



BUDAPESTI MŰSZAKI ÉS GAZDASÁGTUDOMÁNYI EGYETEM
Villamosmérnöki és Informatikai Kar

Híradástechnikai tanszék
Adatbiztonság laboratórium (CrySyS)

BIZTONSÁGOS ÚTVONALVÁLASZTÁS
TÖBBUGRÁSOS VEZETÉKNÉLKÜLI
HÁLÓZATOKBAN

Tézisfüzet

Ács Gergely

Konzulens:
Dr. Buttyán Levente

Budapest

2009

1. Bevezetés

Az útvonalválasztás alapvető hálózatrétegbeli szolgáltatás többugrásos vezeték nélküli hálózatokban. Egy támadó könnyen megbéníthatja az egész hálózat működését az útvonalválasztó protokoll megtámadása által. Ráadásul ezek a támadások általában nem igényelnek sok erőforrást a támadó részéről, néhány útvonalválasztó üzenet manipulálása vagy új fabrikált üzenetek beszúrása már elégséges ahhoz, hogy a támadó felborítsa a hálózat normál működését. Ebben a disszertációban a többugrásos vezeték nélküli hálózatokra javasolt topológia alapú útvonalválasztó protokollok útvonalfelderítésének a biztonságával foglalkozom.

A legtöbb vezeték nélküli ad hoc és szenzorhálózatokra javasolt útvonalválasztó protokoll vagy nem biztonságos, vagy pedig biztonságosnak tervezték, de biztonságukat csak informális érveléssel igazolták. Az informális érvelés viszont hibázási lehetőségeket rejt magában a támadások szövevényes és bonyolult jellege miatt. Ugyan a különböző üzenethitelesítési és kulcs-csere protokollok klasszikus és jól ismert problémák a tradicionális vezeték nélküli hálózatokban [Bellare *et al.*, 1998] [Pfitzmann and Waidner, 2001a], a biztonságos vezeték nélküli útvonalválasztó protokollok formális analízisének irodalma meglepően szegény. Ugyan néhány korábbi munkában már használtak formális technikákat a többugrásos útvonalválasztó protokollok biztonságának elemzésére [Yang and Baras, 2003] [Papadimitratos and Haas, 2002], de ezen protokollokat elsősorban ad hoc hálózatokra javasolták. Ráadásul ezen technikák vagy csak kizárólag bizonyos konkrét protokollok elemzésére alkalmazható [Papadimitratos and Haas, 2002], vagy pedig a biztonság-definíciójuk olyan erős [Yang and Baras, 2003], hogy kétséges olyan protokoll létezése, amely kielégítené azt. Ezeken kívül nem léteznek olyan eszközök, amelyek lehetővé tennék útvonalválasztó protokollok biztonsági elemzését szintén hiányoznak.

2. Kutatási célkitűzések

*Céлом, hogy azonosítsam a vezeték nélküli hálózatokra javasolt biztonságos útvonalválasztó protokollok tervezési elveit biztonságuk **szisztematikus és precíz** elemzése által.*

Céljaim részletesebben a következők:

1. kifejleszteni egy új és általános formális keretrendszert, amelyben a biztonságos útvonalválasztás precíz definíciója megadható, és az útvonalválasztó protokollok matematikailag elemezhetőek. *Általános* ebben a kontextusban azt jelenti, hogy a modell figyelembe veszi az útvonalválasztó protokollok változatosságát [J4] [J5] többugrásos vezeték nélküli hálózatokban.
2. demonstrálni a keretrendszer használhatóságát valós példákon keresztül: megmutatni, hogyan elemezhetőek ebben a modellben létező biztonságos útvonalválasztó protokollok, amelyeket vezeték nélküli ad hoc és szenzorhálózatokra javasoltak. Valamint új biztonságos útvonalválasztó protokollokat tervezni, és bizonyítani ezek biztonságát ebben a modellben.

3. Kutatási módszerek

Általános értelemben analitikus technikát használok az útvonalválasztó protokollok biztonsági elemzéséhez, amely hasonló a szimulációs paradigmához (ld. [Mao, 2004] V. és VI. részét). Megjegyzem, hogy a szimulációs paradigma nem kapcsolódik a hagyományos értelemben vett

hálózati szimulációkhoz. A szimulációs paradigma alapja egy olyan számításméleti modell, amelyet eddig is sikeresen alkalmaztak különböző kriptográfiai protokollok biztonságának a bizonyítására. Az általam javasolt modell hasonló a szimulációs paradigmához, ahol a biztonságot mint a valós (ahol a támadó nincs korlátozva leszámítva azt, hogy polinomiális időben kell futnia) és ideális (ahol bizonyos támadások definíció szerint nem lehetségesek) világmodellek megkülönböztethetlenségeként definiálták. Másrészt viszont fontos különbségek is húzódnak a klasszikus szimulációs megközelítés és az én munkám között. A valós világmodell helyett az én modellemben a dinamikus modell írja le a protokoll-résztevők valóságos működését, valamint az ún. biztonsági célfüggvény specifikálja, hogy a elemezendő protokollnak hogyan kellene működni ideálisan; minden szimulációs futás végén a biztonsági célfüggvényt alkalmazzuk az összes becsületes csomópont útvonalválasztó állapotára, hogy eldöntsük, hogy a protokoll a specifikált biztonsági cél szerint működik-e. A protokoll biztonságos, ha ez a célfüggvény „nem elfogadható” eredményt csak elhanyagolható valószínűséggel ad vissza, ahol a „nem elfogadható” pontos definíciója protokoll függő. Ez a függvény különböző lehet különböző típusú útvonalválasztó protokollokra, de az általános megközelítés miszerint ennek a függvénynek a kimenetét hasonlítjuk össze egy előre definiált „elfogadható” értékkel változatlan.

A modellem része egy olyan támadó modell, amely különbözik a standard Dolev-Yao modellettől [Dolev and Yao, 1981], ahol a támadó képes minden kommunikációt kontrollálni a hálózatban. Vezetéknélküli ad hoc és szenzorhálózatokban a támadó vezetéknélküli eszközöket használ a rendszer megtámadásához, és így ésszerűbb azt feltételezni, hogy a támadó csak az antennája általa lefedett területen képes interferálni más csomópontok kommunikációjával. Ezen felül néhány szituációban képes lehet közvetlenül egymással kommunikáló csomópontok üzeneteit manipulálni, ami viszont nem teljesül vezetékes hálózatokban. Így szükséges a rádiókommunikáció broadcast természetének modellezése is.

4. Új eredmények

1. TÉZIS. [C2] [J3] [J1] [J2] [J4] [J5] *Javaslok egy új és általános matematikai keretrendszert, ami áll egy modellből és egy bizonyítási technikából, amely lehetőséget ad az útvonalválasztás biztonságának definiálására, egy adott útvonalválasztó protokoll modellezésére, és annak bizonyítására, hogy egy útvonalválasztó protokollok kielégíti a biztonság definícióját ebben a modellben.*

Ad hoc és szenzorhálózatok útvonalválasztó protokolljainak biztonsági hibái nagyon szövevényesek lehetnek. Következésképp ezen protokollok biztonságáról alkotott állítások, amelyeket csak informális érveléssel igazoltak mint pl. [Karlov and Wagner, 2003] or [Hu *et al.*, 2002], veszélyesek lehetnek. Ugyan néhány kísérletet már tettek arra, hogy formális módszerekkel elemezzék ezen protokollok biztonságát [Yang and Baras, 2003; Marshall, 2003; Papadimitratos and Haas, 2002], ezek vagy nem elég általánosak, hogy különböző protokollok biztonságát elemezni lehessen, vagy pedig nem megfelelő feltételezéseket használtak a bizonyítás során. Ezen technikák vagy csak néhány specifikus útvonalválasztó protokoll elemzésére alkalmasak [Papadimitratos and Haas, 2002; Marshall, 2003], vagy a biztonsági definíciójuk olyan erős, hogy kétséges olyan protokoll létezése amely kielégíti a definíciót.

Fontos hangsúlyozni, hogy a javasolt keretrendszer leginkább arra használható, hogy egy protokoll biztonságát bebizonyítsuk (ha valóban biztonságos), de arra közvetlenül nem alkalmazható, hogy támadásokat találjunk olyan protokollokban, amelyek hibásak. Viszont, ezen támadások indirekt módon felfedezhetőek, ha megpróbáljuk bebizonyítani a protokoll biztonságát, és megvizsgáljuk hol akad el a bizonyítás.

A keretrendszer magasszintű leírása a következő. Először az analizálandó protokoll működését a dinamikus modellel modellezzük. Ez egy számításelméleti modell, amely leírja a protokoll működését annak minden részletével. A dinamikus modell tartalmaz egy támadót is, ami egy tetszőleges folyamat (vagyis nem feltétlen követi a protokoll működési szabályait), és az egyetlen megkötés, hogy polinomiális időben kell futnia. Ez megengedi, hogy tetszőleges támadást figyelembe vegyünk így téve a modellt általánossá. Ahelyett, hogy a szimulációs paradigma szerint egy ideális világmodellt konstruálnék [Bellare *et al.*, 1998; Pfitzmann and Waidner, 2001a; Shoup, 1999; Pfitzmann and Waidner, 2001b; Backes and Pfitzmann, 2004], a biztonsági célfüggvényt használom a protokoll biztonsági céljának reprezentálására (megjegyzem, hogy egy hasonló megközelítést használnak [Backes and Pfitzmann, 2004]-ben, ahol az integritási tulajdonságot mint a Needham-Schroeder-Lowe nyilvános kulcsú kriptográfiai protokoll biztonsági célját definiálták a szerzők). Ezt a függvényt alkalmazzuk a bec sületes csomópontok útvonalválasztó bejegyzéseinek halmazán annak eldöntésére, hogy az kielégít-e bizonyos biztonsági kritériumokat vagy sem. A biztonsági célnak a rendszer tolerált tökéletlenségét is magába kell foglalnia. Ezek olyan támadások, amelyek elkerülhetetlenek, vagy pedig túl költséges ellenük védekezni, és így inkább toleráljuk őket. A protokollt akkor mondjuk biztonságosnak, ha azt végrehajtva a dinamikus modellben a biztonsági cél csak elhanyagolható valószínűséggel sérül.

A keretrendszert a következő részek alkotják: támadó modell, hálózati modell, biztonsági célfüggvény, dinamikus modell, biztonság definíciója, és a bizonyítási technika.

Támadó modell. A támadó elsődleges célja az útvonalválasztó protokoll elsődleges céljainak megghiúsítása [J4] [J5]. Általánosan ezen célok lehetnek a csomagkézbesítési ráta csökkentése, a forgalom felügyeletének növelése, a hálózati késleltetés növelése, valamint a hálózat élettartamának csökkentése.

Az eddigi modellekben a támadónak teljes felügyelete volt a bec sületes protokollrésztvevők kommunikációja felett. Ez azt jelentette, hogy a támadó képes az üzeneteket olvasni, módosítani, ill. törölni bármely két bec sületes résztvevő között, vagy éppen új fabrikált üzeneteket beszúrni bármely bec sületes résztvevőnek. Ez egy megfelelő modell lehet az Internet alapú hálózatokban, ahol néhány speciális hálózati elemhez (pl. router) történő hozzáférés során a támadó megszerezheti ezt a fajta ellenőrzést. Ezzel szemben vezeték nélküli ad hoc és szenzorhálózatokban a támadó akkor képes hasonló szintű kontrollra, ha fizikailag jelen van minden közvetlen összeköttetésnél a hálózatban. Ugyan ez előfordulhat speciális hálózati topológiák (pl. csillag) esetén, a gyakorlatban ennek kivételezése általában költséges a hálózat sima topológiája miatt. Így feltételezem, hogy a támadó egy átlagos csomóponttal megegyező kommunikációs képességgel rendelkezik ad hoc hálózatokban, míg szenzorhálózatokban a támadónak még lehetnek nagyobb erőforrással rendelkező ún. laptop típusú eszközei. Minden támadó csomópont képes rendszeren belüli (pl. csatornázás) vagy rendszeren kívüli (pl. más frekvencia csatornát, vagy közvetlen vezetékes kapcsolatot féreglyuk megvalósításához).

