyanakkor a 9(a). ábra azt mutatja, hogy nagyobb teljesítményű MC esetén nem hogy nem csökkent, hanem nőtt a késleltetés.

A késleltetés növekedésének megértésére, részletesen megvizsgáltam, a gyenge kulcsú eljárás hatását. A digitális aláírás generálásának (Δt_{gen}) és ellenőrzésének (Δt_{verif}) gyorsításából mindkét fél hasznot húz, ugyanakkor a tanúsítvány lánc meghosszabodása (t_{cert}) és a többlet adat továbbítása (t_{trav}) mindkét fél számára késleltetést okoz.

Mindezt egybe vetve általánosan elmondható, hogy a gyenge kulcs használata előnyös az egyik fél számára amennyiben a 10. képlet igaz rá.

$$t_{cert}^{(B)} + t_{trav} < \Delta t_{gen}^{(A)} + \Delta t_{verif}^{(B)} \tag{10}$$

ahol A a felső indexben jelöli annak a félnek okozott időkülönbséget, amely a tanúsítványt generálta, és B jelöli a másik felet. Δt_{op} jelöli az op (lehet gen vagy $verif$) művelet hosszú távú kulccsal ($t_{op}(S)$) és gyenge kulccsal ($t_{op}(w)$) végzett késleltetés különbségét, amint a 11. képlet mutatja.

$$\Delta t_{op} = t_{op}(S) - t_{op}(w) \tag{11}$$

4.4. Szabálytalanul viselkedő routerek azonosítása Link-state routing esetén Vezetéknélküli Mesh Hálózatokban

4. TÉZISCSOPORT:. *Egy újfajta hírnév alapú rendszert mutatok be szabálytalanul viselkedő routerek azonosítására és elkerülésére Link-state útvonalválasztás esetén Vezetéknélkül Mesh Hálózatokban. [C1]*

Egy olyan eljárást javasolok, amelyik azonosítja a szabálytalanul viselkedő routereket az adatok továbbítása során, és visszajelzést ad a kontrol felület számára, hogy ezek a routerek már az útvonalak felépítése során elkerülhetők legyenek.

A javasolt szabálytalanul viselkedő router azonosító eljárás három fázisból áll. Az első fázis során, amelyet *forgalom vizsgálat*nak nevezek, minden gateway, amelyek feltételezésem szerint jobban védettek, mint az egyszerű routerek, éppen ezért jól viselkednek, információt gyűjt a hozzá tartozó útvonalakban résztvevő routerek viselkedéséről. A második fázisban, melynek neve *router értékelés*, a gateway-ek azonosítják a gyanúsan viselkedő routereket az előző fázisban begyűjtött információ alapján. Ennek eredményeképp a gateway-ek minden routerhez egy ún. Node Trust Value-t számítanak, amit a hálózatban közzétesznek. Végül, a harmadik fázisban, melynek neve *reakció*, az access pointok új utakat választanak figyelembe véve a routerek Node Trust Value értékeit.

4.1. TÉZIS:. *Egy újfajta hírnév alapú rendszert javasolok szabálytalanul viselkedő routerek azonosítására és elkerülésére Link-state útvonalválasztás esetén Vezetéknélkül Mesh Hálózatokban. A routerek hírneve számlálók alapján kerülnek számításra. Mindegyik router egy számlálót tart fenn minden egyes adatfolyam számára, és azt számolja, hogy mennyi üzenetet továbbított az adott folyamban. A számlálók értékét elküldik az adatfolyam egyik végét jelentő gatewaynek. A gateway kiszámolja az adatfolyamban szereplő minden egyes router hírnév értékét, amelyet Node Trust Value-nak nevezek, úgy, hogy azzal is számol, hogy a szabálytalanul viselkedő routerek hamis értéket is küldhetnek. Szimuláció segítségével megmutatom, hogy a fent leírt eljárás segítségével a szabálytalanul viselkedő routerek megkülönböztethetőek a jól viselkedőektől. [C1]*

A forgalom elemzése érdekében a javasolt eljárás azt követeli meg a csomópontoktól, hogy egy-egy számláló segítségével kövessék mindegy egyes adatfolyamhoz tartozó továbbított csomagok számát. Azt feltételezem, hogy minden egyes adatcsomag fejléce tartalmaz egy azonosítót, ami meghatározza, hogy mely adatfolyamhoz tartozik a csomag, valamint egy hitelesítő kódot, ami által a routerek kizárólag a sértetlen és hitelesített csomagokat számolják. A számlálók értékeit a gateway bizonyos időközönként leolvassa.

Mivel a szabálytalanul viselkedő routerek hamis számláló értéket is küldhetnek, a gateway nem közvetlenül a számlálók értékeiből számolja a Node Trust Value-t. Ehelyett, a gateway különböző magyarázatokkal írja le a kapott értékeket. Minden magyarázatban a routerek gyanúsítottak vagy ártatlanok lehetnek, ezáltal a magyarázatok felírhatók bináris vektorként. Egy adott router Node Trust Value-ja a különböző magyarázatok gyanúsításainak súlyozott összege. Minél kevesebb gyanúsítás routert tartalmaz egy magyarázat annál nagyobb súllyal bír. Az egyszerűség kedvéért, feltételezem, hogy a routerek közötti kapcsolat jó minőségű, ezért a csomagok elvesztését kizárólag a routerek szabálytalan viselkedése okozhatja.

A cnt^i számláló reprezentálja az i. routeren egyik irányba áthaladó forgalmát. Azonban a szabálytalanul viselkedő routerek nem feltétlenül jól állítják be ezeket az értékeket. Tekintsük a következő egyszerű példát, ahol egy szabálytalanul viselkedő router két jó router között található. A szabálytalan router beállíthatja számláló értékét a bejövő csomagok számának (cnt^i_{in}) megfelelően ($cnt^i = cnt^i_{in}$). Ebben az esetben a gateway azt olvassa ki a kapott számokból, hogy a szabálytalan router előtti linken nincs adatvesztés, mivel $cnt^i = cnt^{i-1}$. Viszont a következő linken a különbség $cnt^{i+1} - cnt^i$. Ezen információk alapján lehetetlen megkülönböztetni, hogy az i. router valójában továbbította-e az üzenetet és az $i+1$. router dobta el vagy pedig az i. dobta el azokat és az $i+1$. már csak cnt^{i+1} csomagot kapott. Hasonlóan, több magyarázat van arra az esetre is, ha a támadó a küldött számlálót a kimenő csomagok számának (cnt^i_{out}) megfelelően állítja be ($cnt^i = outcounter^i$).

