BUDAPESTI MŰSZAKI ÉS GAZDASÁGTUDOMÁNYI EGYETEM
HÁLÓZATI RENDSZEREK ÉS SZOLGÁLTATÁSOK TANSZÉK

HÁLÓZATI PROTOKOLLOK AUTOMATIZÁLT BIZTONSÁGI ELLENŐRZÉSE ÉS QUERY AUDITÁLÁSI ALGORITMUSOK A VEZETÉKNÉLKÜLI SZENZOR HÁLÓZATOK KÖRNYEZETÉBEN

Ta Vinh Thong

Tézisfüzet

Témavezető

Dr. Buttyán Levente
Hálózati rendszerek és Szolgáltatások Tanszék
Budapest Műszaki és Gazdaságtudományi Egyetem

Budapest, Hungary
2013

1. Bevezetés

A doktori értekezésemben a biztonsági protokollok számára tervezett új formális és automatizált ellenőrzési módszereket javaslom. A dolgozatomban elsősorban olyan protokollokkal valamint algoritmusokkal foglalkozom, amelyek a vezeték nélküli szenzor hálózatokra (rövidítve: WSNs) terveztek. A dolgozatom a kővetkező három fő témából áll: (1) vezeték nélküli ad-hoc szenzorhálózatokra tervezett útvonal-választó protokollok formális és automatizált biztonsági elemzése; (2) vezeték nélküli szenzor hálózatokra tervezett transzport protokollok formális és automatizált ellenőrzése; és (3) query auditálási algoritmusok a statisztikai adatbázisokban tárolt érzékeny adatok védelmére. A következőkben egy rövid áttekintést nyújtok a három kutatási témámról. Megjegyzem, hogy ebben a fejezetben csak a fő problémákról fogok tárgyalni, amely motivációként szolgált a kutatásom során. A kutatási célok, a főbb kihívások, valamint a konkrét módszertanokról a következő három fejezetben fogom tárgyalni.

Első téma: Az első témám a vezeték nélküli szenzor hálózatok egy speciális alkalmazásához kapcsolódik, méghozzá olyan alkalmazásokban, ahol a telepített szenzor eszközök müködésközben változtathatják a helyzetüket, mint például a közlekedő járművek hálózata. Ezt a fajta hálózatot mobil ad-hoc szenzor hálózatnak nevezik. A vezetéknélküli mobil ad-hoc szenzor hálózatok esetén nincs előre definiált hálózati topológia, így a kommunikációhoz útvonal felfedezés szükséges a szenzor párok között. Mihelyt a két kommunikáló szenzor megegyezett egy útvonalban, amely több további közvetítő szenzort tartalmazhat, a további adatcsere és kommunikáció ezen az útvonalon keresztül történik. A forrás által küldött csomagot a közbenső szenzorok továbbitják amíg nem éri el a célt. Az útvonal felfedezési eljárásokat különböző útvonal-választó protokollok definiálják. A közelmúltban több támadást is publikáltak ismert útvonal-választó protokollok ellen, amely során a protokoll üzenetek ügyes manipulálásával a támadó (támadók) eléri, hogy nem létező útvonalakat fogadnak el a felek és azon keresztül próbálnak kommunikálni. Ennek a fajta támadásnak, amit dolgozatomban *útvonal hamisító* támadásnak nevezem, kritikus hatása van mivel a nem létező útvonalakon való kommunikálás sok felesleges energiát emészt fel, nagy mértékben csökkentve ezzel a hatékonyságot.

Második téma: Az második témám a vezeték nélküli szenzor hálózatokra tervezett transzport protokollok (WSN transzport protokollok) biztonsági ellenőrzéséhez kapcsolódik. A vezeték nélküli szenzor hálózatoknak néhány alkamazásában, mint például a multimédia szenzor hálózatokban [6] elvárt, hogy a szenzorok nagy mennyiségű adatot továbbítanak garantált minőség (QoS) mellett. Ezek az alkamazások megkövetelik a transzport protokollok használatát, a megbizható adatkézbesítési és torlódás kezelési tulajdonságuk miatt. A vezeték nélküli szenzor hálózatban sajnos nem használhatjuk a vezetékes hálózatokban ismert és bevált transzport protokollokat, mint a TCP (Transmission Control Protocol), mert nagyon sok olyan műveletet tarmalmaznak ami sok energiát emészt fel, s így a szenzorok gyors lemerüléséhez vezet. Emiatt sok olyan transzport protokollt dolgoztak ki szenzor hálózatokra, amelyek energia hatékonyabbak (lásd pl. [38]). A főbb tervezési kritériumok, amelyeket a WSN transzport protokolloknak terjesíteniük kell a megbizhatóság és az energia hatékonyság. Sajnos azonban a legtöbb ilyen protokoll csak addig tudja ezt a két feltételt kielégíteni amíg a hálózat minden résztvevője jóindulatú. Olyan környezetben azonban ahol a támadó módosíthatja az üzeneteket, nem teljesítik a kritériumokat, mivel nem tartalmaznak megfelelő biztonsági megoldásokat. Általánosságban kétféle támadásról beszélhetünk, ez egyik a megbizhatóság elleni támadás, a másik pedig az úgynevezett energiamerítő támadás. Előbbi esetben a támadás akkor tekinthető sikeresnek amikor az adatvesztés észrevétlen marad, míg utóbbi esetben a támadónak (támadóknak) sikerül lemerítenie a szenzorokat felesleges nagy energiát igénylő számítások elvégeztetésével.

Harmadik téma: A harmadik témám a vezeték nélküli szenzor hálózatoknak a kórházi környezetben való alkamazásával kapcsolatos, ahol betegek orvosi adatait (pl. EKG, testhőmérséklet, vérnyomás) testre rögzíthető szenzorokkal mérik. A mért adatokat egy személyi eszközzel (pl. okostelefon) gyűjtik és az eszközön belüli adatbázisban tárolják. Ideális esetben a mért tárolt orvosi

adatokhoz csak a jogosult személy férhet hozzá (pl. kezelő orvos). Azonban néhány esetben külső feleknek (pl. biztosító cégek, kutatók) is adnak hozzáférést a tárolt adatoknak valamilyen sztatisztikai információjához. Ezek a sztatisztikai adatok (pl. a tárolt adatok átlaga) nem titkosak, és egy fontos követelmény, hogy a sztatisztikai információk egy halmazából az érzékeny adatokat ne lehessen kiszámolni. Például a tárolt adatok átlagait lehet lekérdezni de az átlagokból ne lehessen kikövetkeztetni egy-egy konkrét adatra. Ahhoz hogy ezt biztosítsák, úgynevezett *query auditorokat* telepítenek az eszközökre.

A query auditálás (QA) egy intezíven tanulmányozott probléma, amelynek célja a sztatisztikai adatbázishoz intézett kérdéseket kezelni, olymódon hogy a válaszokból az érzékeny adatokat ne lehessen kikövetkeztetni. Két tipust különböztetünk meg, az offline és az online query auditálás. Az első esetben az auditor a múltban feltett kérdések és azok válaszai alapján detektálja, hogy történt-e érzékeny adat szivárgás. A második esetben az auditor megvizsgálja, hogy az új kérdésre szabad-e válaszolni (a múltbeli kérdésekre és válaszokra alapozva), hogy ne szivárogjanak ki érzékeny adatok. Ezenkivül az információ szivárgás illetően megkülönböztetünk a teljes felfedési modellt (full diclosure model) és a részleges felfedési modellt (partial disclosure model). Akkor mondjuk, hogy egy x adat teljesen fel van fedve, ha az x értékét egyértelműen megtudjuk határozni, míg a részleges felfedés azt jelenti, hogy az x értékét egy adott kicsi intervallum közé tudjuk becsülni, vagy valamilyen eloszlást követ.