Amikor a támadó kompromittál egy bec sületes csomópontot képes megszerezni annak minden kriptográfiai kulcsát (feltéve, hogy ilyen kulcsokat használnak a protokoll futása során).

Ez egyidejűleg megenged néhány olyan támadást, amelyek vagy túl költségesek, vagy pedig nem az útvonalválasztási réteg ellen irányulnak. Ezek magukba foglalják a side-channel támadásokat (pl. csatornázás) [Burmester and de Medeiros, 2007], rushing támadásokat [Hu, 2003], különböző DoS támadásokat, Sybil támadásokat [Douceur, 2002], és a node replication támadásokat [Bryan *et al.*, 2005]. Ezen támadásokat a modell nem foglalja magába.

A támadó aktív abban az értelemben, hogy az üzenetek lehallgatása mellett képes új üzeneteket fabrikálni és beszúrni, valamint képes olyan létező üzeneteket módosítani, törölni, üzenetszekvenciákat átrendezni és késleltetni, amelyek áthaladnak rajta. Fontos megjegyezni, hogy a hagyományos vezetékes hálózatokkal szemben a támadó képes lehet két közvetlenül egymással kommunikáló csomópontok üzeneteit manipulálni.

Ebben a disszertációban nem foglalkozom minden az útvonalválasztó protokollra irányuló támadással [B1]. Olyan üzenetek manipulálását felhasználó támadásokra fókuszálok, amelyek a becsületes csomópontok útvonalválasztó bejegyzéseinek korrupciójára irányul, ahol egy bejegyzés egy útvonal reprezentációja az adott cél irányába. Ez a reprezentáció lehet az csomópontok azonosítóinak listája, amelyek az utat alkotják mint pl. DSR esetében, vagy pedig következő csomópont azonosítója, amelyen keresztül léteznie kellene egy útnak a cél felé egy bizonyos költséggel. A támadó célja, hogy a becsületes csomópontok olyan bejegyzéseket használjanak, amelyek nem konzisztensek az adott hálózati topológiával, ahol a konzisztencia definíciója protokollfüggő, és az ilyen bejegyzéseket inkorrekt útvonalválasztó bejegyzésnek hívjuk.

Ugyan a figyelembe vett támadások az összes ismert támadás csak kis részét alkotják, még néhány „biztonságos” útvonalválasztó protokoll is támadható ezekkel a támadásokkal, ahol a támadó kizárólag csak egyszerű üzenetmanipulációt alkalmaz.

Hálózati modell. Feltételezem, hogy minden becsületes eszköz pontosan egy átvívó egységgel rendelkezik a hálózatban. Ha a támadó több átvívó egységgel rendelkezik, akkor mind-egyiket egy különálló támadó csomópontként reprezentálok a hálózatban. A hálózat statikus, és feltételezem, hogy a szenzorhálózatokban egyetlen bázisállomás van.

A becsületes csomópontokat v_0, \dots, v_k jelöli, ahol v_0 a bázisállomást jelöli szenzorhálózatok esetében, a támadó csomópontokat pedig v_{k+1}, \dots, v_{k+m} jelöli. Az összes csomópontot V , a támadó csomópontok halmazát V^* jelöli, ahol $|V| = n = m + k + 1$, és $|V^*| = m$.

A szomszédossági relációk jellemzésére bevezetem a \mathbf{E} mátrixot, amit elérhetőségi mátrixnak nevezek, és mérete $n \times n$. $E_{i,j}$ ($0 \leq i, j \leq n - 1$) reprezentálja azt a kimeneti teljesítményt, amelyet v_i támogat, és ahhoz szükséges, hogy v_i kommunikáljon v_j -vel (azaz ha v_i $E_{i,j}$ teljesítményt használja egy üzenet többszórásához, akkor azt v_j is hallja). Ha v_j nem képes üzenetet venni v_i -től (pl. akadályok vannak köztük, vagy a szükséges kimeneti teljesítményszint túl magas v_i számára) $E_{i,j} = \infty$.

Feltételezem, hogy minden becsületes csomópont használ egyetlen globálisan egyedi azonosítót a hálózatban, és ezen azonosítókat hitelesítik valamilyen módon (pl. kriptográfiai módszerekkel). Ezen azonosítók halmazát L -el jelölöm, és létezik egy $\mathcal{L} : V \rightarrow 2^{L \cup \{\text{undef}\}}$ függvény, amely minden csomópontoz azonosítók egy részhalmazát rendeli, ahol $\text{undef} \notin L$ olyan csomópontokhoz rendelődnek, amelyeknek nincs azonosítójuk. A támadó modellnek megfelelően feltételezem, hogy a támadó rendelkezhet (hitelesített) azonosítókkal a hálózatban, amelyet L^* jelöl, és felteszem, hogy minden támadó csomópont képes minden ilyen azonosítót használni (azaz $\mathcal{L}(v_{k+j}) = L^*$ minden $1 \leq j \leq m$ -re). Továbbá minden v_i ($1 \leq i \leq k$) becsületes csomópontoz $\mathcal{L}(v_i)$ egy egyelemű halmaz, és $\mathcal{L}(v_i) \notin L^*$.

Végezetül, a $\mathcal{C} : V \rightarrow \mathbb{R}$ költségfüggvény hozzárendel minden csomópont-hoz egy útvonal-választási költséget (pl. a minimális processzá-lási költséget, vagy konstans 1-et a hopszám modellezése céljából, stb.), amely az útvonalvá-lasztási költséget befolyásolhatja.

Konfiguráció: Egy hálózat *konfigurációja* egy ötös: $conf = (V, V^*, \mathcal{L}, \mathbf{E}, \mathcal{C})$.

Feltételezem, hogy a konfiguráció statikus (legalábbis az analízis ideje alatt).

Biztonsági célfüggvény. A rendszer állapotát az összes becsületes csomópont összes útvonalvá-lasztási bejegyzése reprezentálja. Azért csak a becsületes csomópontok bejegyzéseit veszem figyelembe, mert a támadó csomópontok nem feltétlen követik az útvonalvá-lasztó protokoll szabályait.

Mivel a bejegyzések specifikációja az analizálandó útvonalvá-lasztó protokolltól függ, a rendszerá-lapot definíciója szintén protokollfüggő. A $\mathcal{F} : \mathbb{G} \times \mathbb{S} \rightarrow \{0, 1\}$ biztonsági célfügg-vény egy bináris függvény, ahol \mathbb{S} jelöli az összes rendszerá-lapot halmazát, és \mathbb{G} az összes konfiguráció halmazát. Legyen \mathcal{F} 0 értékű minden olyan rendszerá-lapot és konfiguráció párra ami inkorrekt, máskülönb-en adjon vissza 1-et (vagy fordítva). Ennek a függvénynek a célja, hogy megkülönböztesse a „támadott” (inkorrekt) állapotokat a „nem támadott” (korrekt) á-lapotoktól.

Dinamikus modell. A dinamikus modellt ami megfelel egy $conf = (V, V^*, \mathcal{L}, E, \mathcal{C})$ kon-figurációnak és egy \mathcal{A} támadónak $sys_{conf, \mathcal{A}}$ -vel jelöljük. A protokoll résztevevők működését interaktív és probabilisztikus Turing gépekkel modellezem. A számításnak akkor van vége, ha minden becsületes csomópontot reprezentáló gép végső állapotba ér, vagy bekövetkezik egy time-out.

$sys_{conf, \mathcal{A}}$ kimenete a biztonsági célfüggvény értéke a számítás eredményeként kapott rend-szerá-lapokra és a $conf$ konfigurációra alkalmazva. A rendszerá-lapotot a becsületes csomó-pontok útvonalvá-lasztó bejegyzéseinek összessége adja. A modell kimenetét $Out_{conf, \mathcal{A}}^{\mathcal{F}}(r)$ -vel jelölöm, ahol r a modell véletlen bemenete. $Out_{conf, \mathcal{A}}^{\mathcal{F}}$ jelöli a $Out_{conf, \mathcal{A}}^{\mathcal{F}}(r)$ -t leíró véletlen valószínűségi változót, amikor r -t egyenletes eloszlás szerint választjuk.

A modell biztonsági paraméterét κ -val jelölöm (pl. κ jelölheti annak kriptográfiai primi-tívnek a hosszát, amit a protokoll használ mint pl. MAC, vagy digitális aláírás, stb.)

A fenti modell alapján a útvonalvá-lasztás biztonsága a következőképpen definiálható.

1. Definíció. *Egy útvonalvá-lasztó protokoll biztonságos egy \mathcal{F} biztonsági célfüggvényt tekintve, ha bármely $conf$ konfigurációra, és bármely \mathcal{A} támadóra annak a valószínűsége, hogy $Out_{conf, \mathcal{A}}^{\mathcal{F}}$ egyenlő 0-val elhanyagolható függvénye κ -nak.*¹

Bizonyítási technika. Egy protokoll bizonyítása során meg kell mutatnunk, hogy azok a rendszerá-lapotok, amelyek megsértik a biztonsági célt (vagyis létezik egy $conf$ konfigurá-ció úgy, hogy \mathcal{F} -et alkalmazva ezekre a rendszerá-lapotokra az nullát ad $conf$ konfigurációval) csak elhanyagolható valószínűséggel fordulnak elő. Csakhogy az összes konfiguráció száma egy adott számú csomópont-ra a csomópontok számának exponenciális függvénye. Így ha a bizo-nyítás során az összes ilyen rendszerá-lapot és konfiguráció párt kellene vizsgálni, és ellenőrizni, hogy \mathcal{F} 0-t ad ezen párokra, elsőre egy nehéz feladatnak tűnik. Szerencsére minden ilyen pár

¹egy $\mu(x) : \mathbb{N} \rightarrow \mathbb{R}$ függvény elhanyagolható, ha minden c pozitív egész számra és minden elég nagy x -re (azaz létezik $N_c > 0$ minden $x > N_c$ -re), $\mu(x) \leq x^{-c}$

redukálható volt néhány alapesetre minden olyan protokoll esetében, amelyet a disszertációban elemeztem. Ezután azt kell megmutatni, hogy minden ilyen alapeset csak elhanyagolható valószínűséggel fordul elő, amiből következik, hogy a protokoll eleget tesz az 1. definíciónak. Ennek belátáshoz azt meg kell mutatni, hogy ezek az alapesetek csak akkor fordulhatnak elő a modellben, ha a támadó sikeresen megtöri a protokoll által felhasznált kriptográfiai primitívet. Viszont, ha ezek feltételezeten biztonságosak, akkor ennek az események a valószínűsége elhanyagolható függvénye a κ biztonsági paraméternek.

A gyakorlatban ha nem tudjuk belátni egy protokoll biztonságát a modellben az egy biztonsági problémára utal a protokollban, és gyakran konstruálható támadás a protokoll ellen úgy, hogy megnézzük pontosan hol akad el a bizonyítás.

2. TÉZIS. *[C2] Adaptálom az 1. tézisben javasolt általános biztonsági keretrendszeremet a TinyOS beaconing nevű vezeték nélküli szenzorhálózatokban használt protokollra, és bebizonyítom, hogy a hitelesített TinyOS beaconing, amelyet [Perrig et al., 2002]-ben javasoltak, nem biztonságos egy olyan biztonsági célfüggvényt tekintve, amely megköveteli, hogy ha egy becsületes csomópont beállít egy másik csomópontot mint szülőt, akkor a két csomópont szomszédos, vagy mindegyiknek kell lennie legalább egy szomszédjának aki támadó csomópont.*

Eredetileg a TinyOS [Hill et al., 2000] szerzői egy nagyon egyszerű útvonalválasztó protokollt javasoltak, amit TinyOS beaconing-nek neveztek el. Ebben a protokollban minden csomópont egy globálisan egyedi azonosítóval van megcímezve, és a bázisállomás periodikusan kezdeményez egy útvonalfelderítést a hálózat egy beaconnel történő elárasztásával. Ennek célja egy fa alapú útvonalválasztási topológia létrehozása. [Perrig et al., 2002]-ban a szerzők egy egyszerű kriptográfiai kiterjesztést alkalmaznak, hogy hitelesítsék a bázisállomás által küldött beacont. A TinyOS beaconing ezen hitelesített változata a μ Tesla sémát használja az integritás eléréshez; minden kulcs az egymást követő beacon-intervallumokban kerül szétosztásra. Hogy a modellemmel összhangban legyenek, bemutatom ennek a protokollnak egy olyan variánsát, amely ua. a biztonságot nyújtja mint [Perrig et al., 2002]. Következésképp az összes támadás ezen új protokoll ellen működik a [Perrig et al., 2002]-ben javasolt protokoll ellen is.