A támadó modellnek megfelelően, a szabálytalan router ξ valószínűséggel küldi a gateway-nek a bejövő csomagok számát, és $1-\xi$ valószínűséggel a kimenő csomagok számát. Olyan szélsőséges eseteket is vizsgálok, amikor a $\xi = 0$ és $\xi = 1$.

A $\overline{exp}$ magyarázat egy olyan vektor, ahol az i. elem akkor 0, ha a router gyanúsított, azaz szabálytalanul viselkedőnek jelölt, egyébként az i. elem 1. Egy magyarázat akkor érvényes, ha az alábbi állítások igazak rá:

- Ha van elveszett csomag az i. és $i+1$. csomópont között, legalább az egyiknek gyanúsítottnak kell lennie.
- Ha az i. és j. csomópont egyike sem gyanúsított, és nincs csomagvesztés közöttük, akkor semelyik másik, közöttük lévő router nem lehet gyanúsított.

Minden magyarázathoz tarozik egy súly. Kétféle súlyozást vizsgáltam, mindegyik esetben a súly értéke a gyanúsított routerek számától függ. Legyen a gyanúsított routerek száma az $\overline{exp}$ magyarázatban $|\overline{exp}|$, valamint ezen az útvonalon résztvevő routerek száma $||\overline{exp}||$. A két különböző súlyozó függvényt ($w_1()$ és $w_2()$) sorrendben a 12. és 13. képlet definiálja.

$$w_1(\overline{exp}) = q^{|\overline{exp}|} \cdot (1-q)^{||\overline{exp}||-|\overline{exp}|}, 0 < q \leq 1 \tag{12}$$

$$w_2(\overline{exp}) = \begin{cases} 1 & \text{if } |\overline{exp}| = \min_{\forall \overline{exp}_f}(|\overline{exp}_f|) \\ 0 & \text{else} \end{cases} \tag{13}$$

A 13. képlet esetén csak azokkal a magyarázatokkal kell számolni, ahol a gyanúsítottak száma minimális.

Adott számláló sorozat esetén $\overline{exp}_e$ magyarázatok halmazát a g gateway, amely az adott útvonal végén található t időpontban a következőképp használja fel az i. router Node Trust Value értékének ($\eta^{r(t)}_{i,g}$) meghatározására:

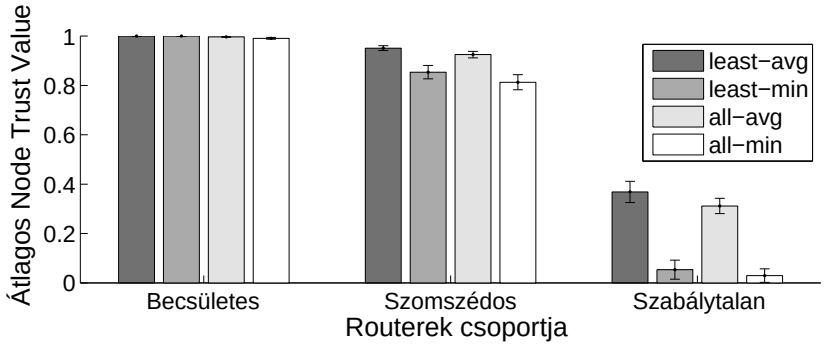
$$\eta^{r(t)}_{i,g} = \sum_{\forall \overline{exp}_e} \frac{w(|\overline{exp}_e|)}{\sum_{\forall \overline{exp}_f} w(|\overline{exp}_f|)} \cdot \overline{exp}_e(i) \tag{14}$$

ahol minden egyes $\overline{exp}_e(i)$ magyarázat súlyozásra kerül a korábban ismertetett súlyozó függvények valamelyikének normalizált értékével. A $\eta^{r(t)}_{i,g}$ értéke mindig a $[0,1]$ intervallumba esik.

A megoldás hatékonyságának vizsgálatára szimulációkat futtattam 200 mesh csomópont egyenletesen véletlenszerű elhelyezésével egy két dimenziós területen. A mesh csomópontok egy részhalmaz gateway, egy másik részhalmaza szabálytalanul viselkedő router lett.

A 11. ábrán a routerek átlagos Node Trust Value-ja látható három különböző csoportba rendezve 95 %-os konfidencia intervallummal. A három különböző csoport a 1) szabálytalan routerek, 2) szabálytalan routerek szomszédságában lévő, jól működő routerek, és 3) többi jól

működő router. Az utóbbi két csoportot külön kezelem, mivel a szabálytalan routerek a megoldás sajátosságai miatt lecsökkenthetik a szomszédos jól működő routerek Node Trust Value értékét. Minden csoportnál négy oszlop látható. Minden egyes oszlop a megoldás valamely beállításának felel meg. A `all` és a `least` sorrendben a 12 és a 13. képletben definiált súlyozó függvény használatát jelzi. A `min` és a `avg` aggregáló függvényeket reprezentálnak, melyeket részletesebben a 4.2 tézisben részletezek.



11. ábra. **Routerek csoportosított átlagos Node Trust Value értékei 95 %-os konfidencia intervallummal**

Ahogy a 11. ábrán látszik a jól működő routerek Node Trust Value-ja maximális. Ezzel szemben a szabálytalan routerek értékei szignifikánsan alacsonyabbak. A szabálytalan routerek szomszédainak Node Trust Value értéke ugyan magas, de ahogy várni lehetett, lényegesen alacsonyabb, mint a többi jól működő routernek. Mindez azt jelenti, hogy az útvonalválasztó eljárások meg tudják különböztetni a szabálytalan routereket nagy valószínűséggel a jól működőektől.