2. Kutatási célkitűzések

Ahogy az 1. fejezetben tárgyaltuk, kritikus biztonsági lyukak találhatóak sok ismert útvonal-választó és WSN transzport protokollokban, beleértve sok olyan protokollt is amelyek kriptográfiai megoldásokat tartalmaznak, és biztonságosnak hitték a tervezők. A protokollokban rejlő biztonsági hibákat gyakran nehéz észtrevenni a protokoll definiciójából adodó hatalmas számú viselkedési forgatókönyv miatt. Sok esetben a protokoll tervezők csak manuálisan és informálisan ellenőrzik a protokollt, emiatt sajnos sok rejtett hibát nem vesznek észtre. Ezen a problémán segít a formális és szisztematikus ellenőrzési módszer, amit sikeresen és széleskörűen alkalmaznak a szoftver tervezés során. A legnagyobb előnye a formális analízis módszereknek az, hogy preciz matematikai háttéren alapulnak és igy sokkal megbizhatóbbak mint az informális analízis. Továbbá a formális analízis általában nagy kifejező erejű formális nyelveket használ, lehetővé téve a automatizált ellenőrzés megvalósítását.

Az irodalomban sok formális nyelv valamint automatizált modell ellenőrzési módszer található különböző protokollok és rendszerek tulajdonságainak analízisére, e.g., [17], [29], [32], [8], [34], [27]. Azonban ezek a módszerek nem útvonal-választó protokollokra lettek tervezve, így nem tartalmazzák a szükséges szintaktikai és szemantikai nyelvi elemeket, mint például a broadcast küldés. Emiatt ezeket az eszközöket nem lehet közvetlenül használni útvonal-választó protokollok elemzésére, vagy csak korlátozottan. Ennek hatására olyan módszereket és modellezési nyelveket publikáltak az utóbbi években e.g., [18], [19], [35], [7], [27], [12], [3], [37], [33], amely tartalmazzák az ad-hoc hálózatokra jellemző modellezési elemeket. Azonban ezeknek a módszereknek több hátránya is van: (i) az analízis nem automatizált; (ii) habár automatizált de nem útvonal hamisító támadások detektálására lettek tervezve.

Hasonlóképpen, a legjobb tudomásom szerint még nem ajánlottak módszert a WSN transzport protokollok formális és automatizált biztonsági ellenőrzésére. Ennek az egyik oka az lehet, hogy a WSN transzport protokollok nagyon komplex viselkedési elemeket tartalmazhatnak, mint például a időzítések, a probabilisztikus viselkedés, és a kriptográfiai műveletek, együttesen. Sajnos a legtöbb kapcsolodó analízis módszer és eszköz (pl. [29], [32], [8], [34], [27], [24]) nem használható közvetlenül

WSN transzport protokollok biztonsági elemzésére a korlátozott szintaktikai és szemantikai modellezési elemek miatt. Megcélozva ezt a problémát az első két témában a kutatásom arra fókuszál, hogy új *formális* és *automatikus* analízis módszereket dolgozzak ki, amellyel bebizonyítható vagy cáfolható útvonal-választó protokollok valamint WSN transzport protokollok biztonsága.

A query auditálás (QA) egy intezíven tanulmányozott probléma, és a múltban többféle auditort dolgoztak ki különböző problémákra [5]. Ezekben a munkákban az érzékeny adat amit megakarunk védeni az individuális adatok (pl. egy adott alkamazott fizetése). Ennek talán az az oka, hogy sok esetben valamilyen sztatisztikai adatokra vonatkozó kérdésre kiváncsiak (pl. a női alkamazottak átlagfizetése) és ilyen esetekben egy adatbázis rekord egy-egy emberhez tartozik [5]. Én ezzel szemben egy újszerű query auditálási próbléma felvetést definiálom, amelyben az aggregált adatok számítanak érzékenyben. Ez egy kórházi környezetben érdekes lehet, ahol az mérések (vérnyomások, EKG adatok) szélső értékei (pl. maximuma vagy minimum) valamilyen betegségre utalhatnak, amit szeretné a beteg ha kiderülne. A célom ebben az új beállítás mellett hatékony offline és online query auditálási algoritmusokat kidolgozni. Pontosabban az adatbázisban tárolt adatok egy részhalmazának maximumának (minimum) védelmére dolgoztam ki query auditorokat, ahol a kérdező az adott adathalmaz átlagára kérdezhet.

3. Kihívások

Ebben a fejezetben tárgyalom a három kutatási témában előforduló főbb kihívásokat. Az útvonalválasztó protokollok elemzése témában egyrészt az olyan specifikus modellezési elemeket kell támogatni mint a broadcast kommunikációt, szomszédság fogalmát, kommunikációs tartományt. Új tételek és biszimulációs definiciók szükségesek az ad-hoc hálózati környezetben specifikus támadók modellezéséhez, valamint az útvonal hamisító támadások leírásához. Másrészt, az útvonal-választó protokollok automatizált ellenőrzése során nagy számú hálózati topológia és erős támadó modellt kell figyelembe vennünk. Ez hatalmas méretű állapotteret eredményez, amit a mostani számítógépek nem mindig tudják kezelni. A célom, hogy olyan elemzési módszert dolgozzak ki, amely képes tetszőleges hálózati topológiát figyelembe venni és erős támadókat kezelni, amelyre az előző módszerek nem voltak képesek.

A WSN transzport protokollok formális és automatizált biztonsági ellenőrzése terén a legfőbb kihívás az, hogy ezek a protokollok nagyon komplex viselkedési elemeket tartalmazhatnak, mint például a valósidejű és probabilisztikus, és a kriptográfiai műveletek, amit támogatnia kell az analizáló módszernek. Továbbá a WSN transzport protokollok mint például az SDTP protokoll [11] magába foglalja mind a három említett viselkedési elemet. Emiatt ennek a protokoll osztálynak az analízise nagyon bonyolult. Legjobb tudomásom szerint még nem javasolták formális és automatizált biztonsági ellenőrzés módszereket WSN transzport protokollokra.

A query auditálás témában a legtöbb kapcsoló munkánál (pl. [13], [30], [14], [23]), az adatbázisban tárolt individuális attribútumokról azt feltételezik, hogy értéküket a (-∞, ∞) intervallumból veszik. Ezzel ellentétben én azt feltételezem, hogy az értékük egy véges $[\alpha, \beta]$, $\beta > \alpha$, intervallumba esik, ami általában igaz egy betegtől mért adatra (pl. testhőmérséklet). Ez a feltételezés azonban több új problémát vezet be, mert azok az auditorok amik megelőzik az érzékeny adatok kiszivárgását a első esetben nem biztos, hogy müködnek a második esetben. Pontosabban az véges $[\alpha, \beta]$ intervallum esetén a támadónak nagyobb lehetősége van kikövetkeztetni az érzékeny adatot a felső határok miatt.