Ennek a hitelesített TinyOS beaconingnek az üzeneteit és működését szemlélteti a 1. ábra. Feltételezzük, hogy a bázisállomás rendelkezik egy nyilvános-privát kulcspárral, amit aláírás-generálásra használ, valamint minden szenzor rendelkezik ezen pár nyilvános részével. Kezdetben B bázis létrehoz egy beacont, ami tartalmaz egy BEACON konstans üzenetazonosítót, egy generált rnd véletlent, a bázis id_B azonosítóját, és egy sig_B aláírást mindezek az elemeken. Utána a bázis elárasztja a hálózatot ezzel a beaconnel. Minden X szenzor, amely megkapja ezt az üzenetet ellenőrzi, hogy duplikátum-e a kapott beacon. Ha igen, akkor eldobja a beacont. Egyébként ellenőrzi a sig_B aláírást. Ha ez korrekt, akkor X beállítja id_B -t szülőnek, és újraküldi a beacont miután módosította a küldő id_B azonosítóját a saját id_X azonosítójára. Máskülönben X eldobja az üzenetet. Minden szenzor amely megkapja ezt az üzenetet ugyanazokat a lépéseket hatja végre mint X .

Az adattovábbítás során minden szenzor a kapott adatcsomagokat a szülőnek küldi a bázis irányába.

Mivel a támadó képes üzeneteket cserélni támadócsomópontok között rendszeren kívüli (pl. féreglyuk) vagy belüli (pl. alagutazás) csatornákon, amelyek ellen nagyon költséges védekezni, egy becsületes csomópontpárt „szomszédnak” tekintek, ha mindkettőnek van legalább egy támadó szomszédja.

$B \rightarrow *$:	$(\text{BEACON}, \text{rnd}, \text{id}_B, \text{sig}_B)$
$X \rightarrow *$:	$(\text{BEACON}, \text{rnd}, \text{id}_X, \text{sig}_B)$

1. táblázat. A hitelesített TinyOS beaconing üzenetei és működése.

2. Definíció (Álszomszédok). *Két $v_i, v_j \in V \setminus V^*$ ($i \neq j$) becsületes csomópont álszomszéd, akkor és csak akkor ha létezik x, y ($k + 1 \leq x, y \leq k + m$) úgy, hogy $E_{i,x} = 1$ és $E_{j,y} = 1$, valamint $v_x, v_y \in V^*$.*

Két csomópont álszomszéd csak akkor, ha mindegyiküknek van legalább egy támadó szomszédja. Munkám további részében megkülönböztetem az álszomszédokat a közvetlen szomszédtól; két v_i, v_j becsületes csomópont közvetlen szomszéd, ha $E_{i,j} = 1$. Megjegyzem, hogy ha két csomópont közvetlen szomszéd akkor még lehetnek álszomszédok is.

Emlékeztetek arra, hogy a rendszerállapot a becsületes csomópont útvonalválasztó bejegyzéseinek együttese. Ezen rendszerállapot egy adott *conf* konfigurációval reprezentálható egy $(k + 1) \times (k + 2)$ méretű T^{conf} mátrix-szal a hitelesített TinyOS beaconing esetében. Erre a mátrixra mint útvonalválasztási topológiára hivatkozom a továbbiakban egy adott *conf* konfiguráció esetén.

Minden $0 \leq i \leq k$ -re,

- és $0 \leq j \leq k$ -re, $T_{i,j}^{conf} = 1$, ha v_i becsületes csomópont minden üzenetet v_j becsületes csomópontnak továbbít, máskülönben legyen $T_{i,j}^{conf} = 0$.
- $T_{i,k+1}^{conf} = 1$, ha v_i becsületes csomópont minden üzenetet egy támadó csomópontnak továbbít, máskülönben legyen $T_{i,k+1}^{conf} = 0$.

Megjegyzem, hogy T^{conf} minden sorát és oszlopát nullától sorszámozok, és ez minden más mátrixra igaz a munkámban.

Ilyen módon minden útvonalválasztási topológia tekinthető úgy mint egy irányított gráf, amit T^{conf} mátrix ír le. Valójában T^{conf} egy véletlen valószínűségi változó, ahol a véletlenséget a mért adatok, a processzási és átviteli idők, stb. okozzák.

Egy egyszerű biztonsági célja lehet a hitelesített TinyOS beaconingnek, hogy legyen minden útvonalválasztási bejegyzés korrekt a hálózatban. Nevezetesen kívánatos, hogy egy v_i szenzor képes legyen elérni v_j szenzort, ha v_i beállítja $\mathcal{L}(v_j)$ -t mint szülő, tehát $E_{i,j}$ legyen egy véges érték, vagy v_i és v_j legyenek álszomszédok.

Legyen a hitelesített TinyOS beaconing biztonsági célfüggvénye, amit \mathcal{F}^{ATB} -vel jelölök, olyan, hogy 1-et adjon vissza minden olyan rendszerállapot és konfiguráció párra, ahol minden i, j -re igaz, ha $T_{i,j} = 1$, akkor v_i és v_j közvetlen vagy álszomszédok. Máskülönben legyen $\mathcal{F}^{ATB} = 0$

1. Tétel. *A hitelesített TinyOS beaconing nem biztonságos a \mathcal{F}^{ATB} függvényt tekintve.*

A bizonyítás arra a tényre épül, hogy egy beacon közvetlen küldője nem hitelesíti a beacont. Így egy támadó könnyen küldhet beacont tetszőleges becsületes csomópont nevében. A teljes bizonyítást a disszertáció tartalmazza.

3. TÉZIS. [J3] Terveztem egy új biztonságos forrás alapú útvonalválasztó protokollt vezeték nélküli ad hoc hálózatok számára, amit *endairA*-nak nevezek. *endairA* az *Ariadne* [Hu et al., 2002] megfordítása, mert a *request* üzenetek aláírása helyett a közbenső csomópontok a *reply* üzenetet írják alá. Az *endairA* hatékonyabb mint az *Ariadne*, mert kevesebb kriptográfiai műveletet igényel összességében a csomópontoktól. Adaptálom az 1. tézisben javasolt általános modellt dinamikus forrás alapú útvonalválasztó protokollokra, és bebizonyítom, hogy az *endairA* biztonságos egy olyan biztonsági célfüggvényt tekintve, amely megköveteli, hogy minden visszaadott út amit a protokoll ad vissza a forrás csomópontnak tartalmazza azonosítók egy olyan sorozatát, hogy

- az első azonosító a forrás csomópontához tartozik,
- az utolsó csomópont a célcsomópontához tartozik,
- nem tartalmaz ismétlődő azonosítókat,
- és minden nem kompromittált közbenső azonosító, amelyek vagy egymást követők vagy nem egymást követők de közöttük csak kompromittált azonosítók vannak, megfeleltethetők olyan csomópontpárnak a hálózatban, amelyek közvetlen vagy álszomszédok.

Az *endairA*-ban az útvonalfelderítés kezdeményezője generál egy kérést, amely tartalmazza a kezdeményező és a cél azonosítóját és egy véletlenül generált kérés-azonosítót. Minden közbenső csomópont, amely először kapja meg ezt a kérést hozzáfűzi a saját azonosítóját az eddig felhalmozott útvonalhoz a kérésben, és továbbküldi azt. Amikor a kérés eléri a célt, az generál egy választ. A válasz tartalmazza a kezdeményező és a cél azonosítóit, a felhalmozott útvonalat amely a kérésből származik, és a cél aláírását ezeken az elemeken. A válasz a kezdeményező felé kerül visszaküldésre azon az útvonalon, amelyen a kérés érkezett. Minden közbenső csomópont amely megkapja a választ először ellenőrzi, hogy a saját azonosítója szerepel-e az útvonalban, és hogy az megelőző ill. követő azonosítók szomszédos csomópontokhoz tartoznak-e. Minden közbenső csomópont azt is ellenőrzi, hogy a válaszban található aláírások helyesek-e. Ha bármely ellenőrzés sikertelen, a válasz eldobásra kerül. Máskülönben a közbenső csomópont aláírja a választ, és továbbadja az útvonalon a következő csomópontnak a kezdeményező felé. Amikor a kezdeményező megkapja a választ, ellenőrzi, hogy az első azonosító az útvonalban szomszédhoz tartozik-e. Ha igen, akkor ellenőrzi, hogy minden aláírás helyes-e. Ha minden ellenőrzés sikeres, a kezdeményező elfogadja a kapott útvonalat.

Az *endairA* üzeneteit és működését szemlélteti a 2. ábra.

Az *endairA* protokollnak van egy jelentős előnye más hasonló forrás alapú protokollokkal szemben, mint amilyen az *Ariadne* is: hatékonyabb, mivel az SRDP-hez [Kim and Tsudik, 2005] hasonlóan kevesebb kriptográfiai műveletet igényel összességében a csomópontoktól. Ennek oka, hogy az *endairA* csak a válaszüzenetek feldolgozása során igényel kriptográfiai műveleteket, és a válasz üzeneteket csak azok a csomópontok dolgozzák fel, amelyek szerepelnek az üzenetben található útvonalban. Ezzel szemben az *Ariadne* esetében a kérés üzenetet kell a csomópontoknak aláírniuk, amit viszont minden csomópontnak meg kell tennie a hálózatban, hiszen a kérés az egész hálózatot elárasztja.

Megjegyzem, hogy az SRDP [Kim and Tsudik, 2005] nagyon hasonló az *endairA*-hoz abban az értelemben, hogy a kérés üzenetek aláírása helyett a közbenső csomópontok csak a válasz

$S \rightarrow *$:	$(\text{rreq}, S, D, id, ())$
$A \rightarrow *$:	$(\text{rreq}, S, D, id, (A))$
$B \rightarrow *$:	$(\text{rreq}, S, D, id, (A, B))$
$T \rightarrow B$:	$(\text{rrep}, S, T, (A, B), (sig_T))$
$B \rightarrow A$:	$(\text{rrep}, S, T, (A, B), (sig_T, sig_B))$
$A \rightarrow S$:	$(\text{rrep}, S, T, (A, B), (sig_T, sig_B, sig_A))$

2. táblázat. Egy példa az endairA működésére és üzeneteire. Az útvonalfelderítés kezdeményezője S , a cél T , és a közbenső csomópontok A és B . id egy véletlen kérés azonosító. sig_A , sig_B , és sig_T rendre az A , B , és T csomópontok aláírásai. Minden egyes aláírást a megelőző üzenetmezőkön (beleértve a többi aláírást) generálnak a csomópontok.

üzeneteket írják alá. Ugyanakkor fő különbség, hogy [Kim and Tsudik, 2005] fókusza olyan kriptográfiai technikák vizsgálata, amelyek különböző szintű biztonságot, hatékonyságot, és robusztusságot biztosítanak. Ezen primitívek közös tulajdonsága, hogy helyettesítik az aláírások listáját egyetlen aggregált aláírással vagy MAC-kel, amelyet a közbenső csomópontok iteratívan számolnak. Ezen mechanizmus célja a kommunikációs többletterhelés csökkentése. Ezzel szemben az én munkám fókusza a biztonságos forrásalapú útvonalválasztó protokollok tervezése és formális analízise. Végül megjegyzem, hogy az endairA-t először [Ács *et al.*, 2005]-ben publikáltam, ami korábban volt mint [Kim and Tsudik, 2005].

A minimum amit egy forrás alapú protokoll útvonalfelderítésétől elvárunk, hogy csak létező útvonalat adjon vissza. Az általam definiált biztonsági cél ezen elvárásra épül. Figyelembe véve, hogy a támadó képes üzeneteket cserélni támadó csomópontok között belső illetve külső csatornákon, ami ellen túl költséges lenne védekezni, bevezetem a plauzibilis útvonal fogalmát.