4.2. TÉZIS:. *Egy olyan eljárást javasoltam, amiben a routereket a 4.1. tézisben ismertetett Node Trust Value-val arányos valószínűséggel veszik figyelembe az útvonalválasztás során. Szimuláció segítségével megmutattam, hogy a szabálytalanul viselkedő routerek azonosítás és az útvonalválasztó algoritmusoknak köszönhetően az eldobott csomagok átlagos száma 50 %-kal csökkent, miközben az útvonalak hossza csak minimálisan nőtt. [C1]*

Mivel a gateway-ek a routereket több útvonalon is értékelhetik, valamint az access pointok is több gatewaytől kaphatnak Node Trust Value-t, ezért valamilyen módon ezeket az értékeket aggregálni kell.

Mindegyik $\eta_{i,g}^{r(t)}$ egy n hosszú ablakon keresztül kerülnek felhasználásra. Ezek az értékek érkezhetnek különböző útvonalakról (r_k), vagy azonos útvonalról, de más időben (t_l). Kétféle konkrét aggregáló f függvényt vizsgálok: minimum és átlag.

$$\eta_{i,g}^{(gw)} = f(\eta_{i,g}^{r_1(t_1)}, \eta_{i,g}^{r_2(t_2)}, \ldots, \eta_{i,g}^{r_n(t_n)}) \tag{15}$$

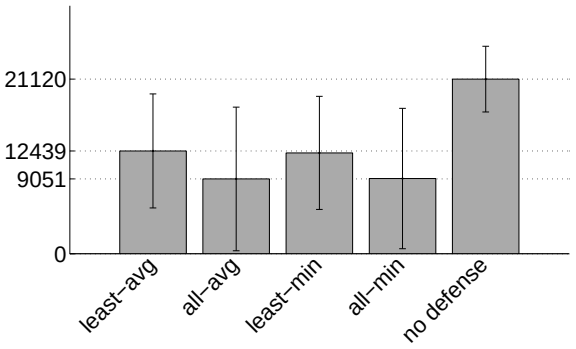
Az a access point minden g_k gatewaytől csak az utolsó $\eta_{i,g_k}^{(gw)}$ értéket veszi figyelembe. A Node Trust Value, amit végül az access point kiszámol ($\eta_{a,i}^{(ap)}$) és az útvonalválasztás során felhasznál szintén az f függvény segítségével kerül kiszámításra:

$$\eta_{a,i}^{(ap)} = f(\eta_{i,g_1}^{(gw)}, \eta_{i,g_2}^{(gw)}, \ldots, \eta_{i,g_m}^{(gw)}) \tag{16}$$

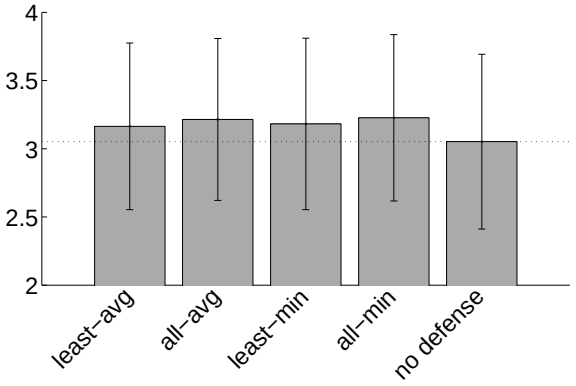
ahol m azon gateway-ek száma, amelyektől az access point az i routerről értékelést kapott.

Az útvonalválasztás során az access point meghatároz egy ún. résztérképet, amin az útvonalválasztó protokoll lefut. Az i access point a j routert $\eta_{i,j}^{(ap)}$ valószínűséggel hagyja benne a résztérképben.

Azonban ezzel a hozzáállással a résztérkép lehet, hogy nem összekötött, ezért ez nem garantálja, hogy az access point talál útvonalat a gateway-hez. Amikor ez a helyzet áll elő, egy új résztérképet kell generálni. Azért, hogy biztosítva legyen, hogy az eljárás belátható időn belül véget érjen, egy küszöbértéket definiáltam, amely kezdetben 1, és minden sikertelen résztérkép generálása után csökken ν-val. Minden i router, amelyre igaz, hogy $\eta_{a,i}^{(ap)} > 1 - r \cdot \nu$, bekerül a résztérképbe (r a sikertelen próbálkozások száma).



12. ábra. **Eldobott csomagok átlagos száma 95 %-os konfidencia intervallummal**



13. ábra. **Az útvonalak átlagos hossz 95 %-os konfidencia intervallummal**

A 12. ábrán az eldobott csomagok átlagos száma látható (95 %-os konfidencia intervallumot feltüntetve) szabálytalan routert azonosító eljárás különböző paraméterei szerint csoportosítva. Ezeket az eredmények ahhoz az esethez hasonlítom, amikor nincs védelem. Ahogy az ábráról leolvasható az eldobott csomagok száma jelentősen csökkent a javasolt eljárásnak köszönhetően.

A vizsgált QoS érték az útvonalak hop száma volt. A 13. ábrán a kiválasztott útvonalak átlagos hop száma látható 95 %-os konfidencia intervallummal. Ahogy látható, az útvonalak hossza nem növekedett szignifikánsan a fent leírt eljárással. Ez annak köszönhető, hogy sok esetben az access pointok hasonló hosszúságú, de szabálytalan routereket elkerülő útvonalakat tudtak választani.

5. Az eredmények alkalmazása

Ebben a tézisfüzetben, két különböző többugrásos vezetéknélküli hálózat adattovábbítás biztonsági kérdéseivel foglalkozom: 1) Késleltetés Tűrő Hálózatok és 2) Vezetéknélküli Mesh Hálózatok. Mindkét esetben különböző problémákat vizsgáltam. Ebben a fejezetben leírom, hogy miként lehet az új eredményeket felhasználni.