4. Módszertan

Az útvonal-választó protokollok biztonsági ellenőrzéséhez egy processz algebra variánst dolgoztam ki amit *sr*-kalkulusnak neveztem el. Az előző kapcsolodó munkákhoz képest az *sr-kalkulus* a kifejezőbb szintaxist és szemantikát, amelyek szükségesek az útvonal-választó protokollok analízálásához: (i.) kriptográfiai primitivek and műveletek, (ii.) broadcast kommunikáció, és (iii.) a kommunikációs tartomány a vezeték nélküli közegben. Az *sr*-kalkulus a korábban javasolt applied π-kalkulus [17], az omega kalkulus [35] és a CMAN [18] kombinációjának tekinthető, kiegészítve kisebb modosításokkal és bővítésekkel. Emellett egy teljesen automatizált ellenőrzési módszert javasoltam az útvonal hamisító támadások detektálására, aminek az *sr-verif* nevet adtam. Az *sr*-verif módszer egy indirekt következtetésű bizonyítási technikán alapul, kombinálva a jól ismert logikai rezolúcióval.

A WSN transzport protokollok biztonsági elemzésére egy újszerű probabilisztikus-időzített kalkulust javasoltam kriptográfiai protokollok számára, amelynek a $crypt^{prob}_{time}$ nevet adtam. A $crypt^{prob}_{time}$ kalkulus alapkoncepcióját a más kutatók által javasolt kalkulusok [17], [20], [16] inspirálták. A $crypt^{prob}_{time}$ kalkulus az applied π-calculus, amely támogatja kriptográfiai, a probabilisztikus applied π-kalkulus [20], és az időzített automata alapú kalkulus [16] kombinációjának egy modósított és bővített változata. Ezenkivül egy automatizált biztonsági ellenőrzési módszert ajánlok a WSN transzport protokollokra, amely a jól ismert általános célú PAT processz analízis eszköztár [36] használatán alapul. A legjobb tudomásom szerint a PAT eszköztárt még nem használtak ilyen célra, holott a nagy kifejező erejű szintaktika és szemantikája jól alkalmazható erre a célra.

A harmadik témát illetően, a teljes felfedési modellbeli offline és online query auditorok kidolgozása során a jól ismert lineáris egyenlet és lineáris optimizációs problémára vezettem vissza a query auditálási problémát. A részleges felfedési modellre vonatkozó query auditor kidolgozása során a [26]-ban javasolt hatékony véletlen mintavételezési megközelítést, valamint a sztatisztikában ismert Chernoff és Union bound-ot alkalmazom.

5. Új Eredmények

Ebben a fejezetben tárgyalom a fő kutatási eredményeimet fő tézisek és azonbelül altézisek formájában, valamint röviden ismertetem a megoldásokat. Az módszerek részletes ismertetése a doktori disszertációm tartalmazza.

5.1. Útvonal-választó protokollok formális és automatizált biztonsági elemzése

Kutatásom során elsősorban az úgynevezett on-demand source routing protokollokkal foglalkozom, ahol az útvonalat a rajta levő csomópontok azonosítóinak listája reprezentál, és amely a request és reply üzenetek részei. Az analízáló módszer kidolgozása során azt feltételeztem, hogy a támadók kompromittált hálózati csomópontok, amelyek rendelkeznek minden olyan képességgel és tudással mint egy nem kompromittált (becsületes) csomópont, de olyan (a protokolltól eltérő) dolgokat is csinálhatnak amiket a becsületes csomópont nem képes. Például egy támadó csomópont a tudása szerint modósíthatja és továbbíthatja az üzeneteket. A támadó csomópontok együttmüködhetnek és párhuzamosan futhatnak egyszerre különböző protokoll session-nekben.

1. Téziscsoport. *A biztonsági útvonal-választó protokollok biztonsági ellenőrzésére a processz algebrának egy új variánsát, az sr-kalkulust és egy logikai rezolúción alapuló új automatizált elemzési módszert, az sr-verifet javasoltam [Th05, Th06, Th07, Th08]. A javasolt módszereknek a legnagyobb*

előnye, hogy olyan modellezési elemeket támogatják amik a biztonsági útvonal-választó protokollok megkövetelnek, mint a kriptográfiai primitívek és a broadcast kommunikáció. A legjobb tudomásom szerint az általam javasolt módszerek az első olyan módszer, amely biztonsági útvonal választó protokollok elemzésére optimalizáltak. A javasolt módszereket sikeresen alkalmaztam ismert biztonsági útvonal-választó protokollok, SRP [31], Ariadne [22], és endairA [3], elemzésére.

A [12]-ban azonosított probléma szolgált fő motivációként a biztonsági útvonal-választó protokollok számára formális és automatizált biztonság ellenőrzési módszer kidolgozásához. Ebben a munkában sok biztonságosnak hitt útvonal-választó protokollról megmutatták, hogy mégis sebezhetőek. A szerzők azonosították néhány rejtett hibát az SRP és az Ariadne biztonsági protokollokban, az ismert szimulációs paradigma formális bizonyítási keretrendszer segítségével. Ez az első olyan probálkozás, amely formális analízist alkalmaz sikeresen útvonal-választó protokollok elemzésére. A [12]-ban bemutatott módszernek az a legynagyobb hátránya, hogy az ellenőrzés nem automatizálható, emiatt olyan módszer kidolgozására van szükség, amely lehetővé teszi a szisztematikus és automatizált ellenőrzést.

5.1.1. Az útvonal-választó protokollok formális biztonsági analízisére javasolt módszer

1.1. Tézis. *Az útvonal hamisító támadások detektálására a processz algebrának egy új variánsát, az sr-kalkulust javasoltam [Th05, Th06, Th08]. Az sr-kalkulus a mások által javasolt applied π-kalkulus [17], az omega-kalkulus [35] és a CMAN [18] nyelveken alapul. Az sr-kalkulus legnagyobb előnye az előbbiekhez képest, hogy minden olyan modellezési elemeket támogatják amik a biztonsági útvonal-választó protokollok megkövetelnek, mint a (i) kriptográfiai primitívek és a (ii) broadcast kommunikáció. Az útvonal-választó protokollok biztonságának bizonyításához vagy cáfolásához új (a vezeték nélküli ad-hoc hálózatokra szabott) cimkézett biszimuláció definiciót fogalmaztam meg. Végül megmutattam, hogy az sr-kalkulus szintaxisa és szemantikája jól definiáltak.*

Az általam javasolt *sr*-kalkulus előnye a nagy kifejező ereje, mivel lehetővé teszi a broadcast kommunikció, a szomszédság tulajdonság és a kommunikációs tartomány modellezését mint a CMAN [18] és az ω-kalkulus [35], valamint a kriptográfiai primitívek és műveletek leírását mint az applied π-kalkulus és a spi-kalkulus [1, 17]. Emellett egy új szintaktikai és szemantikai elemet is tartalmaz *active substitution with range* néven, amely lehetővé teszi számunkra a támadó tudásbázisának a modellezését. Az *sr*-kalkulus továbbá magába foglalja újszerű, probléma specifikus tételeket és biszimulációs definiciókat, amelyeknek segítségével bebizonyíthatjuk illetve megcáfolhatjuk az útvonal-választó protokollok biztonságát. A következőkben egy rövid áttekintést adok a javasolt kalkulusról. Az *sr*-kalkulus tipus-rendszere és formális szintaxisa a disszertációm 2.5.1 és 2.5.2 fejezetében található, formális szemantikájáról pedig az 2.5.3 fejezetében olvashatjuk.