3. Definíció (Plauzibilis útvonal). Egy $\ell_1, \ell_2, \dots, \ell_n$ azonosítókból álló sorozat plauzibilis egy $conf$ konfigurációt és \mathcal{L} címkéző függvényt tekintve, ha az $\ell_1, \ell_2, \dots, \ell_n$ azonosítók mindegyike különböző, és létezik egy v_1, v_2, \dots, v_t ($2 \leq t \leq n$) becsületes csomópontokból álló sorozat, hogy

- $\mathcal{L}(v_1) = \ell_1$ és $\mathcal{L}(v_t) = \ell_n$;
- minden $1 \leq i \leq t - 1$ esetén,
 - létezik $1 \leq j, d \leq n - 1$ úgy, hogy $\mathcal{L}(v_i) = \ell_j$ és $\mathcal{L}(v_{i+1}) = \ell_{j+d}$, ahol minden $j + 1 \leq z \leq j + d - 1$ esetén $\ell_z \in L^*$;
 - v_i és v_{i+1} közvetlen vagy álszomszédok.

Emléztetek arra, hogy a rendszerállapot az összes becsületes csomópont összes útvonalválasztó bejegyzéseinek halmaza. Forrás alapú útvonalválasztás esetén, egy bejegyzés magába foglalja az útvonalat (azaz a csomópont azonosítók sorozatát) amit adattovábbításra használnak a cél fel, amely ezen sorozat utolsó eleme. Legyen a forrás alapú protokollok \mathcal{F} függvénye 0 minden olyan rendszerállapotra és konfigurációra, ami tartalmaz egy nem plauzibilis útvonalat, ahol ez a nem plauzibilis útvonal egy becsületes csomópontoz tartozik. Máskülönb legyen \mathcal{F} értéke 1. Az 1. definíció szerint ha bármely becsületes csomópont a dinamikus modellben visszaad egy nem plauzibilis útvonalat nem elhanyagolható valószínűséggel egy adott konfigurációra, akkor a protokoll nem biztonságos.

2. Tétel. *Az endairA egy biztonságos forrás alapú útvonalválasztó protokoll vezetéknélküli ad hoc hálózatokra, ha az aláírás-séma biztonságos választott nyílt szövegű támadás ellen.*

A bizonyítás a disszertációban megtalálható. Mivel az Ariadne nem biztonságos ugyanebben a modellben, a modellem képes különbséget tenni forrás alapú útvonalválasztó protokollok között biztonság szempontjából. Az analízis egy következménye, hogy egy forrás alapú biztonságos útvonalválasztó protokollnak mindig hitelesítenie kell a válasz üzeneteket.

4. TÉZIS. [C1] *Adaptálom az 1. tézisben javasolt általános modellt dinamikus távolságvektor alapú útvonalválasztásra vezeték nélküli ad hoc hálózatokban, és bebizonyítom, hogy az SAODV [Zapata and Asokan, 2002] egy nem biztonságos útvonalválasztó protokoll egy olyan biztonsági célfüggvényt tekintve, amely megköveteli, hogy ha egy forráscsomópont rendelkezik egy útvonalválasztó bejegyzéssel a célcsoomópont felé, akkor létezik egy útvonal a hálózatban, amely*

- *a forráscsomópontból indul,*
- *a célcsoomópontban végződik,*
- *a költsége kisebb vagy egyenlő mint a bejegyzésben szereplő költség, és*
- *minden egymást követő becsületes csomópont az útvonalon rendelkezik egy olyan következő hop azonosítóval a cél felé, amely vagy kompromittált azonosító, vagy pedig az útvonalon fekvő következő becsületes csomópont azonosítója, amely csomópont közvetlen vagy álszomszéd.*

Az SAODV [Zapata and Asokan, 2002] az On-demand Distance Vector (AODV) [Perkins and Royer, 1999] útvonalválasztó protokoll biztonságos változata. Az SAODV működése hasonló az AODV működéséhez azzal a különbséggel, hogy kriptográfiai módszereket használ az üzenetek integritásának biztosításához, valamint a hopszám rosszindulatú manipulálásnak megakadályozásához. Az SAODV üzenetei (azaz a kérések és a válaszok) rendelkeznek egy változó és egy nem változó résszel. A nem változó rész magába foglalja többek között a csomópontok sorszámait, a forrás és cél címét, és egy kérés azonosítót, míg a változó rész tartalmazza a hopszám információt. Különböző mechanizmusokat használnak a különböző részek védelmére.

A nem változó részeket a forrás és a cél aláírása védi. Ez biztosítja, hogy a nem változó részeket egy támadó nem tudja módosítani anélkül, hogy azt egy becsületes csomópont ne detektálná.

A hopszám védelmére a szerzők egyirányú hash láncokat javasolnak. Amikor egy csomópont egy útvonalválasztó üzenetet küld (azaz kérést vagy választ) először beállítja `HopCount` mezőt 0-ra és a `MaxHopCount` mezőt pedig egy előre definiált `TimeToLive` értékre. Utána generál egy *seed* véletlen számot, és behelyezi ezt az üzenet `Hash` mezéjébe. Utána kiszámolja a `TopHash` értéket úgy, hogy a *seed* értéket hasheli `MaxHopCount` számszor. A `MaxHopCount` és a `TopHash` mezők az üzenet nem változó részéhez tartoznak, míg a `HopCount` és `Hash` mezők a változó részéhez. Minden csomópont amely egy kérést vagy választ kap hasheli a `Hash` mező értékét (`MaxHopCount – HopCount`) számszor, és ellenőrzi, hogy a kapott érték egyezik-e a `TopHash` mező értékével. Ezután mielőtt továbbküldené az üzenetet, a csomópont növeli a `HopCount` mező értékét eggyel, és frissíti a `Hash` értékét úgy, hogy egyszer hasheli annak értékét.

A hash lánc használatának lényege, hogy ha adott a `Hash`, `TopHash`, és `MaxHopCount` mezők értékei, akkor bárki ellenőrizheti `HopCount` mező értékét. Másrészről, előző hash értékeket kiszámolni nem lehet a `Hash` mező értékéből, a hash lánc egyirányú tulajdonsága miatt. Ez biztosítja, hogy egy támadó nem képes a hopszámot csökkenteni, és így nem tudja az útvonalat rövidebbnek feltüntetni.

Az útvonalválasztó tábla egy bejegyzése egy adott v csomópont esetén a következő három elemet tartalmazza: a cél azonosítóját, a következő hop azonosítóját a cél felé, és az útvonal vélt költségét. Feltételezem, hogy a kisebb költségű útvonalakat részesítik a csomópontok előnyben.

Következésképpen a rendszer állapota a modellben egy $Q \subset (V \setminus V^*) \times L \times L \times \mathbb{R}$ halmazzal reprezentálható úgy, hogy bármely (v, z_{tar}, z_{nxt}, c) és $(v', z'_{tar}, z'_{nxt}, c')$ elemre Q -ban, ha $v = v'$ és $z_{tar} = z'_{tar}$ és $z_{nxt} = z'_{nxt}$, akkor $c = c'$. A (v, z_{tar}, z_{nxt}, c) négyes Q -ban egy bejegyzést reprezentál v útvonalválasztó táblájában, ahol z_{tar} a cél azonosítója, a következő hop a cél felé z_{nxt} , és c az útvonal vélt költsége. Azon négyesek együttese, amelyek első eleme v reprezentálják v útvonalválasztó tábláját, és az összes ilyen négyes reprezentálja az összes csomópont útvonalválasztó tábláját (vagyis a rendszer állapotát). Vegyük észre, hogy megengedjük azt, hogy egy csomópont táblája több bejegyzést is tartalmazzon ugyanarra a célra vonatkozóan, de a következő hopoknak különbözőeknek kell lenniük.

Figyelembe véve, hogy az SAODV a hopszámot használja mit útvonalmetrikát, $\mathcal{C} : V \rightarrow \mathbb{R}$ minden csomóponthoz konstans 1-et rendel. A formalizmus megkönnyebbítése érdekében bevezetem a működő út fogalmát.

4. Definíció (Működő út). *A $(v_{\ell_0}, v_{\ell_1}, \dots, v_{\ell_{d-1}}, v_{\ell_d})$ becsületes csomópontok sorozatát működő útnak nevezzük conf konfigurációt illetően, ha minden $0 \leq i \leq d - 1$ esetén v_{ℓ_i} és $v_{\ell_{i+1}}$ közvetlen vagy álszomszéd.*

A korrekt állapotot a következőképp definiálom.

5. Definíció (Korrekt állapot). *Egy Q állapot korrekt, ha minden $(v_{src}, z_{dst}, z_{nxt}, c_{src}) \in Q$ bejegyzésre létezik $(v_{\ell_i}, z_{dst}, z_{\ell_i}, c_{\ell_i}) \in Q$ ($1 \leq i \leq d$) bejegyzések olyan sorozata, amely*

- $(v_{src}, v_{\ell_1}, \dots, v_{\ell_{d-1}}, v_{dst})$ egy működő út, ahol $v_{\ell_d} = v_{dst}$,
- $z_{dst} \in \mathcal{L}(v_{dst})$,
- legyen $v_{\ell_0} = v_{src}$ és $z_{\ell_0} = z_{nxt}$,
 - ha $v_{\ell_{i-1}}$ és v_{ℓ_i} közvetlen de nem álszomszédok, akkor $z_{\ell_{i-1}} \in \mathcal{L}(v_{\ell_i})$,
 - ha $v_{\ell_{i-1}}$ és v_{ℓ_i} álszomszédok, akkor $z_{\ell_{i-1}} \in \mathcal{L}(v_{\ell_i})$, vagy $z_{\ell_{i-1}} \in L^*$,
- $\sum_{i=1}^{d-1} \mathcal{C}(v_{\ell_i}) \leq c_{src}$.

Intuitíve egy rendszer korrekt állapotban van, ha minden becsületes csomópont összes bejegyzése korrekt abban az értelemben, hogy ha v_{src} rendelkezik egy bejegyzéssel ahol z_{dst} a cél, z_{nxt} a következő hop, c_{src} a költség, akkor valóban létezik egy útvonal a hálózatban, hogy

- v_{src} csomópontból indul,
- egy olyan csomópontba végződik, amely azonosítója z_{dst} ,
- költsége kisebb vagy egyenlő mint c_{src} , és
- minden egymást követő becsületes csomópont az úton rendelkezik egy olyan következő hop azonosítóval, amely vagy korrupt, vagy egy közvetlen vagy álszomszédhoz tartozik.

A dinamikus távolságvektor alapú útvonalválasztás \mathcal{F} biztonsági célfüggvénye 0-t rendel minden olyan rendszerállapot és konfiguráció párhoz, ahol a rendszer állapot inkorrekt, egyébként 1-et.

3. Tétel. *Az SAODV egy nem biztonságos távolságvektor alapú útvonalválasztó protokoll vezetéknélküli ad hoc hálózatokra.*

A bizonyítás arra épül, hogy az SAODV nem garantálja, hogy a következő hop és a hopszám információ korrekt egy bejegyzésben. Ennek oka az előző hop hitelesítésének hiánya. A bizonyítást a disszertáció részletezi.

5. TÉZIS. *[C1] Az 4. tézisben javasolt adaptált keretrendszert használva bebizonyítom, hogy az ARAN [Sanzgiri et al., 2002] egy biztonságos útvonalválasztó protokoll vezetéknélküli ad hoc hálózatokban figyelembe véve a 4. tézisben leírt biztonsági célfüggvényt.*

Ahogy az SAODV [Zapata and Asokan, 2002], az ARAN is publikus kriptográfiát használ az integritás biztosításához. Az ARAN-ban minden csomópont az elsőként kapott útvonalválasztó üzenet alapján számolja ki az útvonalat, és minden további üzenetet ami ugyanahhoz az útvonalfelderítéshez tartozik eldobnak. Ez azt jelenti, hogy az ARAN nem feltétel a legrövidebb hanem a leggyorsabb utat fedezi fel a hálózatban. Az SAODV-hez hasonlóan a forrás és a cél hitelesíti a kérést ill. a választ digitális aláírással, viszont az SAODV-vel szemben itt minden közbenső csomópont is aláírja az üzenetet. Jobban mondva minden egyes közbenső csomópont ellenőrzi az előző csomópont aláírását, és azt frissíti a saját aláírására mielőtt továbbküldené az üzenetet. Az ARAN üzeneteit és működését a 3. ábra szemlélteti.