A Késleltetés Tűrő Hálózatokat illetően egy olyan alkalmazási környezetet képzeltem el, ahol helyhez köthető információt kell továbbítani közeli célpontokhoz érdeklődésüknek megfelelően. Ezen hálózatok tipikusan kisméretű mobil eszközökből állnak, melyek mobil felhasználókhoz tartoznak.

Turisták közötti információ cserére, ahelyett, hogy egy on-line hirdetőtáblát állítanánk fel, ahol a turistáknak nemcsak a szolgáltatásért, hanem a hálózat hozzáférésért is fizetni kell, egy város méretű Késleltetés Tűrő Hálózat nagyon olcsó megoldást tud kínálni. Ebben a megoldásban

az információt a store-carry-and-forward elvnek megfelelően Bluetooth-t használó eszközök (pl., mobil telefon, PDA) segítségével lehet terjeszteni kihasználva a turisták mobilitását.

Autós Ad hoc Hálózatokban (Vehicular Ad hoc Networks — VANET), az autók egymással kommunikálnak, hogy 1) ezáltal nagyobb biztonságot és magasabb átbocsátó-képességet biztosítsanak a forgalom számára és 2) szórakoztassák az utasokat. A VANET hálózatok speciális követelményeinek kielégítésére a jelenlegi tervezési elveknek megfelelően útmenti infrastruktúra telepítésére van szükség. Azonban a telepítés magas költsége miatt bizonyos területeken az autók DTN segítségével tudnak kommunikálni egymással. A második célt illetően valószínűleg nem éri meg külön infrastruktúrát kiépíteni a szórakoztatás számára, viszont a DTN továbbra is egy megfelelő kommunikációs módot jelenthet.

Egy tipikus DTN hálózatban, mint amiket előbb bemutattam, az infrastruktúra hiánya miatt a végfelhasználók felelőssége az adattovábbítás. Éppen ezért, a DTN hálózatok, szemben az infrastruktúra alapú hálózatokkal, olcsó, de nem megbízható adattovábbítást tudnak csak biztosítani. A megbízhatóság azonban növelhető, amennyiben sikerül a felhasználókat motiválni egymás üzeneteinek továbbítására. Egy szélsőséges példát tekintve, amikor senki sem hajlandó mások részére üzenetet továbbítani, az üzenetek csak akkor érnek célba, ha a forrás és a célpont közvetlenül találkoznak egymással. A fenti példákat tekintve ez azt jelentené, hogy 1) a turisták csak akkor tudják meg, hogy zárva van egy múzeum, amikor már ott vannak a múzeumnál, vagy 2) egy sofőr akkor értesül egy balesetről, amikor már közel van hozzá, nem pedig akkor, amikor még könnyen elkerülhetné azt egy másik útvonalon. A barter alapú megoldás arra ösztönzi a felhasználókat, hogy mások számára is továbbítsanak üzenet, mintegy helyettesíthetővé téve az infrastruktúrát a DTN-nel.

A követhetőség szintén egy vizsgálandó probléma a DTN hálózatokban. Mivel a felhasználók tárolják és továbbítják az üzeneteket miközben mozognak, követhetővé válhatnak, amennyiben a továbbító protokollt nem kellő körültekintéssel tervezik meg. A turista példánál maradva, célzott hirdetésekkel lehetne bombázni a turistákat az alapján az információ alapján, hogy merre jártak. Természetesen a VANET hálózatokban is visszaélésre adhat lehetőséget a privacy megsértése. Anonim kommunikáció lehetőségét már korábban is vizsgálták mobil ad hoc hálózatokban. Azonban adódik egy DTN specifikus probléma is a store-carry-and-forward elv alkalmazása miatt. Konkrétan a felhasználókról profilt lehet felépíteni az alapján az információ alapján, hogy mit osztanak meg és milyen adathoz akarnak hozzájutni. A Hide-and-Lie éppen az ilyen támadások ellen került kifejlesztésre.

A barter és a Hide-and-Lie javaslatokat és azok vizsgálatait a BIONETS (BIOlogically inspired NETwork and Services) EU-s projekt számára készítettem. Az FP6 project célja egy olyan infrastruktúra nélküli hálózat kifejlesztése, amelyben az evolúciós szolgáltatások automatikusan idomulnak a felhasználók igényeihez. A projekt 2006-ban kezdődött és 2010. februárjában ért sikeresen véget. További információ megtalálható a `http://www.bionets.eu` honlapon.

Mind a barter, mind a Hide-and-Lie eljárások megjelentek, mint BIONETS technikai riport. Ráadásul a barter eljárás integrálásra került a BIONETS szimulátorban. A BIONETS simulator egy OMNeT++ [BV11] alapú szimulátor, amelyen keresztül a projekt eredményei kerültek bemutatásra integrált módon.

A Vezetéknélküli Mesh Hálózatok szélessávú hozzáférést biztosítanak mobil felhasználók számára, akik akár QoS érzékeny alkalmazásokat is futtathatnak. Ezen hálózatok üzemeltetését különálló operátorok együttesen is végezhetik, ami akkor is előnyös lehet mindenki számára, ha közben egymás konkurrensei. Ezen kívül a több csatornás hozzáférés kezelése több interfészen keresztül nagy haszonnal járhat az operátorok számára.

Az újfajta, gyors, tanúsítvány alapú hitelesítési eljárást, melyet több operátor által üzemeltetett Vezetéknélküli Mesh Hálózatok számára javasoltam, mobil üzleti felhasználók tudják leginkább kihasználni, akik üzleti útjuk során üzleti szolgáltatásokhoz és valós idejű multimédia

alkalmazásokhoz kívánnak hozzáférni. Az alkalmazottak hatékonysága tovább növelhető, ha a hálózati hozzáférés olyan olcsó, mint amit a Vezetéknélküli Mesh Hálózatok ma ígérnek. Azonban az üzleti felhasználók elvárják, hogy a 3G-vel azonos minőségű kapcsolattal rendelkezzenek. Ezért a felhasználói újra-hitelesítés az új access pointoknál rendkívül fontos, azonban ez tolerálhatatlan késleltetést is okozhat. Kiváltképp akkor, amikor az access point, ahova a felhasználó csatlakozik más operátor által üzemeltetett, mint az elhagyott access point.