1.2. Tézis. *Alkalmazva az általam javasolt sr-kalkulust és címkézett biszimulációt, bebizonyítottam, hogy az ismert SRP biztonsági útvonal-választó protokoll sebezhető az útvonal hamisító támadásokkal szemben, egy kompromittált csomópontot feltételezve.*

A következőkben intuitivan vázolom az általam javasolt új *címkézett biszimuláció definicióját*, amelynek segítségével tudjuk bizonyítani a protokollok biztonságát. A formális definició leírást a korlátos oldalszám miatt csak a disszertációban tárgyalom, ugyanis sok segéd definiciót és jelőlést igényel. A bővebb és formálisabb definició a disszertációm 2.5.3. fejezetében található. A címkézett biszimuláció két vezeték nélküli ad-hoc hálózat között definiálandó, és azt mondja, hogy két hálózat akkor van címkézett biszimulációban egymással ha egy külső megfigyelő nem tudja megkülönböztetni egymástól a két hálózatot az elkapott hálózati üzenetek alapján.

1. Definició. *Egy adott hálózati topológiára vonatkozó címkézett biszimuláció (jelölése $\approx_l^N$) a legnagyobb olyan szimmetrikus reláció ($\Re$) két azonos topológiájú és csomópontú hálózat között, amelyre igaz a következő három pont:*

1. *A két hálózatban kiküldött üzenetek halmazát nem lehet megkülönböztetni egymástól, s azt mondjuk, hogy a két hálózat statikusan ekvivalens;*
2. *Az egyik hálózat úgy tudja szimulálni a másik hálózatban levő csomópontok belső számításait (belső redukció), hogy utána a két hálózat sztatikusan ekvivalens maradt, és fordítva.*
3. *Az egyik hálózat úgy tudja szimulálni a másik hálózatban levő csomópontok cimkézett akcióit (üzenet küldés, fogadás), hogy utána a két hálózat sztatikusan ekvivalens maradt, és fordítva.*

A címkézett biszimuláción alapuló bizonyítási technika a következő: Egy *routeprot* biztonsági útvonal-választó protokoll elemzéséhez definiálok a *routeprot*-ot és egy másik variánsát, *routeprotideal*, *sr*-kalkulus szintaxis használatával. A *routeprotideal* a *routeprot*-nak egy ideális változata, amelyben a forrás csomópont mindig tudja, hogy az általa visszakapott válaszüzenetben levő útvonal helyes-e, és amennyiben helyes akkor kiküldi az *Accept* konstanst, jelezve ezzel, hogy elfogadta az útvonalat. Az SRP protokoll sebezhető az útvonal hamisító támadásokkal szemben mert *routeprot* és *routeprotideal* nincsenek címkézett biszimulációban egymással. Ehhez megmutattam, hogy van olyan topológia és tranziciók egy sorozata, amely után *routeprotideal* kiadja az *Accept* konstanst amit *routeprot* nem tudja szimulálni. Az SRP részletes elemzése a disszertáció 2.6 fejezetében található.

1.3. Tézis. *Javasoltam egy újszerű visszafele-következtetés alapú bizonyítási algoritmus (röviden BDSR) source routing útvonal-választó protokollokra, amely kombinálja az sr-kalkulust a visszafele-következtetés technikával. A BDSR algoritmus segítségével bebizonyítottam, hogy az ismert Ariadne protokoll sebezhető az útvonal hamisító támadással szemben, egy támadó csomópontot feltételezve. Továbbá bebizonyítottam, hogy az ismert endairA protokoll biztonságos egy támadó csomópont esetén, viszont sebezhető több együttmüködő csomópont esetén.*

Egy szisztematikus bizonyítási algoritmust, a BDSR-t, dolgoztam ki, amely lehetővé teszi az útvonal-választó protokollok hatékony biztonsági elemzését. A BDSR visszafele-következtetési elven müködik, kiindulva abból a feltételezésből, hogy a forrás csomópont elfogadta egy nem hamis utat, és a protokoll specifikációja alapján visszafelé, lépésről lépésre haladva megprobáljuk kikövetkeztetni, hogy ez hogyan történhetett. Ha mindenesetben ellenmondásba ütközünk, akkor ez azt jelenti, hogy a protokoll biztonságos, különben pedig a támadást adjuk vissza.

A BDSR újdonsága az, hogy visszafele egy kidolgozott algoritmus szerint próbálja meg bebizonyítani a címkézett biszimuláció fennállását a valós (*routeprot*) és az ideális (*routeprotideal*) hálózat között. Ez lehetővé teszi a kimerítő analízist és így a protokoll biztonságának bizonyítását komplexebb útvonal választó protokollok esetén mint a Ariadne és az endairA. A disszertáció 2.7 fejezetében található a BDSR algoritmus részletes leírása.

5.1.2. Az útvonal-választó protokollok automatizált biztonsági ellenőrzésére javasolt módszer

1.4. Tézis. *Javasoltam egy teljesen automatizált ellemzési módszert, az sr-verif néven, a source routing tipusú útvonal-választó protokollok biztonsági ellenőrzésére [Th07, Th08]. Az sr-verif a javasolt BDSR algoritmuson alapul, kombinálva a logikában jól ismert rezolucióval. Bebizonyítottam az sr-verif helyességét, megmutatva, hogy amikor az sr-verif visszaad egy támadást akkor az valóban egy érvényes támadás. Továbbá bebizonyítottam, hogy az sr-verif nem kerül végtelen következtetési ciklusba, és véges lépés után terminál. Végül megadtam az sr- verif komplexitását is.*

Az *sr*-verif egyik előnye a kapcsoló modell-ellenőrzökkel szemben (pl. [7, 35]) az, hogy a protokollok működését az *sr*-kalkulus (egyszerűsített) szintaxissal adhatjuk meg, ami támogatja a kriptográfiai műveletek, a broadcast kommunikációt. Egy másik előnye az elöző munkákkal [12, 2, 3, 4, 18] szemben az, hogy teljesen automatizált az ellenőrzés. Nagy elönye például [7]-val szemben, hogy az ellenőrzés nincs adott hálózati topológiához kötve, hanem tetszőleges topológiát feltételez. Az egyetlen megkötés az, hogy hálózatban levő csomópontok száma véges. Végül a [37, 33] munkákkal szemben, amely loop-ok detektálására törekedett, én elsősorban biztonsági ellenőrzésre fókuszáltam.

Az általam javasolt *sr*-verifet a széleskörben használt Proverif automatikus ellenörző eszköz [9] ihlete. Azonban ellentétesen a Proveriffel, amely biztonsági protokollok elemzésére tervezték, az *sr*-verif a biztonsági útvonal-választó protokollokra optimalizált és sok újdonságot tartalmaz mint a szomszédság, a broadcast kommunikáció és az eltérő támadó modell. Míg a Proverifben a támadó mindent lehallgat, addig az *sr*-verifben csak a szomszédai által küldött üzeneteket.