$S \rightarrow *$:	$(RREQ, T, cert_S, N_S, t, Sig_S)$
$A \rightarrow *$:	$(RREQ, T, cert_S, N_S, t, Sig_S, Sig_A, cert_A)$
$B \rightarrow *$:	$(RREQ, T, cert_S, N_S, t, Sig_S, Sig_B, cert_B)$
$T \rightarrow B$:	$(RREP, S, cert_T, N_S, t, Sig_T)$
$B \rightarrow A$:	$(RREP, S, cert_T, N_S, t, Sig_T, Sig_B, cert_B)$
$A \rightarrow T$:	$(RREP, S, cert_T, N_S, t, Sig_T, Sig_A, cert_A)$

3. táblázat. Egy példa az ARAN működésére és üzeneteire. A felderítés kezdeményezője S , a cél T , és a közbenső csomópontok A és B . N_S egy véletlen kérés-azonosító. Sig_A , Sig_B , és Sig_T rendre az A , B , és T csomópontok aláírásai, valamint $cert_A$, $cert_B$, és $cert_T$ rendre a A , B , és T csomópontok publikus tanúsítványai. t jelöli az aktuális időbélyeget. Minden egyes aláírást az üzenet azon mezői fölött számolnak, amelyek megelőzik az aláírást (beleértve a többi aláírást).

Figyelembe véve, hogy az ARAN az üzenetterjedési késleltetést (vagyis a fizikai időt) használja mint útvonalmetrikát, $C : V \rightarrow \mathbb{R}$ hozzárendeli minden csomópontához annak minimális késleltetését (azaz azt a minimális késleltetést, amit az adott csomópont okoz az üzenet terjedése során).

A korrekt állapotot, és így a biztonsági célfüggvényt hasonlóképpen definiáljuk mint ahogy azt az SAODV esetében tettük.

4. Tétel. *Az ARAN egy biztonságos távolságvektor alapú útvonalválasztó protokoll vezetéknélküli ad hoc hálózatokra, ha a felhasznált aláírás-séma biztonságos választott nyílt szövegű támadás ellen.*

A bizonyítást a disszertáció részletezi [C1]. Az ARAN-nal szemben az SAODV [Zapata and Asokan, 2002] nem biztonságos ebben a modellben, mivel az SAODV nem biztosítja a szomszédok hitelességét. Ez mutatja, hogy a modellem képes különbséget tenni távolságvektor alapú útvonalválasztó protokollok között biztonság szempontjából. Az analízis egyik konklúziója, hogy a forrás és cél hitelessége nem elégséges ahhoz, hogy egy protokoll biztonságos legyen a modellemben.

6. TÉZIS. *[C3] Adaptálom az 1. tézisben javasolt általános biztonsági modellt kapcsolatállapot alapú útvonalválasztásra vezetéknélküli szenzor hálózatokban, és bebizonyítom, hogy az INSENS [Deng et al., 2002] egy biztonságos útvonalválasztó protokoll egy olyan biztonsági célfüggvényt tekintve, amely megköveteli, hogy*

- *ha egy v becsületes csomópont beállít egy másik v' csomópontot mint szülőt, akkor a bázisállomás valóban v' -t számolta v szülőjének,*
- *ha a bázisállomás szerint két csomópont szomszédos, akkor azok vagy közvetlen vagy álszomszédok.*

Az INSENS egy biztonságos kapcsolatállapot alapú útvonalválasztó protokoll szenzor hálózatokra. Először a bázis kezdeményezi az útvonalválasztási topológia felépülését úgy, hogy elárasztja a hálózatot egy kéréssel (1. fázis). Ezután minden csomópont összeállítja a saját szomszédossági listáját azáltal, hogy áthallja a szomszédoktól kérést. Majd minden csomópont visszaküldi a saját szomszédossági listáját a bázisnak azon az útvonalon, amelyen a kérést kapták (2. fázis). Ezután a bázis kiszámolja minden egyes csomópontnak az útvonalirányító tábláját, és szétküldi azt minden egyes csomópontnak egy szélességi fa bejárással (3. fázis). Az INSENS protokoll szimmetrikus kulcsú kriptográfiát (MAC) használ a hitelesség és integritás biztosításához (minden csomópont megoszt egy titkos kulcsot a bázissal). A MAC-ek használata mellett minden csomópont rejtjelezi a bázisnak küldött topológia információt.

Az INSENS működését és üzeneteit szemlélteti a 3. ábra. Először a v_0 bázis kezdeményezi az útvonalválasztási topológia felépítését azáltal, hogy elárasztja a hálózatot egy kérés üzenettel (1. fázis), ahol `hash` a következő eleme a hash láncnak. A hash lánc használatának célja a bázis hitelességének biztosítása, valamint néhány DoS jellegű támadás megakadályozása. Minden csomópont képes összeállítani a saját szomszédossági listáját a kérés áthallása miatt. Minden v_{ℓ_i} csomópont, amely megkapja a kérést lokálisan eltárolja $MAC_{v_{\ell_{i-1}}}^{REQ}$ -et és $v_{\ell_{i-1}}$ azonosítóját. Mielőtt továbbküldené a kérést, v_{ℓ_i} kicseréli a kérésben $MAC_{v_{\ell_{i-1}}}^{REQ}$ -et $MAC_{v_{\ell_i}}^{REQ}$ -re, amelyet a MAC-et megelőző elemeken generálnak. Ha egy v_{ℓ_x} csomópont nem kap több kérést meghatározott ideig, akkor elküldi a saját szomszédossági listáját $v_{\ell_{x-1}}$ -nek, akitől az első hiteles kérést kapta (2. fázis). Itt $Enc_{v_{\ell_x}}(path_{v_{\ell_x}}, neighborlist_{v_{\ell_x}})$ jelöli v_{ℓ_x} szomszédossági listáját és az útvonalat amin a kérés érkezett rejtjelezve a megfelelő szimmetrikus kulccsal; $neighborlist_{v_{\ell_x}}$ tartalmazza minden szomszéd azonosítóját és a MAC értéküket amit az 1. fázisban kaptak, $path_{v_{\ell_x}}$ jelöli $[v_{\ell_x}, \dots, v_{\ell_1}, v_0, MAC_{v_{\ell_x}}^{REQ}]$ -t, ami annak az útnak a megfordítása

amin az első hiteles kérés érkezett beleértve v_x MAC értékét, valamint $\text{MAC}_{v_{\ell_x}}^{\text{NLIST}}$ a v_{ℓ_x} által számolt MAC mindezek az elemeken. Amikor a bázis megkapja a szomszédossági listát minden csomóponttól kiszámolja minden csomópont útvonalirányító tábláját, majd ezt szétosztja a hálózatban egy szélességi fa bejárással (3. fázis). $\text{Enc}_{v_{\ell_1}}(\text{ftable}_{v_{\ell_1}})$ jelöli v_{ℓ_1} csomópont útvonalirányító tábláját rejtjelezett formában, és $\text{MAC}_{v_{\ell_1}}^{\text{FTABLE}}$ jelöli a MAC-et amit a bázis számol az üzenet elemein.

Phase 1:	
$v_0 \rightarrow *$: (REQ, hash, $[v_0]$)
$v_{\ell_i} \rightarrow *$: (REQ, hash, $[v_0, \dots, v_{\ell_{i-1}}, v_{\ell_i}]$, $\text{MAC}_{v_{\ell_i}}^{\text{REQ}}$)
Phase 2:	
$v_{\ell_x} \rightarrow v_{\ell_{x-1}}$: (NLIST, hash, $\text{MAC}_{v_{\ell_{x-1}}}^{\text{REQ}}$, v_{ℓ_x} , $\text{Enc}_{v_{\ell_x}}(\text{path}_{v_{\ell_x}}, \text{neighborlist}_{v_{\ell_x}})$, $\text{MAC}_{v_{\ell_x}}^{\text{NLIST}}$)
Phase 3:	
$v_0 \rightarrow v_{\ell_1}$: (FTABLE, v_{ℓ_1} , hash, $\text{Enc}_{v_{\ell_1}}(\text{ftable}_{v_{\ell_1}})$, $\text{MAC}_{v_{\ell_1}}^{\text{FTABLE}}$)

4. táblázat. The operation and messages of INSENS.

Az 2.. tételhez hasonlóan a rendszert egy adott *conf* konfiguráció esetén egy $(k+1) \times (k+2)$ méretű T^{conf} mátrixszal reprezentáljuk, amit útvonalválasztási topológiának hívunk. A következőkben T^{conf} *conf* indexét nem jelölöm, ha a konfiguráció esetén egy adott kontextusban az egyértelműen meghatározható.

Megmutatom, hogy az INSENS rendelkezik a következő tulajdonságokkal:

1. Ha egy v_i ($1 \leq i \leq k$) becsületes csomópont beállítja $v_j \in V$ ($0 \leq j \leq n-1$) csomópontot szülőként adattovábbítás céljából, akkor a bázis valóban v_j -t számolta ki v_i szülőjének.
2. Ha a bázis szerint v_j és v_i szomszédok, akkor azok közvetlen vagy álszomszédok.

Intuitíve ha az INSENS rendelkezik ezzel a két tulajdonsággal, akkor ha egy becsületes csomópont rendelkezik egy szomszédos szülő csomóponttal, akkor azt a bázis számolta ki neki. Ráadásul az is garantált, hogy a bázis ezt a számítást talán nem teljes (a támadó mindig képes eldobni olyan üzeneteket amely szomszédossági listát tartalmaznak, ami ellen nem tudunk védekezni), de mindig korrekt szomszédossági információk alapján végzi.

Ahhoz, hogy formalizáljuk a fenti biztonsági célt, bevezetjük a \mathcal{G} mátrix-függvényt. \mathcal{G} modellezi azt a centralizált topológia számítást, ahol a paraméter egy $(k+1) \times (k+2)$ méretű \mathbf{N} mátrix, amely a bázis helyesnek vélt szomszédossági relációkat leíró mátrixot jelöli (vagyis $N_{i,j} = 1$ ha a bázis szerint v_i az v_j szomszédja, egyébként $N_{i,j} = 0$. Bármely $0 \leq i \leq k$ esetén $N_{i,k+1} = 1$, ha v_i becsületes csomópontnak van legalább egy olyan szomszédja, aki támadó csomópont, máskülönben $N_{i,k+1} = 0$). \mathcal{G} kimenete azon útvonalbejegyzések összessége (vagyis az útvonalválasztási topológia), amelyeket az egyes csomópontoknak kell beállítani a saját útvonalirányítási táblájukban.

6. Definíció (Korrekt útvonalválasztási topológia). Egy \mathbf{T} útvonalválasztási topológia korrekt *conf* konfigurációt tekintve, ha létezik \mathbf{E}' mátrix úgy, hogy minden i, j estén teljesül, hogy ha $T_{i,j} = 1$, akkor $\mathcal{G}(\mathbf{E}')_{i,j} = 1$, ahol $(k+1) \times (k+2)$ méretű \mathbf{E}' mátrixot \mathbf{E} mátrixból származtatjuk a következőképpen. Minden $0 \leq i, j \leq k$ esetén $E'_{i,j} = 0$, ha v_i és v_j nem közvetlen és nem is álszomszédok. Minden $0 \leq i \leq k$ esetén $E'_{i,k+1} = 0$, ha v_i nem rendelkezik támadó szomszédal.

A biztonságos kapcsolatállapot alapú útvonalválasztás biztonsági célfüggvénye legyen 0 minden olyan rendszerállapot és konfiguráció párra, ahol a rendszerállapot (azaz az útvonalválasztási topológia) inkorrekt. Máskülönben \mathcal{F} legyen 1.