A tanúsítvány alapú gyors hitelesítést kiegészítettem egy ún. gyenge kulcsú eljárással. Ez az eljárás minden olyan környezetben felhasználható, ahol a digitális aláírás késleltetése kritikus, azonban csak az üzenetek hitelességét kell igazolni, a letagadhatatlanságot nem. Egy konkrét esetben ez az eljárás alkalmazásra került egy olyan környezetben, ahol a hálózatban elárasztásra került üzeneteket digitális aláírással látták el. A digitális aláírás generálásának és ellenőrzésének gyorsítását a gyenge kulcsú eljárás segítségével oldották meg.

A tanúsítvány alapú hitelesítés és a gyenge kulcsú eljárást valós környezetben vizsgáltam. A hostapd és a wpa_supplicant [Mal09] implementáció segítségével ágyaztam EAP formátumba a hitelesítés üzeneteit. Ezért IEEE 802.11 vezetéknélküli hálózatokban kisebb fejlesztések után az implementáció felhasználható.

Link-state útvonalválasztó protokollok számára fejlesztettem egy szabálytalanul viselkedő routerek azonosítására és elkerülésére alkalmas eljárást. A fő előnye a jelenlegi megoldásokkal szemben, hogy az eljárás nem igényli szomszédos routerek megfigyelését, amelynek hatékonysága megkérdőjelezhető többcsatornás rendszerekben. Az eljárás OLSRd [ols10] környezetben is implementálásra került.

A szabálytalanul viselkedő routerek azonosítása hasznos lehet pl. video megfigyelő rendszerekben. Társasházakban előfordulhat, hogy a video megfigyelő rendszert telepítenek az illegális cselekedet észlelésére. Köszönhetően a Vezetéknélküli Mesh Hálózatok alacsony telepítési költségeinek, a tulajdonosok úgy dönthetnek, hogy a kamerák képeit a monitor szobába vezetéknélküli kapcsolatokon keresztül továbbítják. Azonban a mesh routerek viselkedését egy külső támadó módosíthatja, mivel azok általában fizikailag nem védettek. Egy támadó, aki átveszi az irányítást egy csomópont felett, el tudja érni a útvonalválasztást segítő kontroll üzenetek módosításával, hogy a kamerák képei rajta keresztül menjenek a monitor szobába. Ezek után a támadó már könnyen megakadályozhatja a képek sikeres célbaérését. Egy ilyen sikeres támadás alatt bármilyen illegális cselekedet végrehajtható anélkül, hogy bárki később azonosítható lenne. Éppen ezért a szabálytalanul viselkedő mesh routerek azonosítása rendkívül fontos.

A gyors hitelesítési és a szabálytalanul viselkedő routerek azonosítását végző eljárást egy olyan EU-s projekt számára készítettem, amely több operátor által üzemeltetett Vezetéknélküli Mesh Hálózatokban rejlő lehetőségeket kívánt kiaknázni. Az FP7-es project EU-MESH néven (`http://www.eu-mesh.eu`) indult 2008-ban, és sikeresen befejeződött 2010 harmadik negyedévében.

Hivatkozások

[ABV+04] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible Authentication Protocol (EAP). RFC 3748 (Proposed Standard), June 2004. Updated by RFC 5247.

[BGLB02] Ljubica Blažević, Silvia Giordano, and Jean-Yves Le Boudec. Self organized terminode routing. *Cluster Computing*, 5:205–218, April 2002.

[BV11] Zoltán Böjthe and Andras Varga. Omnet++ network simulation framework. `http://www.omnetpp.org/`, 2011.

[FT91] D. Fudenberg and J. Tirole. *Game Theory*. MIT Press, 1991.

[Har75] J.A. Hartigan. *Clustering algorithms*. John Wiley & Sons, Inc. New York, NY, USA, 1975.

[IEE01] IEEE Std 802.1X-2001. IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control, June 2001.

[IEE04] IEEE Std 802.11i™. Medium Access Control (MAC) security enhancements, amendment 6 to IEEE Standard for local and metropolitan area networks part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications., July 2004.

[IEE08] IEEE 802.11r™-2008. IEEE Standard for Information Technology – Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 2: Fast BSS Transition, July 2008.

[Mal09] Jouni Malinen. WPA/RSN Supplicant (wpa_supplicant) and WPA/RSN/EAP Authenticator (hostapd) v0.6.7. `http://hostap.epitest.fi/`, 2009.

[ols10] olsrd. an ad hoc wireless mesh routing daemon, 2010. `http://www.olsr.org`.

[PVS07] Antonis Panagakis, Athanasios Vaios, and Ioannis Stavrakakis. On the Effects of Cooperation in DTNs. In *Proc. of The Second IEEE/Create-Net/ICST International Conference on COMmunication System softWAre and MiddlewaRE (COMSWARE)*, pages 1–6, January 7-12 2007.

[SUM10] SUMO. Simulation of Urban MObility. `http://sumo.sourceforge.net/`, 2010.

6. Publikációk

Könyvfejezetek

[B1] I. Askoxylakis, B. Bencsáth, L. Buttyán, L. Dóra, V. Siris, and A. Traganitis. *Cross-layer security and resilience in wireless mesh networks.* Cross Layer Designs in WLAN Systems, Troubador Publishing Ltd, Emerging Communication and Service Technologies Series, 2010.

Nemzetközi folyóiratcikkek

[J1] I. Askoxylakis, B. Bencsáth, L. Buttyán, L. Dóra, V. Siris, D. Szili, and I. Vajda. Securing Multi-operator Based QoS-aware Mesh Networks: Requirements and Design Options. *Wireless Communications and Mobile Computing (Special Issue on QoS and Security in Wireless Networks)*, 10(5):622–646, 2009.

[J2] L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda. Barter Trade Improves Message Delivery in Opportunistic Networks. *Elsevier Ad Hoc Networks*, 8(1):1–14, January 2010.