Az *sr*-verifben az útvonal-választó protokollokat az *sr*-kalkulus egyszerűsített szintaxisával specifikáljuk. Ez a specifikációt majd lefordítjuk a fordító szabályok segítségével a logikában ismert Horn-klózok halmazára. Ezt a klózokból álló halmazt *protokoll szabályoknak* nevezzük. Egy támadó csomópont számítási kapacitása is Horn-klózok halmazából állnak, és támadó szabályoknak hivjuk. Továbbá a hálózati topológia és a támadó kezdeti tudása szintén egy logikai szabály (tény) halmazként van definiálva. A következtetési algoritmus a logikai szabályokra végzett rezolúciók egy sorozata. Bővebb leírás az algoritmusról a disszertációm 2.8 fejezetében található. A disszertációm 2.8.10 fejezetében bebizonyítottam, hogy az *sr*-verif soha nem kerül végtelen következtetési ciklusba és mindig terminál. A disszertációm 2.8.11 fejezetében megmutattam, hogy az *sr*-verif helyes, tehát amikor egy támadást detektál, akkor az tényleg egy érvényes támadás. Végül az algoritmus komplexitásáról részletesebben a disszertációm 2.8.12 fejezetében olvashatjuk.

1.5. Tézis. *Az sr-verif segítségével megmutattam azt, hogy az SRP és az Ariadne protokollok sebezhetőek egy darab támadó csomópont esetén, valamint az endairA protokoll tamádható kettő támadó esetén.*

5.2. WSN transzport protokollok formális és automatizált biztonsági ellenőrzése

A második téziscsoportban a második kutatási témámmal kapcsolatos új eredményeket részletezem, szintén fő tézis és altézisek formájában.

2. Téziscsoport. *WSN transzport protokollok formális elemzésére javasoltam egy új probabilisztikus-időzített kalkulust kriptográfiai protokollokra, amit* $\text{crypt}^{prob}_{time}$ *névre kereszteltem. Emellett egy automatizált ellenőrzési módszert is javasoltam a jól ismert, mások által tervezett PAT processz analízis toolkit [36] alkalmazásával. A* $\text{crypt}^{prob}_{time}$ *és a PAT processz analízis toolkit használatával megmutattam, hogy a mások által publikált DTSN és SDTP transzport protokollok sebezhetőek. Kidolgoztam és publikáltam egy új WSN transzport protokollt, az* $SDTP^{+}$*-t [Th11], amire bebizonyítottam hogy biztonságos azokkal a támadásokkal szemben, amelyekkel szemben a DTSN és SDTP protokollok sérülékenyek. [Th11, Th13, Th12] a kapcsolodó publikációim ehhez a témakörhöz.*

Annak ellenére, hogy a WSN transzport prokollok tervezésénél figyelembe veszik a rosszindulatú környezetben való működést, mégis a legtöbb tervező nagymértékben elhanyagolja a biztonsági megoldásokat, ami azt eredményezi, hogy ezek a protokollok csak jóindulatú környezetben működnek megbizhatóan [10]. Általánosságban kétféle támadásról beszélünk WSN transzport protokollok esetén, megbizhatóság elleni támadás és energia emésztő támadás. Az első esetben a támadó akkor sikeres ha eléri, hogy az üzenetvesztés észtrevétlen marad, utóbbi esetben pedig sikeresen ráveszi a

szenzor csomópontokat felesleges számításokat amivel lemeríti a szenzorokban telepített elemeket. A WSN transzport protokollok komplex működése miatt az informális és manuális ellenőrzés nagyon hiba érzékeny, és a rejtett hibák könnyen észtrevétlen maradhatnak. Tehát sokkal pontosabb formális és szisztematikus ellenőrzési módszerek szükségesek, hogy javítsuk az elemzés megbizhatóságát.

5.2.1. A WSN transzport protokollok biztonsági elemzése javasolt formális módszer

2.1. Tézis. *Javasoltam egy új probabilisztikus-időzített kalkulust, a $crypt^{prob}_{time}$-t, kriptográfiai protokollokra [Th13, Th12]. A legjobb tudomásom szerint ez az első olyan kalkulus, amely támogatja egyszerre a következő három viselkedési karakterisztikát: (i) formális szintaxis és szemantikát tartalmaz a kriptográfiai primitivekre, (ii) támogatja az időzített konstrukciókat ami lehetővé teszi a valósidejű rendszerek elemzését; (iii) probabilisztikus szintaktikai és szemantikai elemeket is magába foglal a probabilisztikus rendszerek kezelésére. Továbbá javasolok egy új definiciót, a gyenge probabilisztikus időzített biszimulációt a WSN transzport protokollok biztonságának bizonyításához illetve cáfolásához.*

A $crypt^{prob}_{time}$ alap koncepcióját a előző kapcsolodó munkák [17], [20], [16] inspirálta, amelyek külön-külön támogatja a fent említett három működési karakterisztikát. Pontosabban a $crypt^{prob}_{time}$ alapja az applied π-kalkulus [17], amely letisztult szintatikát és szemantikát definiál a kriptográfiai műveletek leírására; Az applied π-kalkulus [20] probabilisztikus bővítése; és az időzített automata terminológiával tervezett processz algebra nyelv [16]. A $crypt^{prob}_{time}$ tervezési elve ennek a három munkának az elvén alapul, néhány modósítással és bővítéssel.

Habár az általam javasolt $crypt^{prob}_{time}$-et első sorban WSN transzport protokollok elemzésére használtam, ugyanúgy használható más protokollok analízálására, amelyek rendelkeznek fenti a három működési elemmel. A célom a $crypt^{prob}_{time}$ kalkulussal az, hogy egy olyan precíz matematikai háttérrel rendelkező módszert javasoljak a probabilisztikus időzített kriptográfiai protokollok elemzésére. Az $crypt^{prob}_{time}$ ebben a formájában még nem lehet automatizált ellenörzésre kibővíteni, hanem lekell egyszerűsíteni és átalakítani, s a jövőbeli munkák egyikét képezi. A disszertációmban ehelyett egy már ismert, jól megtervezett automatizált ellenőrzési eszközt, a PAT toolkitet [36] használom, annak ellenére, hogy nem olyan erős szintaktikát és szemantikát támogat mint a $crypt^{prob}_{time}$.

A $crypt^{prob}_{time}$ alkotó "gerince", amit *crypt*-nek nevezzük, az applied π-calculus [17] egy modósított verziója, amely támogatja a kriptográfiai elemeket. Az applied π-calculus eltérően, az automatán alapuló koncepciója miatt inkább rekurzív processz hívást definiál mint processz replikációt. Ezenkivül például a *crypt* szintaktikája integer-eket is definiál, valamint olyan processzeket amely integer-ek összehasonlításáért felelős, ami nincsen az applied π-kalkulus alapváltozatában. A *crypt* időzítés elemekkel való bővítése az [16]-ban tárgyalt időzített kalkuluson és az időzített automatán [25] alapul. A probabilisztikus kiterjesztés pedig a [20]-ban javasolt kalkusluson és az [16]-ban tárgyalt probabilisztikus automatán alapul. A legnagyobb különbség az általam javasolt $crypt^{prob}_{time}$ és az említett munkák között az, hogy a megoldásom egyszerre támogatja az idő és probabilisztikus elemeket, valamint az alapként használt *crypt* kalkulus sokkal kifejezőbb. Végül felruháztam a $crypt^{prob}_{time}$-t egy új definicióval, a *gyenge probabilisztikus időzített biszimulációval*, amely lehetővé teszi biztonsági tulajdonságok bizonyítását és cáfolatát.