5. Tétel. *Az INSENS egy biztonságos kapcsolatállapot alapú útvonalválasztó protokoll vezetéknélküli szenzorhálózatokra, ha a MAC séma biztonságos választott nyílt szövegű támadás ellen, és a rejtjelező séma biztonságos üzenetvissafejtő támadással szemben.*

A bizonyítás, amelyet a disszertáció részletez, erősen függ attól, hogy az INSENS rejtjelezi a lokális topológia információt. A rejtjelezés használata ebben az esetben alapvető fontossággal bír: amellet, hogy a szomszédossági relációk bizalmasságát nyújtja, megakadályozza, hogy a támadó olyan becsületes csomópontokat személyesítsen meg, amelyeknek nincs támadó szomszédjuk. Például, ha nem alkalmaznánk rejtjelezést, akkor egy közbenső támadó csomópont könnyen megszerezhetné a szükséges azonosítókat és MAC^{REQ} értékeket az NLIST üzenetekből ahhoz, hogy összeállítson és szétküldjön fabrikált REQ üzeneteket. Fontos megjegyezni, hogy a támadónak nem kell szomszédossági viszonyban állnia a megszemélyesítendő csomóponttal. Ez nyilvánvalóan megsértené a fentebb már részletezett biztonsági célfüggvényt, mivel a támadó eléri, hogy a bázis hamis szomszédossági relációk alapján számolja ki az útvonalválasztási topológiát. Továbbá mivel a MAC^{REQ} értékek korrektek, megeshet, hogy sem a támadó szomszédai sem a bázis nem fogja a támadást detektálni. A formális analízisem így a következő megfigyeléshez vezetett: kapcsolatállapot alapú útvonalválasztás esetén minden csomópontnak rejtjelezve kell küldeni más távoli csomópontoknak a helyi szomszédossági információkat.

7. TÉZIS. [J6] *Javaslok egy új biztonságos decentralizált címkekapcsolás alapú útvonalválasztó protokollt, amit Secure-TinyLUNAR-nak nevezek, és a TinyLUNAR [Osipov, 2007] biztonságos változata vezeték nélküli szenzorhálózatokra. Címkekapcsolást és kizárólag hatékony szimmetrikus kriptográfiát használva a Secure-TinyLUNAR hatékonyabb vezeték nélküli szenzorhálózatokban mint a létező biztonságos ad hoc útvonalválasztó protokollok (pl. az ARAN [Sanzgiri et al., 2002]). Adaptálom az 1. tézisben javasolt általános modellt címkekapcsolás alapú útvonalválasztásra vezeték nélküli szenzorhálózatokban, és bebizonyítom, hogy a Secure-TinyLUNAR biztonságos egy olyan biztonsági célfüggvényt illetően, amely megköveteli, hogy ha egy forrás csomópont rendelkezik egy útvonalválasztási bejegyzéssel egy célcsoomópont felé, akkor létezik olyan útvonal a hálózatban, amely*

- *a forráscsoomóponttól indul,*
- *a célcsoomópontig tart,*
- *késleltetése nem nagyobb mint a bejegyzésben található késleltetés, és*
- *minden v, v' egymást követő becsületes csomópontnak van rendre olyan r, r' bejegyzése, hogy az r bejegyzés következő hop címe és kimenő címkéje megegyezik rendre v' azonosítójával és az r' bemenő címkéjével, ha v és v' közvetlen de nem álszomszédok. Ha v és v' álszomszédok, akkor vagy az r következő hop címe és kimenő címkéje egyezik meg rendre v' azonosítójával ill. r' kimenő címkéjével, vagy v' egy támadó csomópont. Ha v' a cél, akkor r' kimenő címkéje egy alkalmazás-azonosító.*

Figyelembe véve a szenzor alkalmazások változatosságát világos, hogy nem lehet egy univerzális biztonságos útvonalválasztó protokollt javasolni minden alkalmazásra. Egy alternatív megoldás lehet valamely biztonságos ad hoc útvonalválasztó protokoll, mint pl. [Zapata and Asokan, 2002], [Sanzgiri et al., 2002], [Hu et al., 2002] alkalmazása, viszont ezen protokollokat nem alacsony energiafogyasztású szenzor-eszközökre tervezték, hiszen az alkalmazott aszimmetrikus kriptográfiai primitívek jelentős kommunikációs és számítási költségeket indukálhatnak. Ezért tervezek egy új biztonságos útvonalválasztó protokollt vezeték nélküli szenzorhálózatokra, amelyek figyelembe veszik a szenzorok erőforráskorlátait, és kizárólag MAC-et használnak az útvonalfelderítést során. A címkekapcsolás alapú paradigma miatt minden csomópontnak csak egy byte címzési többletköltsége van az adattovábbítás során, így téve hatékonyá a protokollt relatíve statikus hálózatokban.

A TinyLUNAR [Osipov, 2007]-hoz hasonlóan minden csomópont rendelkezik egy egyedi azonosítóval, és minden csomópont között a link kétirányú. Feltesszük, hogy minden csomópontpár a hálózatban megoszt egymással egy szimmetrikus kulcsot, amely célra bármely az irodalomban korábban szenzorhálózatokra javasolt kulcskiosztási protokoll (ld. [Çamtepe and Yener, 2005]) használható. Minden csomópontról feltételezzük továbbá, hogy ismeri a közvetlen szomszédait.

A következőkben csak a főbb működési különbségeket írom le az eredeti (és nem biztonságos) TinyLUNAR [Osipov, 2007] protokollhoz képest.

Route request: Jelöljük A szomszédait N_x^A -val, ahol x értéke 1 és A szomszédainak száma között változik (pl., ha A -nak szomszédai J, T, P , akkor egy potenciális jelölés lehet $N_1^A = J, N_2^A = T, N_3^A = P$, ahol $1 \leq x \leq 3$)

Amikor egy S csomópont csomagot kíván küldeni D csomópontnak elküldi azt minden szomszédjának többesküldéssel:

$$S \rightarrow * : (\text{RREQ}, \text{rnd}, S, D, \text{addr}_S, \text{label}_{S \rightarrow S}^{\text{In}}, \text{MAC}_{S,D})$$

ahol $\text{rnd}, S, D, \text{addr}_S, \text{label}_{S \rightarrow S}^{\text{In}}$ mezők jelentése ugyanaz mint az eredeti TinyLUNAR protokoll esetében, $\text{MAC}_{S,D}$ pedig az üzenethitelesítő kód amit S generál az üzenet többi elemén kivéve addr_S és $\text{label}_{S \rightarrow S}^{\text{In}}$ mezőket felhasználva a D -vel megosztott közös szimmetrikus kulcsot. Ezen broadcast üzenet vétele során egy szomszédos J csomópont ellenőrzi, hogy S valóban szomszédja. Ha igen, akkor J csomópont unicast módon továbbküldi a következő üzenetet minden egyes szomszédnak kivéve azt, amelytől J a kérést kapta (jelen esetben S):

$$\text{minden olyan } x\text{-re, amelyre } N_x^J \neq S, J \rightarrow N_x^J : (\text{RREQ}, \text{rnd}, S, D, \text{addr}_J, \text{label}_{J \rightarrow S}^{\text{In}}, \text{MAC}_{S,D}, \text{MAC}_{J,N_x^J}^{\text{prv}})$$

ahol $\text{MAC}_{J,N_x^J}^{\text{prv}}$ az előző hop MAC, amelyet minden elem generálnak felhasználva a J és N_x^J között megosztott kulcsot. S minden szomszédja és minden azt követő csomópont egy kérés vétele során ugyanazokat a lépéseket hajtja végre amiket korábban J (kivéve, hogy az előző hop által számolt MAC-et frissítik a sajátjukkal). Végül a kérés eléri D -t, tegyük fel, hogy Z -n mint utolsó hopon keresztül.

A kérés terjedés során feltesszük, hogy minden csomópont atomi és unicast módon küldi tovább a kérést a közvetlen szomszédainak (vagyis a küldő addig nem engedi el a csatornát, amíg minden kérést el nem küldött a szomszédainak), és a szomszédos csomópontok addig nem kezdik el továbbítani a kérést amíg a küldő minden szomszédja azt meg nem kapta.

Route reply: A kérés vétele során D ellenőrzi $\text{MAC}_{S,D}$ és $\text{MAC}_{Z,D}^{\text{prv}}$ hitelesítő kódokat. Ha az ellenőrzés sikeres, akkor D létrehozza a következő választ, amelyet elküld Z -nek:

$$D \rightarrow Z : (\text{RREP}, \text{rnd}, \text{addr}_D, \text{label}_{Z \rightarrow S}^{\text{Out}}, \text{label}_{D \rightarrow D}^{\text{In}}, \text{MAC}_{D,S})$$

ahol rnd a kérés azonosítója amit a megfelelő kérésben kapott, $\text{MAC}_{D,S}$ a D által a fenti üzenet elemein generált üzenethitelesítő kód kivéve a $\text{addr}_D, \text{label}_{Z \rightarrow S}^{\text{Out}}$ és $\text{label}_{D \rightarrow D}^{\text{In}}$ elemeket felhasználva az S -sel megosztott közös kulcsot. Véve ezt az unicast üzenete, Z először ellenőrzi, hogy D valóban szomszédja-e. Ha igen, akkor Z hozzáfűzi $\text{MAC}_{Z,K}^{\text{prv}}$ -t az üzenethez, és elküldi az így kapott üzenetet közvetlenül K -nak akitől Z az rnd azonosítójú kérést kapta:

$$Z \rightarrow K : (\text{RREP}, \text{rnd}, \text{addr}_Z, \text{label}_{K \rightarrow S}^{\text{Out}}, \text{label}_{Z \rightarrow D}^{\text{In}}, \text{MAC}_{D,S}, \text{MAC}_{Z,K}^{\text{prv}})$$

Itt $\text{MAC}_{Z,K}^{\text{prv}}$ az előző hop MAC, amelyet Z generál az üzenet elemein beleértve $\text{addr}_Z, \text{label}_{K \rightarrow S}^{\text{Out}}$ és $\text{label}_{Z \rightarrow D}^{\text{In}}$ elemeket. Ugyanezen szabályokat követve minden közbenső csomópont ugyanazokat a lépéseket teszi amit Z (kivéve, hogy az előző hop által számolt MAC-et frissítik a sajátjukkal). Végezetül a válasz eléri S forrást, aki miután ellenőrizte az előző hop MAC-et és $\text{MAC}_{D,S}$ -t a válasz üzenetben használhatja a kiépített útvonalat adattovábbításra.

Az ok amiért nem használok digitális aláírást a kérés és válasz üzenetek hitelesítésére az, hogy a publikus kulcsú kriptográfia (PKC) jelentős számítási többletterhelést indukál szenzorokon. A PKC még mindig elmarad a standard szimmetrikus kriptográfia mögött számítási költségek szempontjából: egy digitális aláírás ellenőrzése 3 nagyságrenddel lassabb mint egy MAC ellenőrzése, míg az aláírás generálás 4 nagyságrenddel lassabb.

$\mathcal{C} : V \rightarrow \mathbb{R}$ rendelje minden csomóponthoz azt a késleltetést, amit a csomópont okoz az üzenet továbbítása során. Tegyük fel, hogy $\mathcal{C}(v^*) = 0$ minden $v^* \in V^*$ -re.

Mielőtt definiálnám a címkekapcsolás alapú útvonalválasztás biztonsági célfüggvényét, bevezetek néhány definíciót a formalizmus megkönnyítése végett.

7. Definíció (Horgony bejegyzés). Egy $(v_{src}, v_{dst}, \text{addr}_{next}, \text{label}_{v_{src} \rightarrow v_{dst}}^{\text{Out}}, \text{delay}_{v_{src}, v_{dst}})$ horgony bejegyzés v_{src} csomópont egy útvonalválasztó bejegyzésének reprezentációja, ahol a célcso-
mópont azonosítója v_{dst} azonosítója, a következő hop lokális címe a cél felé addr_{next} , a forrás
kimenő címkéje a cél felé $\text{label}_{v_{src} \rightarrow v_{dst}}^{\text{Out}}$, és a leggyorsabb út késleltetése addr_{next} csomóponton
keresztül a cél felé $\text{delay}_{v_{src}, v_{dst}}$.

8. Definíció (Közbenső bejegyzés). Egy $(v_{im}, \text{addr}_{next}, \text{label}_{v_{im} \rightarrow v_{dst}}^{\text{In}}, \text{label}_{v_{im} \rightarrow v_{dst}}^{\text{Out}})$ közbenső
bejegyzés egy v_{im} közbenső csomópont útvonalválasztó bejegyzésének a reprezentációja, ahol a
következő hop lokális címe a cél felé addr_{next} , valamint v_{im} bemenő ill. kimenő címkéje a cél
felé rendre $\text{label}_{v_{im} \rightarrow v_{dst}}^{\text{In}}$ és $\text{label}_{v_{im} \rightarrow v_{dst}}^{\text{Out}}$.