[J3] L. Buttyán, L. Dóra, F. Martinelli, and M. Petrocchi. Fast Certificate-based Authentication Scheme in Multi-operator maintained Wireless Mesh Networks. *Elsevier Computer Communications*, 33(8):907–922, April 2010.

Nemzetközi konferencia és workshop cikkek

[C1] G. Ács, L. Buttyán, and L. Dóra. Misbehaving Router Detection in Link-state Routing for Wireless Mesh Networks. In *Proceedings of the Second IEEE WoWMoM Workshop on Hot Topics in Mesh Networking (HotMESH'10)*, Montreal, Canada, June 2010.

[C2] A. Bohák, L. Buttyán, and L. Dóra. An User Authentication Scheme for Fast Handover Between WiFi Access Points. In *Proceedings of the Third Annual International Wireless Internet Conference*, Austin, Texas, USA, October 22-23 2007. ACM. (invited paper).

[C3] L. Buttyán and L. Dóra. An Authentication Scheme for QoS-aware Multi-operator maintained Wireless Mesh Networks. In *Proceedings of the First IEEE WoWMoM Workshop on Hot Topics in Mesh Networking (HotMESH'09)*, Kos, Greece, June 2009.

[C4] L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda. Barter-based cooperation in delay-tolerant personal wireless networks. In *Proceedings of the First IEEE WoWMoM Workshop on Autonomic and Opportunistic Communications*. IEEE Computer Society Press, June 2007.

[C5] L. Buttyán, L. Dóra, and I. Vajda. Statistical Wormhole Detection in Sensor Networks. In *Proceedings of Security and Privacy in Ad-hoc and Sensor Networks: Second European Workshop*, pages 128–141, Visegrad, Hungary, July 13-14 2005. Springer-Verlag GmbH.

[C6] L. Dóra and T. Holczer. Hide-and-Lie: Enhancing Application-level Privacy in Opportunistic Networks. In *Proceedings of the Second International Workshop on Mobile Opportunistic Networking ACM/SIGMOBILE MobiOpp 2010*, Pisa, Italy, February 22-23 2010.

Nemzeti folyóiratcikkek

[N1] L. Buttyán and L. Dóra. Wifi biztonság - a jó, a rossz, és a csúf. *Híradástechnika*, May 2006.

Szakdolgozatok

[T1] D. László. Féregjárat detektálása szenzorhálózatokban statisztikus eszközökkel. Master's thesis, Budapesti Műszaki és Gazdaságtudományi Egyetem, Villamosmérnöki és Informatikai Kar, 1111 Budapest, Egry József u. 18., May 2005.

Egyéb

[O1] D. László. Féregjárat detektálása szenzorhálózatokban statisztikus eszközökkel. TDK III. helyezet, November 2004. Budapesti Műszaki és Gazdaságtudományi Egyetem, Villamosmérnöki és Informatikai Kar.

Hivatkozások a publikációimra

[J2] L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda. Barter Trade Improves Message Delivery in Opportunistic Networks. *Elsevier Ad Hoc Networks*, 8(1):1–14, January 2010.

cikkre a következők hivatkoznak:

[1] A. Mei and J. Stefa. Give2Get: Forwarding in Social Mobile Wireless Networks of Selfish Individuals. In *Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on*, pages 488–497. IEEE, 2010.

[C2] A. Bohák, L. Buttyán, and L. Dóra. An User Authentication Scheme for Fast Handover Between WiFi Access Points. In *Proceedings of the Third Annual International Wireless Internet Conference*, Austin, Texas, USA, October 22-23 2007. ACM. (invited paper).

cikkre a következők hivatkoznak:

[1] Liang Cai, S. Machiraju, and Hao Chen. Capauth: A capability-based handover scheme. In *INFOCOM, 2010 Proceedings IEEE*, pages 1 –5, March 2010.

[2] Zoltán Faigl, Stefan Lindskog, and Anna Brunstrom. Performance evaluation of ikev2 authentication methods in next generation wireless networks. *Security and Communication Networks*, 3(1):83–98, 2010.

[C3] L. Buttyán and L. Dóra. An Authentication Scheme for QoS-aware Multi-operator maintained Wireless Mesh Networks. In *Proceedings of the First IEEE WoWMoM Workshop on Hot Topics in Mesh Networking (HotMESH'09)*, Kos, Greece, June 2009.

cikkre a következők hivatkoznak:

[1] Bing He. *Architecture Design and Performance Optimization of Wireless Mesh Networks.* PhD thesis, University of Cincinnati, Ohio, 2010.

[C4] L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda. Barter-based cooperation in delay-tolerant personal wireless networks. In *Proceedings of the First IEEE WoWMoM Workshop on Autonomic and Opportunistic Communications.* IEEE Computer Society Press, June 2007.

cikkre a következők hivatkoznak:

[1] Panayotis Antoniadis. *Mobile Peer-to-Peer Computing for Next Generation Distributed Environments: Advancing Conceptual and Algorithmic Applications*, chapter Incentives for Resource Sharing in Ad Hoc Networks: Going Beyond Rationality, pages 218–239. IGI Global, 2009.

[2] Hamed Janzadeh, Kaveh Fayazbakhsh, Mehdi Dehghan, and Mehran S. Fallah. A secure credit-based cooperation stimulating mechanism for manets using hash chains. *Future Generation Computer Systems*, 25(8):926 – 934, 2009.

[3] I. Koukoutsidis, E. Jaho, and I. Stavrakakis. Cooperative content retrieval in nomadic sensor networks. In *INFOCOM Workshops 2008, IEEE*, pages 1 –6, April 2008.

[4] Udayan Kumar, Gautam Thakur, and Ahmed Helmy. Protect: proximity-based trust-advisor using encounters for mobile societies. In *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference*, IWCMC '10, pages 636–645, New York, NY, USA, 2010. ACM.

[5] G. Resta and P. Santi. The effects of node cooperation level on routing performance in delay tolerant networks. In *Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON '09. 6th Annual IEEE Communications Society Conference on*, pages 1 –9, June 2009.