A $crypt^{prob}_{time}$ kalkulus formális szintaxisa és működési szemantikája a disszertációm 3.4 és 3.5 fejezetében találhatóak. A következőkben bemutatom a $crypt^{prob}_{time}$-on alapuló bizonyítási technikát, majd demonstrálom néhány publikált WSN transport protokoll elemzését. Erről bövebben a disszertációm 3.6. fejezetében található.

2. Definició. (***Gyenge probabilisztikus időzített biszimuláció***)
Azt mondjuk, hogy két állapot $s_1 = (A^1, v_1)$ és $s_2 = (A^2, v_2)$ gyenge probabilisztikus időzített

biszimulációban van egymással, azaz ($s_1 \ \Re_t^p \ s_2$) *ha*

1. *a külső megfigyelő nem tudja megkülönböztetni az* A^1 *és* A^2 *kimeneteit;*

2. *ha az* s_1 *állapotból egy néma (azaz belső) akció után eljutunk az* s_1' *állapotba* d *idő után akkor* s_2 *ezt egy megfelelő néma (azaz belső), valamilyen* s_2'*-be vezető tranzicióból álló sorozattal tudja szimulálni, és* $s_1' \ \Re_t^p \ s_2'$ *ismét fennáll.*

3. *ha az* s_1 *állapotból egy címkézett (azaz megfigyelhető) akció után eljutunk az* s_1' *állapotba* d *idő után akkor* s_2 *ezt egy megfelelő címkézett (azaz megfigyelhető), valamilyen* s_2'*-be vezető tranzicióból álló sorozattal tudja szimulálni, és* ($s_1' \ \Re_t^p \ s_2'$) *ismét fennáll.*

és fordítva.

3. Definició. *Legyen a Prot() és* $Prot^{ideal}()$ *rendre az adott Prot protokoll valós és ideális verziója. Azt mondjuk, hogy Prot biztonságos ha Prot() és* $Prot^{ideal}()$ *gyenge probabilisztikus időzített biszimulációban vannak egymással:* $Prot() \approx_{pt} Prot^{ideal}()$.

A WSN transzport protokollokra vonatkozó biztonsági tulajdonságok bizonyításához a következő technikát használom: definiálom egy normál ($Prot()$) és egy ideális ($Prot^{ideal}()$) verzióját az adott protokoll leírásnak. Az ideális protokoll a normál (valós) protokollnak egy kiegészített verziója, úgy hogy egy-egy fajta támadás biztonsan ne müködjön benne. Például a csomópontok között hozzáadjuk egy-egy rejtett csatornát hogy informálják egymást arról milyen üzenetet kellene megkapni, így az üzenet módosító támadások nem müködnek az ideális verzióban. Ezután megvizsgálom, hogy $Prot()$ és $Prot^{ideal}()$ gyenge probabilisztikus időzített biszimulációban van-e egymással (lásd 3-as definició).

2.2. Tézis. *Az általam javasolt* $crypt_{time}^{prob}$ *használatával specifikáltam a más szerzők által publikált DTSN protokoll müködését. Ezután bebizonyítottam, hogy a DTSN protokoll sebezhető az adat és kontroll csomagok szándékos módosításával szemben, egy kompromittált csomópontot feltételezve.*

A DTSN protokoll esetén a biztonsági tulajdonság amit szeretnék elemezni az, hogy mennyire sebezhető az üzenet modósító és hamisító támadások ellen. Az üzenetek megfelelő elemeinek manipulálásával elérhető, akár az észtrevétlen üzenetvesztést, akár a szenzorok akkumulátorainak lemerítését.

A 3-as definició szerint definiáltam a DTSN-nek két változatát, a valós $Prot(params)$ és az ideális $Prot^{ideal}(params)$-t. Ezután megmutattam, hogy van olyan PTTS tranzició szekvencia a valós $Prot(params)$-ban, amit a ideális $Prot^{ideal}(params)$ semilyen megfelelő szekvenciával nem tudja szimulálni. Ez a PTTS tranzició szekvencia egy támadást ír le, amelyben a támadó módosítja az üzenet tartalmát és továbbítja a becsületes csomópont felé. A valós protokollban amikor a becsületes csomópont megkapja ezt az üzenetet akkor biztonsági megoldások híján feldolgozza az üzenetet mintha az egy becsületes csomóponttól jönne. Mivel az ideális esetben a fogadó csomópont elfogja dobni ezt a hamis üzenetet ezért nem tudja szimulálni azokat az akciókat amit a valós verzióban végez. A disszertációmban három támadási forgatókönyvet mutattam be, amelyek külön-külön sértik a 2-es definicó egyes pontjait, rendre. A DTSN specifikációja és biztonsági elemzése a disszertáció 3.6.1 és 3.7.1 fejezeteiben találhatók.

2.3. Tézis. *Az általam javasolt* $crypt_{time}^{prob}$ *használatával specifikáltam a más szerzők által publikált SDTP protokoll müködését, amely a DTSN-nek egy biztonsági kiterjesztése. Bebizonyítottam, hogy egy kompromíttált csomópont esetén az SDTP protokoll biztonságos az üzenet módosító/hamisító támadásokkal szemben, viszont két együttmüködő támadó esetén sebezhető.*

Hasonlóan az DTSN esetéhez, definiálok két változatot az SDTP protokollból egy valós és egy ideális változatot. Ezután bebizonyítottam, hogy az ideális verzióban a támadásokat leíró tranziciók

a valós verzióban lehetségesek de az ideális verzió ezeket nem tudja szimulálni semmilyen hasonló tranzicióval. Az SDTP protokoll specifikációja és biztonsági analíziséről a disszertációm 3.6.2 és 3.7.2 fejezteiben olvasható.

2.4. Tézis. *Javasoltam egy új biztonsági WSN transzport protokollt, az SDTP$^+$-t [Th11], a DTSN és SDTP protokollok sebezhetőségeinek foltozására. Specifikáltam az SDTP$^+$-t a crypt$^{prob}_{time}$ kalkulussal és bebizonyítottam, hogy biztonságos az üzenet módosító/hamisító támadásokkal szemben, mind az egy és kettő támadó csomópont esetén.*

Az DTSN és SDTP tervezési hibáinak feltárása után javasoltam egy új biztonsági WSN transzport protokollt, az SDTP$^+$-t, amely az elődeitől különböző biztonsági megoldást alkalmaz. Az SDTP$^+$ célja megerősíteni az adat és kontroll üzenetek hitelesítés és integritás védelmét, a más területen már sikeresen alkalmazott (pl. Ariadne protokoll [22], [21]) hash-lánc [15] és Merkle-fa [28] alkalmazásával. Tudomásom szerint én alkalmazom elöszőr a hash-láncot és Merkle-fát WSN transzport protokoll tervezésére. Az SDTP$^+$ protokoll teljes leírása a diszertációm 3.3.-ik fejezetében található.

Az SDTP$^+$ biztonsági ellenőrzéséhez hasonlóképpen definiálok egy valós és egy ideális verziót a protokollból, majd a 2-es definicó alapján megvizsgálom azokat támadási szenáriókat amik sikeresek voltak a DTSN és az SDTP ellen. Formálisan bebizonyítottam, hogy a hash-lánc és Merkle-fa alkalmazásával a az DTSN and SDTP-ben található sérülékenységeket kiküszöböltem.