9. Definíció (Illeszkedési tulajdonság). v_i egy r_1 útvonalválasztó bejegyzése illeszkedik v_j
($i \neq j$) egy r_2 bejegyzéséhez, ha

- r_1 kimenő címkéje megegyezik r_2 bemenő címkéjével,
- r_1 következő hop címét v_j használja.

Emlékeztetek arra, hogy a rendszer állapotát az összes becsületes csomópont horgony és
közbenső bejegyzéseinek az összessége adja.

10. Definíció (Korrekt állapot). Egy állapot korrekt egy conf konfigurációt tekintve, ha
minden $r_0 = (v_{src}, v_{dst}, \text{addr}_{next}, \text{label}_{v_{src} \rightarrow v_{dst}}^{\text{Out}}, \text{delay}_{v_{src}, v_{dst}})$ horgony bejegyzésre, ahol $v_{src}, v_{dst} \in$
 $V \setminus V^*$, létezik becsületes csomópontok közbenső bejegyzéseinek egy $r_i = (v_{\ell_i}, \text{addr}_{next}, \text{label}_{v_{\ell_i} \rightarrow v_{dst}}^{\text{In}}, \text{label}_{v_{\ell_i} \rightarrow v_{dst}}^{\text{Out}})$
($1 \leq i \leq d$) olyan sorozata, hogy

- $v_{\ell_d} = v_{dst}$ és $\text{label}_{v_{\ell_d} \rightarrow v_{dst}}^{\text{Out}}$ a v_{dst} csomópont egy alkalmazás azonosítója,
- $(v_{src}, v_{\ell_1}, \dots, v_{\ell_{d-1}}, v_{dst})$ egy működő út,
- legyen $v_{\ell_0} = v_{src}$,
 - ha $v_{\ell_{i-1}}$ és v_{ℓ_i} közvetlen de nem álszomszédok, akkor r_{i-1} illeszkedik r_i -hez,
 - ha $v_{\ell_{i-1}}$ és v_{ℓ_i} álszomszédok, akkor vagy r_{i-1} illeszkedik r_i -hez, vagy r_{i-1} következő
hop címe egy szomszédos támadó csomóponthoz tartozik,
- $\sum_{j=1}^{d-1} \mathcal{C}(v_{\ell_j}) \leq \text{delay}_{v_{src}, v_{dst}}$ (vagyis a v_{src} és v_{dst} között felfedezett útvonal késleltetése
nem nagyobb mint az a késleltetés amit v_{src} megfelelő horgony bejegyzése tartalmaz)

A címkekapcsolás alapú útvonalválasztás \mathcal{F} biztonsági célfüggvénye rendeljen 0-t minden
olyan rendszerállapot és konfiguráció párhoz, amely inkorrekt. Máskülönben legyen \mathcal{F} értéke
1.

6. Tétel. A *Secure-TinyLUNAR* egy biztonságos címkekapcsolás alapú útvonalválasztó pro-
tokoll vezeték nélküli szenzorhálózatokra, ha a MAC séma biztonságos választott nyílt szövegyű
támadás ellen.

A bizonyítást a disszertáció részletezi. Fontos megjegyezni, hogy a közbenső csomópontoknak nem szükséges ellenőrizni a forrás és cél hitelességét, ami azt is jelenti, hogy nem szükséges drága aszimmetrikus kriptográfián alapuló broadcast hitelesítő eljárások használata. Ehelyett a Secure-TinyLUNAR a hatékonyabb szimmetrikus kriptográfián alapuló páronkénti MAC-eket használja az előző hop hitelesítésére. Természetesen a globális broadcast hitelesítés hiánya sérülékennyé teszi a protokollt különböző DoS támadások ellen. Viszont ebben az esetben erre a célra egy egyirányú hash lánc használata már elégséges. Ráadásul a hash láncok számítási és kommunikációs költsége jóval kevesebb mint más broadcast hitelesítő eljárásoké mint pl. a digitális aláírás, egyszer használatos digitális aláírás, vagy a μ Tesla [B1].

5. Az eredmények alkalmazása

A munkám gyakorlati haszna kétirányú:

- Javasoltam egy precíz és általános formális keretrendszert, amely hasznosnak bizonyult különböző biztonsági célok validálásában vezeték nélküli ad hoc és szenzor hálózatokra javasolt útvonalválasztó protokollok esetén. Ugyan a validálási folyamat még nem automatizált, egy protokoll-tervező könnyen bebizonyíthatja bármely többugrásos útvonalválasztó protokoll biztonságát vezeték nélküli környezetben a javasolt bizonyítási technikát használva. Ha a protokoll nem biztonságos, akkor a tervező konstruálhat egy támadást ha megkeresi, hogy hol akadt el a bizonyítás.
- Azonosítottam a biztonságos útvonalválasztó protokollok több tervezési elvét azáltal, hogy több protokollnak bizonyítottam a biztonságát. Például ezen elvek magukba foglalják a válasz üzenetek hitelesítést forrás alapú útvonalválasztásnál, a hoponkénti hitelesítést dinamikus távolságvektor alapú útvonalválasztás esetén, vagy a lokális topológia információ rejtjelezését kapcsolatállapot alapú útvonalválasztás esetén. Még ha egy protokoll-tervező nem is validálja egy újonnan javasolt protokoll biztonságát formálisan, ezen elveket követve számos potenciális támadást elkerülhet, amelyeket egyébként informális érvelést használva nehéz felfedezni.

Néhány eredményem felhasználásra került a UbiSec&Sens (Ubiquitous Sensing and Security in the European Homeland, <http://www.ist-ubisecsens.org/>) nevű kutatási projektben 2005 és 2008 között. A projekt egy IST STReP és a kutatást az Európai Közösség hatodik Framework Programme keretében finanszírozta. A UbiSec&Sens elsődleges célja egy biztonságos és megbízható architektúra létrehozása volt közepes és nagy méretű vezeték nélküli szenzorhálózatokra, amely magába foglalta a biztonság és megbízhatóság központú komponensek teljes eszközkészletének tervezését és implementációját. A UbiSec&Sens tevékenysége a biztonság, útvonalválasztás és hálózati feldolgozás metszetére fókuszált. Célja volt, hogy hatékony biztonsági megoldásokat tervezzen és fejlesszen, valamint perzisztens és rejtjelezett elosztott adattárolásra alkalmas módszereket javasoljon. A megoldásokra prototípusok készültek, amiket reprezentatív vezeték nélküli szenzoralkalmazásokban validáltak a mezőgazdaság, közlekedési szolgáltatások, és személyi biztonság területén.

A WSA4CIP (Wireless Sensor and Actuator Networks for Critical Infrastructure Protection, <http://www.wsan4cip.eu/>) egy másik európai kutatási projekt ami a kritikus infrastruktúrák biztonságára fókuszál. A projekt szintén egy IST STReP ami 2009-ben kezdődött és 3 évig tart, valamint az Európai Közösség finanszírozza a hetedik Framework Program keretében. A projekt célja a kritikus infrastruktúrák megbízhatóságának javítása felügyeleti adatok

szolgáltatásával vezeték nélküli szenzor és beavatkozó hálózatok (WSANs) használatával, valamint növelni a kritikus infrastruktúrák védelmének robusztusságát különböző biztonsági és megbízhatósági modulok fejlesztésével WSAN-ok számára. A projekt célja az is, hogy megfelelő támogatóeszközöket fejlesszen ki és demonstrálja a megközelítés megvalósíthatóságát reprezentatív kritikus infrastruktúrákon mint pl. az energia elosztó hálózaton. Mint ilyen, a projekt célja olyan modellek kifejlesztése, amelyben az útvonalválasztó protokollok analízálhatóak mind megelőzés mind reakció szempontjából. A megelőzés természetesen magába foglalja az útvonalfelderítés biztonságának validálását, ami a disszertáció központi témája.

Publikációk

Könyvfejezet

- [B1] G. Ács and L. Buttyán,
Secure Routing in Wireless Sensor Networks,
Wireless Sensor Network Security (Cryptography and Information Security Series),
Eds. J. Lopez and J. Zhou, ISBN: 978-1-58603-813-7, pages 154–203, IOS Press, 2008.

Folyóirat cikkek

- [J1] G. Ács and L. Buttyán,
Ad hoc útvonalválasztó protokollok bizonyított biztonsága,
Híradástechnika, 60(3):41–45, March 2005.
- [J2] G. Ács and L. Buttyán,
Provable Security for Ad Hoc Routing Protocols,
Híradástechnika (English Edition), 60(6):34–38, June 2005.
- [J3] G. Ács and L. Buttyán and I. Vajda,
Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks,
IEEE Transactions on Mobile Computing, 5(11):1533–1544, 2006.
- [J4] G. Ács and L. Buttyán,
Útvonalválasztó protokollok vezetékek nélküli szenzorhálózatokban,
Híradástechnika, 61(12):3–12, December 2006.
- [J5] G. Ács and L. Buttyán,
A taxonomy of routing protocols for wireless sensor networks,
Híradástechnika (English Edition), 62(1):32–41, January 2007.
- [J6] G. Ács and L. Buttyán,
Designing a Secure Label-switching Routing Protocol for Wireless Sensor Networks,
To appear in Periodica Polytechnica (<http://www.pp.bme.hu/>), December, 2008.

Nemzetközi konferencia és workshop cikkek

- [C1] G. Ács and L. Buttyán and I. Vajda,
Provable Security of On-Demand Distance Vector Routing in Wireless Ad Hoc Networks,
In Proceedings of the Second European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS), pages 113–127, Visegrád, Hungary, July 2005.

- [C2] G. Ács and L. Buttyán and I. Vajda,
Modelling Adversaries and Security Objectives for Routing Protocols in Wireless Sensor Networks,
In Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), pages 49–58, Alexandria, VA, USA, October 2006.
- [C3] G. Ács and L. Buttyán and I. Vajda,
The Security Proof of a Link-state Routing Protocol for Wireless Sensor Networks,
In Proceedings of the 3rd IEEE Workshop on Wireless and Sensor Networks Security (WSNS), pages 1–6, Pisa, Italy, October 2007.

Hivatkozások a publikációimra

- [J3] G. Ács and L. Buttyán and I. Vajda,
Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks,
IEEE Transactions on Mobile Computing, 5(11):1533–1544, 2006.

cikkre hivatkoznak:

1. T. R. Andel,
Formal Security Evaluation of Ad-Hoc Routing Protocols,
PhD Dissertation, Florida State University, College of Arts and Sciences, 2007.
2. W. J. Tsaur, P. Haw-Tyng,
A new security scheme for on-demand source routing in mobile ad hoc networks,
In Proceedings of the International conference on Wireless communications and mobile computing (IWCMC), pp 577–582, 2007.
3. W. Tsaur, H. Pai,
A Secure On-Demand Source Routing Scheme Using Hierarchical Clustering in Mobile Ad Hoc Networks,
In Lecture Notes in Computer Science 4743: 513, Springer, 2007.
4. K. El-Defrawy, G. Tsudik,
ALARM: Anonymous Location-Aided Routing in Suspicious MANETs,
In Proceedings of the IEEE International Conference on Network Protocols (ICNP), pages 304–313, 2007.
5. S. Chakrabarti, S. Chandrasekhar, M. Singhal, K. Calvert
Authenticating DSR Using a Novel Multisignature Scheme Based on Cubic LFSR Sequences,
In Proceedings of The Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS), pages 156–171, 2007.
6. M. Burmester, B. de Medeiros,
On the Security of Route Discovery in MANETs,
To appear in IEEE Transactions on Mobile Computing, 2009.
7. T. R. Andel, A. Yasinsac,
Automated Security Analysis of Ad Hoc Routing Protocols
In Proceedings of the Workshop on Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis, 2007.
8. J. van der Merwe, D. Dawoud, S. McDonald,
Key Distribution in Mobile Ad Hoc Networks Based on Message Relaying,
In Proceedings of The Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS), pages 87–100, 2007.
9. X. Su, R. V. Boppana,
On identifying malicious nodes in ad hoc networks,
In Proceedings of the International Conference on Wireless Communications and Mobile Computing, pages 254–259, 2007.