[6] Xiaojuan Xie, Haining Chen, and Hongyi Wu. Bargain-based stimulation mechanism for selfish mobile nodes in participatory sensing network. In *Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON '09. 6th Annual IEEE Communications Society Conference on*, pages 1 –9, June 2009.

[7] Xiong Yong-Ping, Sun Li-Min, Niu Jian-Wei, and Liu Yan. Opportunistic Networks. *Journal of Software*, 20(1):124–137, 2009.

[C6] L. Dóra and T. Holczer. Hide-and-Lie: Enhancing Application-level Privacy in Opportunistic Networks. In *Proceedings of the Second International Workshop on Mobile Opportunistic Networking ACM/SIGMOBILE MobiOpp 2010*, Pisa, Italy, February 22-23 2010.

cikkre a következők hivatkoznak:

[1] Iain Parris and Tristan Henderson. Privacy-enhanced social-network routing. *Computer Communications*, In Press, Corrected Proof:–, 2010.

[C5] L. Buttyán, L. Dóra, and I. Vajda. Statistical Wormhole Detection in Sensor Networks. In *Proceedings of Security and Privacy in Ad-hoc and Sensor Networks: Second European Workshop*, pages 128–141, Visegrad, Hungary, July 13-14 2005. Springer-Verlag GmbH.

cikkre a következők hivatkoznak:

[1] Marianne Azer, Sherif El-Kassas, and Magdy M. S. El-Soudani. A full image of the wormhole attacks - towards introducing complex wormhole attacks in wireless ad hoc networks. *CoRR*, abs/0906.1245, 2009.

[2] Marianne Azer, Sherif El-Kassas, Abdel Wahab Hassan, and Magdy El-Soudani. Intrusion detection for wormhole attacks in ad hoc networks: A survey and a proposed decentralized scheme. *Availability, Reliability and Security, International Conference on*, 0:636–641, 2008.

[3] Marianne A. Azer, Sherif M. El-Kassas, and Magdy S. El-Soudani. A scheme for intrusion detection and response in ad hoc networks. In Houda Labiod and Mohamad Badra, editors, *New Technologies, Mobility and Security*, pages 507–516. Springer Netherlands, 2007. 10.1007/978-1-4020-6270-4-42.

[4] Marianne A. Azer, Sherif M. El-Kassas, and Magdy S. El-Soudani. Immuning routing protocols from the wormhole attack in wireless ad hoc networks. *Systems and Networks Communication, International Conference on*, 0:30–36, 2009.

[5] Zhu Bin, Liao Jun'guo, and Zhang Huifu. Defending wormhole attack in aps dv-hop. In *Communications and Networking in China, 2008. ChinaCom 2008. Third International Conference on*, pages 219 –224, August 2008.

[6] Kasper Bonne Rasmussen and Srdjan Capkun. Implications of radio fingerprinting on the security of sensor networks. In *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on*, pages 331 –340, September 2007.

[7] Hyeon Choi and Tae Cho. Energy efficient mac length determination method for statistical en-route filtering using fuzzy logic. In De-Shuang Huang, Kang-Hyun Jo, Hong-Hee Lee, Hee-Jun Kang, and Vitoantonio Bevilacqua, editors, *Emerging Intelligent Computing Technology and Applications*, volume 5754 of *Lecture Notes in Computer Science*, pages 686–695. Springer Berlin / Heidelberg, 2009. 10.1007/978-3-642-04070-2-74.

[8] Tassos Dimitriou and Athanassios Giannetsos. Wormholes no more? localized wormhole detection and prevention in wireless networks. In Rajmohan Rajaraman, Thomas Moscibroda, Adam Dunkels, and Anna Scaglione, editors, *Distributed Computing in Sensor Systems*, volume 6131 of *Lecture Notes in Computer Science*, pages 334–347. Springer Berlin / Heidelberg, 2010. 10.1007/978-3-642-13651-1-24.

[9] Dezun Dong, Mo Li, Yunhao Liu, Xiang-Yang Li, and Xiangke Liao. Topological detection on wormholes in wireless ad hoc and sensor networks. In *Network Protocols, 2009. ICNP 2009. 17th IEEE International Conference on*, pages 314 –323, October 2009.

[10] Dezun Dong, Mo Li, Yunhao Liu, and Xiangke Liao. Wormcircle: Connectivity-based wormhole detection in wireless ad hoc and sensor networks. *Parallel and Distributed Systems, International Conference on*, 0:72–79, 2009.

[11] Jing Dong, Kurt E. Ackermann, Brett Bavar, and Cristina Nita-Rotaru. Mitigating attacks against virtual coordinate based routing in wireless sensor networks. In *Proceedings of the first ACM conference on Wireless network security*, WiSec '08, pages 89–99, New York, NY, USA, 2008. ACM.

[12] Jing Dong, Kurt E. Ackermann, Brett Bavar, and Cristina Nita-Rotaru. Secure and robust virtual coordinate system in wireless sensor networks. *ACM Trans. Sen. Netw.*, 6:29:1–29:34, July 2010.

[13] S.M. Glass, V. Muthukkumarasamy, and M. Portmann. Detecting man-in-the-middle and wormhole attacks in wireless mesh networks. In *Advanced Information Networking and Applications, 2009. AINA '09. International Conference on*, pages 530 –538, May 2009.

[14] Stephen Mark Glass, Vallipuram Muthukkumarasamy, and Marius Portmann. Detecting man-in-the-middle and wormhole attacks in wireless mesh networks. *Advanced Information Networking and Applications, International Conference on*, 0:530–538, 2009.

[15] Rennie Graaf, Islam Hegazy, Jeffrey Horton, and Reihaneh Safavi-Naini. Distributed detection of wormhole attacks in wireless sensor networks. In Ozgur Akan, Paolo Bellavista, Jiannong Cao, Falko Dressler, Domenico Ferrari, Mario Gerla, Hisashi Kobayashi, Sergio Palazzo, Sartaj Sahni, Xuemin (Sherman) Shen, Mircea Stan, Jia Xiaohua, Albert Zomaya, Geoffrey Coulson, Jun Zheng, Shiwen Mao, Scott F. Midkiff, and Hua Zhu, editors, *Ad Hoc Networks*, volume 28 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 208–223. Springer Berlin Heidelberg, 2010. 10.1007/978-3-642-11723-7-14.