5.2.2. A WSN transzport protokollok biztonsági automatizált ellenőrzésére javasolt módszer

Javasolok egy módszert a DTSN és SDTP protokollok automatizált ellenőrzésére az ismert PAT toolkit [36] alkalmazásával, amely egy széleskörben használt általános célú eszköz, de legjobb tudomásom szerint még nem alkalmazták WSN transzport protokollok ellenőrzésére. A PAT probabilisztikus időzített modulja (PRTS) támogatja a probabilisztikus és időzitett szintaktikai és szemantikai elemeket, ezenkivül C-hez hasonló szintaktikája (pl. arrays, matematikai operátorok, while ciklus, stb.) lehetővé teszi a WSN transzport protokollok komplex működésének leírását. Megkell azonban említeni, hogy a PAT toolkit nem biztonsági protokollok ellenőrzésére optimalizált, és jelen formájában nem támogatja a kriptográfiai primitivek és műveletek leírására szintaktikai elemeket. Emiatt a kriptográfiai elemek modellezése implicit és abstrakt formában történik.

2.5. Tézis. *A PAT toolkit használatával megmutattam a DTSN protokoll sérülékenységét az üzenetet modósító illetve hamisító támadásokkal szemben, egy támadó csomópont esetén [Th13, Th12].*

A DTSN első fő tervezési célja a megbizható üzenet szállítás nyújtása, viszont nem tartalmaz semilyen kriptográfiai megoldást az üzenetek hitelesítésének és integritásának védelmére. Az első állítás, jelöljük *violategoal*-al, segítségével tudjuk ellőrizni, hogy a DTSN eléri ezt a célját amennyiben a hálózati topológia a következő: $S - I - A - D$, ahol S, I, A, D rendre a forrás, a közbenső, a támadó, és a cél csomópontokat jelöli. A PAT toolkitben a hálózati topológiákat a csomópontpárok között definiált kommunikációs csatornákkal lehet modellezni.

```
PAT code:
 #define violategoal (OutBufL == 0 && BufI == 0 && numNACK > 0);
```

A *OutBufL* és *BufI* változók reprezentálják rendre a forrás és a közbenső csomópont buffereiben tárolt üzeneteket. A *numNACK* változó definiálja azoknak az üzeneteknek a számát, amelyeket nem kapott meg a cél csomópont és kéri azok újraküldését. Ezek alapján a *violategoal* azt az állapotot reprezentál

amiben a forrás és a közbenső csomópont törölte minden (az újraküldés céljából) tárolt üzenetet a bufferéből, annak ellenére, hogy újraküldésre szükség van. Ezután lefuttatjuk a PAT modellellenőrzést a *violategoal*-ra, és eredményül kaptunk egy támadási forgatókönyvet. A disszertációmban a többi támadási forgatókönyvre vonatkozó állításokat és topológiákat is részletezem.

2.6. Tézis. *A PAT toolkit használatával megmutattam, hogy az SDTP protokoll biztonságos az üzenet modósító/hamisító támadással szemben egy támadó csomópont esetében, valamint sebezhető két egymással együttmüködő támadó esetén [Th13, Th12].*

Az SDTP protokoll a DTSN első biztonsági kiterjesztése kriptográfiai megoldásokkal. Mint említettem a PAT jelenlegi szintaktikája nem támogatja a kriptográfiai elemek explicit modellezését, így például az *msg* üzenetre a *Kmac* kulccsal számolt MAC (message authentication code) a *msg.Kmac*-el modellezem. Ez a PAT szintaxisa szerint egy összetett üzenetet jelent, amelynek első része a *msg* és második része a *Kmac*. Látható, hogy ez még nem megfelelő mivel alapesetben ez azt jelentené, hogy a *Kmac* kulcsot is hozzáfér nyíltan a támadó. Ahhoz, hogy tényleg egy MAC kódot modellezze *msg.Kmac*, a támadót úgy kell specifikálni, hogy nem használhatja a kulcsot és nem rakhatja rá másik üzenezet, pl. *msgAtt.Kmac*. A többi kriptográfiai primitivet is ilyen módon modellezem. A részletek megtalálhatóak a disszertációmban.

Először megvizsgáltam, hogy biztonsági megoldásokkal az SDTP-nek sikerült-e kiküszöbölni a DTSN sérülékenységeit. Ehhez ellenőriztem az SDTP protokollt a DTSN esetében talált támadási forgatókönyvekre, azaz, az $S - I - A - D$ és $S - A - I - D$ topológiákra és a *violategoal*-ra. Eredményül azt kaptam, hogy *violategoal* nem teljesül, ami azt jelenti, hogy egy darab támadó csomópont esetén az üzenet modósító/hamisító támadással nem lehet töröltetni a csomópontok tároló bufferjeit.

A következőkben megmutatom, hogy két támadó csomópont esetében azonban minden közbenső csomópont bufferjét lehet töröltetni, ami ellenkezik a mind a DTSN és SDTP tervezési céljaival. A DTSN és SDTP tervezési célja az, hogy az end-to-end csomag újraküldésnél hatékonyabb módszert biztosítsák, amelyben a közbenső csomópontok is tárolják és küldhetik újra az elveszett csomagokat. Legyen *violategoal2* az a logikai feltétel, amely azt az állapotot reprezentálja ahol a közbenső csomópontok több üzenetet törlik a bufferükből mint a amennyi szükséges. Elemeztem a *violategoal2*-t a két (együttmüködő) támadó esetén, azaz a $S - A1 - I - A2 - D$ hálózati topológiára, ahol I a közbenső csomópont. Erre a beállításra a PAT olyan támadást detektált, amelyben a két támadó eléri, hogy a közbenső csomópontban törölje minden tárolt üzenetet beleértve azt is, amelyre még szükség lehet újra küldésre. Ennek az az elsődleges oka, hogy az SDTP-ben a közbenső csomópontok nem ellenőrzik a csomag hitelességét, hanem csak a forrás és cél csomópontok az egymással megegyezett kulcs segítségével. Emiatt a támadóknak a hamis üzeneteit is tárolja és dolgozza fel a közbenső csomópont.

5.3. Query auditálási módszerek a sztatisztikai adatbázisokban tárolt érzékeny adatok védelmére

Egy újszerű query auditálási problémát vizsgálom, amelyben nem a egyéni értékek (pl. egy adott időpontban mért adat, vagy egy adott személynek valamilyen információja), hanem egy adathalmaz felett vett aggregált érték. A disszertációmban arra a problémára fókuszálok, amelyben a kérdező bizonyos tárolt adatokra kiszámolt átlagra kérdezhet rá, és a cél, hogy az adathalmaz maximuma (minimuma) ne szivárogjon ki a kérdések és válaszok alapján.

Formálisabban, a következő query auditálási problémát veszem figyelembe: Adott egy t lekérdezésből adodó szekvencia $q_1, \ldots, q_t$ az $X = \{x_1, \ldots, x_n\}$ adatbázis felett. Mindegyik q_i lekérdezés

a (Q_i, AVG) formájú, ahol $Q_i \subseteq \{1, 2, \ldots, n\}$ a lekérdező halmaz és minden x_i a $[\alpha, \beta]$ véges intervallumból veszi az értékeit, $\beta > \alpha$ feltétel mellett. Jelöljük továbbá MAX-al a $x_1, \ldots, x_n$ értékek maximumát, $maximum\{x_1, \ldots, x_n\}$.