10. D. Djenouri, O. Mahmoudi, M. Bouamama, D. Llewellyn-Jones, M. Merabti,
On Securing MANET Routing Protocol Against Control Packet Dropping,
In Proceedings of the IEEE International Conference on Pervasive Services (ICPS),
pages 100–108, 2007.
11. R.V. Boppana, X. Su,
Secure Routing Techniques to Mitigate Insider Attacks in Wireless Ad Hoc Networks,
In Proceedings of the IEEE Wireless Hive Networks Symposium, 2007.
12. T. R. Andel, A. Yasinsac,
Surveying security analysis techniques in manet routing protocols,
In IEEE Communications Surveys & Tutorials 9: (4) 70–84, 2007.
13. T. R. Andel, A. Yasinsac,
Adaptive Threat Modeling for Secure Ad Hoc Routing Protocols,
In Proceedings of the 3rd International Workshop on Security and Trust Management (STM), pages 3–14, 2008.
14. X. Su, R. V. Boppana,
Crosscheck mechanism to identify malicious nodes in ad hoc networks,
In Security and Communication Networks, John Wiley & Sons Ltd., 2: (1) 45-54,
2008.
15. A. König, M. Hollick, T. Krop, R. Steinmetz,
GeoSec: quarantine zones for mobile ad hoc networks,
In Security and Communication Networks, John Wiley & Sons Ltd., 2008.
16. X. Su, R. V. Boppana,
Mitigation of colluding route falsification attacks by insider nodes in mobile ad hoc networks,
Wireless Communications and Mobile Computing, John Wiley & Sons Ltd., 2008.
17. K. El-Defrawy, G. Tsudik,
PRISM: Privacy-friendly routing in suspicious MANETs (and VANETs),
In Proceedings of the IEEE International Conference on Network Protocols (ICNP),
pages 258–267, 2008.
18. M. Fanaei, M. Berenjkoub, A. Fanian,
Resistant TIK-Based endairA Against the Tunneling Attack,
In Proceedings of the 10th International Conference on Advanced Communication
Technology, pages 1461–1466, 2008.
19. Q. Li, Y.-C. Hu, M. Zhao, A. Perrig, J. Walker, W. Trappe,
SEAR: a secure efficient ad hoc on demand routing protocol for wireless networks,
In Proceedings of the ASIAN ACM Symposium on Information, Computer and
Communications Security (ASIA CCS), pages 201–204, 2008.
20. M. Poturalski, P. Papadimitratos, J.-P. Hubaux,
Secure neighbor discovery in wireless networks: formal investigation of possibility,
In Proceedings of the ASIAN ACM Symposium on Information, Computer and
Communications Security (ASIA CCS), pages 189–200, 2008.

21. J. Kim, G. Tsudik,
SRDP: Secure route discovery for dynamic source routing in MANETs,
In Elsevier Ad Hoc Networks, 2008.
22. S. Eidenbenz, G. Resta, P. Santi
The Commit protocol for truthful and cost-efficient routing in ad hoc networks with selfish nodes,
In IEEE Transactions on Mobile Computing 7: (1) 19–33, 2008.
23. M. Poturalski, P. Papadimitratos, J.-P. Hubaux,
Towards provable secure neighbor discovery in wireless networks,
In Proceedings of the ACM Workshop on Formal Methods in Security Engineering (FMSE), pages 31–42, 2008.
24. M. Moe, B. E. Helvik, S. J. Knapskog,
TSR: trust-based secure MANET routing using HMMs,
In Proceedings of the 4th ACM Symposium on QoS and Security for Wireless and Mobile Networks, pages 83–90, 2008.
25. Y. Ren, A. Boukerche,
ARMA: a scalable secure routing protocol with privacy protection for mobile ad hoc networks,
Wireless Communications and Mobile Computing, John Wiley & Sons Ltd., 2009.
26. F. Mohammad, M. Berenjkoub,
Prevention of Tunneling Attack in endairA,
In Proceedings of the Advances in Computer Science and Engineering, Communications in Computer and Information Science (ACSE), pages 994–999, 2009.

[J5] G. Ács and L. Buttyán,
A taxonomy of routing protocols for wireless sensor networks,
Híradástechnika (English Edition), 62(1):32–41, January 2007.

cikkre hivatkoznak:

1. E. Osipov,
tinyLUNAR: One-Byte Multihop Communications Through Hybrid Routing in Wireless Sensor Networks,
In Proceedings of the Next Generation Teletraffic and Wired/Wireless Advanced Networking, pages 379–392, 2007.

[C1] G. Ács and L. Buttyán and I. Vajda,
Provable Security of On-Demand Distance Vector Routing in Wireless Ad Hoc Networks,
In Proceedings of the Second European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS), pages 113–127, Visegrád, Hungary, July 2005.

cikkre hivatkoznak:

1. J. Kong, X. Hong, M. Gerla,
Modeling Ad-hoc rushing attack in a negligibility-based security framework,

- In Proceedings of the 5th ACM Workshop on Wireless Security (WiSe), pages 55–64, 2006.
2. M. Wen, L. Dong, Y. Zheng, K. Chen,
A Framework for Proving the Security of Data Transmission Protocols in Sensor Network,
In Lecture Notes in Computer Science, Intelligence and Security Informatics: 288–294, 2007.
 3. X. Su, R. V. Boppana,
On identifying malicious nodes in ad hoc networks,
In Proceedings of the International Conference on Wireless Communications and Mobile Computing, pages 254–259, 2007.
 4. J. Eriksson, M. Faloutsos, S. V. Krishnamurthy,
Routing amid Colluding Attackers,
In Proceedings of the IEEE International Conference on Network Protocols, pages 184–193, 2007.
 5. X. Su, R. V. Boppana,
Crosscheck mechanism to identify malicious nodes in ad hoc networks,
In Security and Communication Networks, John Wiley & Sons, 2: (1) 45-54, 2008.
 6. M. Burmester, B. de Medeiros,
On the Security of Route Discovery in MANETs,
To appear in IEEE Transactions on Mobile Computing, 2009.
- [C2] G. Ács and L. Buttyán and I. Vajda,
Modelling Adversaries and Security Objectives for Routing Protocols in Wireless Sensor Networks,
In Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), pages 49–58, Alexandria, VA, USA, October 2006.
- cikkre hivatkoznak:*
1. W. Wei-ping, C. Liang, W. Jian-xin,
A Source-Location Privacy Protocol in WSN Based on Locational Angle,
In Proceedings of the IEEE International Conference on Communications (ICC), pages 1630–1634, 2008.
 2. M. Burmester, B. de Medeiros,
On the Security of Route Discovery in MANETs,
To appear in IEEE Transactions on Mobile Computing, 2009.
- [C3] G. Ács and L. Buttyán and I. Vajda,
The Security Proof of a Link-state Routing Protocol for Wireless Sensor Networks,
In Proceedings of the 3rd IEEE Workshop on Wireless and Sensor Networks Security (WSNS), pages 1–6, Pisa, Italy, October 2007.

cikkre hivatkoznak:

1. L. Tobarra, D. Cazorla, F. Cuartero, J. Pardo,
Modelling secure wireless sensor networks routing protocols with timed automata,
In Proceedings of the 3rd ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks, pages 51–58, 2008.

Az összes ismert független hivatkozások száma 36.

Hivatkozások

- [Backes and Pfitzmann, 2004] M. Backes and B. Pfitzmann. A cryptographically sound security proof of the needham-schroeder-lowé public-key protocol. *IEEE Journal on Selected Areas of Computing (JSAC)*, 22(10):2075–2086, 2004.
- [Bellare *et al.*, 1998] M. Bellare, R. Canetti, and H. Krawczyk. A modular approach to the design and analysis of authentication and key exchange protocols. In *Proceedings of the ACM Symposium on the Theory of Computing*, 1998.
- [Bryan *et al.*, 2005] P. Bryan, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2005.
- [Burmester and de Medeiros, 2007] M. Burmester and B. de Medeiros. Towards provable security for route discovery protocols in mobile ad hoc networks, 2007.
- [Deng *et al.*, 2002] J. Deng, R. Han, and S. Mishra. INSENS: Intrusion-tolerant routing in wireless sensor networks. Technical Report CU-CS-939-02, Department of Computer Science, University of Colorado, 2002.
- [Dolev and Yao, 1981] D. Dolev and A. C. Yao. On the security of public key protocols. In *Proceedings of the IEEE 22nd Annual Symposium on Foundations of Computer Science*, pages 350–357, 1981.
- [Douceur, 2002] J. R. Douceur. The sybil attack. In *Proceedings of the International Workshop on Peer-to-Peer Systems (IPTPS)*, 2002.
- [Hill *et al.*, 2000] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister. System architecture directions for networked sensors. In *Proceedings of the International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, 2000.
- [Hu *et al.*, 2002] Y.-C. Hu, A. Perrig, and D. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In *Proceedings of ACM Conference on Mobile Computing and Networking (Mobicom)*, 2002.
- [Hu, 2003] Yih-chun Hu. Rushing attacks and defense in wireless ad hoc network routing protocols. In *Proceedings of ACM Workshop on Wireless Security (WiSe)*, pages 30–40, 2003.
- [Karlof and Wagner, 2003] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1, 2003.
- [Kim and Tsudik, 2005] J. Kim and G. Tsudik. Securing route discovery in dsr. In *Proceedings of the IEEE Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous)*, July 2005.
- [Mao, 2004] W. Mao. *Modern Cryptography: Theory and Practice*. Prentice Hall PTR, 2004.

- [Marshall, 2003] J. Marshall. An analysis of the secure routing protocol for mobile ad hoc network route discovery: using intuitive reasoning and formal verification to identify flaws. msc thesis, department of computer science, florida state university, 2003.
- [Osipov, 2007] E. Osipov. tinylunar: One-byte multihop communications through hybrid routing in wireless sensor networks. In *Proceedings of the 7th International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking (NEW2AN 2007)*, 2007.
- [Papadimitratos and Haas, 2002] P. Papadimitratos and Z. Haas. Secure routing for ad hoc networks. In *Proceedings of SCS Communication Networks and Distributed Systems Modeling Simulation Conf. (CNDIS)*, 2002.
- [Perkins and Royer, 1999] C. Perkins and E. Royer. Ad hoc on-demand distance vector routing. In *Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications*, 1999.
- [Perrig *et al.*, 2002] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar. SPINS: Security protocols for sensor networks. *Wireless Networks Journal (WINE)*, 8, 2002.
- [Pfitzman and Waidner, 2001a] B. Pfitzman and M. Waidner. A model for asynchronous reactive systems and its application to secure message transmission. In *Proceedings of the 22nd IEEE Symposium on Security & Privacy*, 2001.
- [Pfitzman and Waidner, 2001b] B. Pfitzman and M. Waidner. A model for asynchronous reactive systems and its application to secure message transmission. In *Proceedings of the 22nd IEEE Symposium on Security & Privacy*, 2001.
- [Sanzgiri *et al.*, 2002] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer. A secure routing protocol for ad hoc networks. In *Proceedings of the International Conference on Network Protocols (ICNP)*, 2002.
- [Shoup, 1999] V. Shoup. On formal models for secure key exchange (version 4). Technical report, revision of IBM Research Report RZ 3120, 1999.
- [Yang and Baras, 2003] S. Yang and J. Baras. Modeling vulnerabilities of ad hoc routing protocols. In *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, 2003.
- [Zapata and Asokan, 2002] M. G. Zapata and N. Asokan. Securing ad hoc routing protocols. In *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, 2002.
- [Ács *et al.*, 2005] G. Ács, L. Buttyán, and I. Vajda. Provably secure on-demand source routing in mobile ad hoc networks. *Technical Report, CrySyS Lab, Budapest University of Technology and Economics. Also available at <http://eprint.iacr.org/> under report number 2004/159.*, April 2005.
- [Çamtepe and Yener, 2005] S. A. Çamtepe and B. Yener. Key distribution mechanisms for wireless sensor networks: a survey. Technical Report TR-05-07, Rensselaer Polytechnic Institute, Computer Science Department, 2005.