[16] Thaier Saleh Hayajneh. *Protocols for Detection and Removal of Wormholes for Secure Routing and Neighborhood Creation in Wireless Ad Hoc Networks*. PhD thesis, University of Pittsburgh, 2009.

[17] Jinsub Kim, Dan Sterne, Rommie Hardy, Roshan K. Thomas, and Lang Tong. Timing-based localization of in-band wormhole tunnels in manets. In *Proceedings of the third ACM conference on Wireless network security*, WiSec '10, pages 1–12, New York, NY, USA, 2010. ACM.

[18] Fan-rui Kong, Chun-wen Li, Qing-qing Ding, Guang-zhao Cui, and Bing-yi Cui. Wapn: a distributed wormhole attack detection approach for wireless sensor networks. *Journal of Zhejiang University - Science A*, 10:279–289, 2009. 10.1631/jzus.A0820178.

[19] Hae Young Lee and Tae Ho Cho. A report generation method for defending false negative attacks in ubiquitous sensor networks. *International Journal of Computer Science and Network Security*, 7(11):49–54, 2007.

[20] Hae Young Lee and Tae Ho Cho. Statistical en-route filtering of fabricated reports in ubiquitous sensor networks based on commutative cipher. *International Journal of Computer Science and Network Security*, 8(3):216–221, 2008.

[21] Hae Young Lee, Tae Ho Cho, and Hyung-Jong Kim. Fuzzy-based detection of injected false data in wireless sensor networks. In Samir Kumar Bandyopadhyay, Wael Adi, Tai-hoon Kim, and Yang Xiao, editors, *Information Security and Assurance*, volume 76 of *Communications in Computer and Information Science*, pages 128–137. Springer Berlin Heidelberg, 2010. 10.1007/978-3-642-13365-7-13.

[22] Hae Young Lee, Soo Young Moon, and Tae Ho Cho. Adaptive false data filtering method for sensor networks based on fuzzy logic and commutative cipher. In *Computer and Electrical Engineering, 2008. ICCEE 2008. International Conference on*, pages 228 –232, December 2008.

[23] Sanjay Madria and Jian Yin. Serwa: A secure routing protocol against wormhole attacks in sensor networks. *Ad Hoc Networks*, 7(6):1051 – 1063, 2009.

[24] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P. Hubaux. Secure neighborhood discovery: a fundamental element for mobile ad hoc networking. *Communications Magazine, IEEE*, 46(2):132 –139, February 2008.

[25] Tran Van Phuong, Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, and Heejo Lee. Transmission time-based mechanism to detect wormhole attacks. *Asia-Pacific Conference on Services Computing. 2006 IEEE*, 0:172–178, 2007.

[26] Eric Platon and Yuichi Sei. Security software engineering in wireless sensor networks. 2008.

[27] Marcin Poturalski, Panos Papadimitratos, and Jean-Pierre Hubaux. Secure neighbor discovery in wireless networks: Is it possible? Technical Report EPFL-LCA Report 2007-004, Ecole Polytechnique Fédérale de Lausanne, 2007.

[28] Marcin Poturalski, Panos Papadimitratos, and Jean-Pierre Hubaux. Towards provable secure neighbor discovery in wireless networks. In *Proceedings of the 6th ACM workshop on Formal methods in security engineering*, FMSE '08, pages 31–42, New York, NY, USA, 2008. ACM.

[29] B. Prasannajit, Anupama S. Venkatesh, K. Vindhykumari, S.R. Subhashini, and G. Vinitha. An approach towards detection of wormhole attack in sensor networks. *Integrated Intelligent Computing*, 0:283–289, 2010.

[30] Reza Shokri, Marcin Poturalski, Gael Ravot, Panos Papadimitratos, and Jean-Pierre Hubaux. A practical secure neighbor verification protocol for wireless sensor networks. In *Proceedings of the second ACM conference on Wireless network security*, WiSec '09, pages 193–200, New York, NY, USA, 2009. ACM.

[31] Reza Shokri, Marcin Poturalski, Gael Ravot, Panos Papadimitratos, and Jean pierre Hubaux. A low-cost secure neighbor verification protocol for wireless sensor networks. 2008.

[32] Ajit Singh and Kunwar Singh Vaisla. A mechanism for detecting wormhole attacks on wireless ad hoc network. *International Journal of Computer and Network Security*, 2(9):27–31, 2009.

[33] D. Sterne, G. Lawler, R. Gopaul, B. Rivera, K. Marcus, and P. Kruus. Countering false accusations and collusion in the detection of in-band wormholes. In *Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual*, pages 243 –256, December 2007.

[34] Phuong Van Tran, Le Xuan Hung, Young-Koo Lee, Sungyoung Lee, and Heejo Lee. Ttm: An efficient mechanism to detect wormhole attacks in wireless ad-hoc networks. In *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE*, pages 593 –598, January 2007.

[35] T. Van Phuong, Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, and Heejo Lee. Transmission time-based mechanism to detect wormhole attacks. In *Asia-Pacific Service Computing Conference, The 2nd IEEE*, pages 172 –178, December 2007.

[36] Revathi Venkataraman, M. Pushpalatha, T. Rama Rao, and Rishav Khemka. A graph-theoretic algorithm for detection of multiple wormhole attacks in mobile ad hoc networks. *International Journal of Recent Trends in Engineering (IJRTE)*, 1(2):220–222, 2009.

[37] Xia Wang. Intrusion detection techniques in wireless ad hoc networks. In *Computer Software and Applications Conference, 2006. COMPSAC '06. 30th Annual International*, volume 2, pages 347 –349, September 2006.

[38] Xia Wang. Intrusion detection techniques in wireless ad hoc networks. *Computer Software and Applications Conference, Annual International*, 2:347–349, 2006.

[39] W. Znaidi, M. Minier, and J.-P. Babau. Detecting wormhole attacks in wireless networks using local neighborhood information. In *Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on*, pages 1 –5, September 2008.