- Adottak az első t $q_1, \ldots, q_t$ kérdés és azokhoz tartozó t válasz $a_1, \ldots, a_t$. Az offline query auditor feladata detektálni, hogy MAX teljesen kiszivárgott-e ezen kérdések és válaszok alapján.
- Adottak az első $(t-1)$ $q_1, \ldots, q_{t-1}$ kérdés és azokhoz tartozó $(t-1)$ válasz $a_1, \ldots, a_{t-1}$. Közben érkezett a q_t-ik kérdés, és az online auditor az a feladata, hogy eldöntse szabad-e válaszolni a kérdésre vagy nem, hogy MAX értékét ne lehessen kiszámolni az eddigi kérdések és válaszok alapján.

A query auditornak ezt az osztályát, amely értékek részhalmazainak az átlagát lehet kérdezni és MAX értékét szeretnénk megvédeni, $\text{Auditor}_{avg}^{max}$-nak nevezem. A disszertációmban leginkább a MAX értékének védelmét mutattam be, a minimum érték védelme is hasonló módon tervezhető, amiről részletesen a [Th10]-ban tárgyalok.

3. Téziscsoport. *Javasoltam három $\text{Auditor}_{avg}^{max}$ tipusú query auditort: Egy-egy polinomiális idejű offline és online $\text{Auditor}_{avg}^{max}$ tipusú auditort a teljes felfedési modellben, valamint egy szimulálható online $\text{Auditor}_{avg}^{max}$ auditort a részleges felfedési modellben [Th09].*

5.3.1. Offline és Online $\text{Auditor}_{avg}^{max}$ tipusú auditor a teljes felfedési modellben

3.1. Tézis. *Javasoltam egy offline $\text{Auditor}_{avg}^{max}$ tipusú auditort a teljes felfedési modellben. Az általam javasolt offline $\text{Auditor}_{avg}^{max}$ auditor a jól ismert lineáris optimizációs problémán alapul. Megmutattam, hogy a javasolt auditor pontos, tehát ha az auditor detektálja, hogy MAX értéke teljesen kiszivárgott vagy nem, akkor tényleg ez áll fennt.*

A javasolt offline auditor: Az offline $\text{Auditor}_{avg}^{max}$ auditor problémáját visszavezetem a lineáris programozás illetve lineáris optimizációs problémájára. A t darab kérdést egy $t \times n$-es $\bar{A}$ mátrix-al tudjuk reprezentálni. $\bar{A}$ mindegyik sora $r_i = (a_{i,1}, \ldots, a_{i,n})$ egy Q_i kérdéshalmazt reprezentál, ahol $a_{i,j}$, $1 \leq i, j \leq n$, értéke 1 ha $x_j \in Q_i$, és egyébként 0. A kérdésekhez tartozó megfelelő válaszokat egy oszlopvektorral reprezentáljuk $\bar{b} = (b_1, \ldots, b_t)^T$, amelyben b_i a q_i kérdésre adott válasz.

Mivel mindegyik x_i egy $[\alpha, \beta]$ zárt intervallumból veszi az értékét, a következő lineáris egyenletrendszert (más néven a feasible set) kapjuk:

$$\mathcal{L} = \begin{cases} \bar{A}\bar{x} = \bar{b}, \text{where } \bar{x} \text{ is the vector } (x_1, \ldots, x_n)^T. \\ \alpha \leq x_i \leq \beta, \forall x_i : x_i \in \{x_1, \ldots, x_n\} \end{cases}$$

Ezután a $maximize(x_i)$ célfüggvényt hozzácsatolva a $\mathcal{L}$-hez megkapjuk n darab lineáris programozási problémát, P_i, ahol $i \in \{1, \ldots, n\}$. Legyen $x_i^{max} = maximize(x_i)$, ekkor az $x_1, \ldots, x_n$ maximuma az n darab maximális értéknek a maximuma, azaz $x^{opt} = max\{x_1^{max}, \ldots, x_n^{max}\}$.

Jelöljük $\mathcal{P}$-vel a fent említett teljes lineáris programozási problémát az x^{opt} meghatározásához. Megjegyzem, hogy a $\mathcal{P}$ által visszaadott x^{opt} lehet pontos vagy becsült maximum. Pontos maximum akkor lehet az x^{opt} ha (i) $\mathcal{L}$-nek egyértelmű megoldása van, vagy (ii) $\mathcal{L}$-nek nincsen egyértelmű megoldása, de van olyan x_i amire megtudjuk mondani, hogy $x_i = x_{opt}$. Egyébként x^{opt} a pontos maximumnak a legjobb becslése. Megjegyzem, hogy a mi esetünkben a mindig van az egyenletrendszernek megoldása, mivel $x_1, \ldots, x_n$ létező értékek, amit már az adatbázisban tárolódnak.

A fent definiált lineáris programozási probléma alapján az általam javasolt offline auditor a következő lépéseket hajtja végre. Adott t lekérdezés $q_1, \ldots, q_t$ az $X = \{x_1, \ldots, x_n\}$ adathalmaz

felett, és a hozzájuk tartozó válaszok. Azt mondjuk, hogy a MAX értéke teljesen kiszivárgott (vagy fel van fedve) ha a következő két feltétel közül bármelyik érvényes:

- (F1) Amikor $\mathcal{L}$-nek egyértelmű megoldása van, a MAX értéke egyenlő az x^{opt}-vel.
- (F2) Amikor $\mathcal{L}$-nek nincsen egyértelmű megoldása, de van olyan x_i amire megtudjuk mondani, hogy $x_i = x_{opt}$, akkor MAX értéke egyenlő x_i-vel.

Egyébként a támadó nem tudja egyértelműen kiszámolni a MAX értékét.

3.2. Tézis. *Javasoltam két variánst a polinomiális idejű online Auditor$^{max}_{avg}$ tipusú query auditorból a teljes felfedési modellben. Az általam javasolt auditorok a jól ismert lineáris optimizációs problémán alapul. Megmutattam, hogy az általam ajánlott online auditorok védelmet nyújtanak a MAX érték kiszivárgása ellen, a teljes felfedési modellben.*

Az általam ajánlott online auditor (a disszertációm 4.6. fejezetéből): Tekintsük az első $t-1$ kérdés és hozzájuk tartozó választ az $X = \{x_1, \ldots, x_n\}$ adathalmaz felett. Amikor egy újabb q_t kérdés érkezik, akkor az online auditor feladata eldönteni valósidőben, hogy válaszol vagy megtagadja a választ, hogy ne szivárogjon ki a MAX értéke a teljes felfedési modellben. Az általam javasolt online auditor variánsok a lineáris optimizációs problémán alapulnak.

Algorithm 2/a: Online auditor Auditor$^{max}_{avg}$

Inputs: $q_1, \ldots, q_t$, $a_1, \ldots, a_t$, d_{tr}, α, β;

Let $\mathcal{L}^*_t$ be the feasible set formed by the t queries/answers

Let x^{opt}_t be the returned maximum by solving $\mathcal{P}$ with $\mathcal{L}^*_t$

if $|x^{opt}_t - MAX| > d_{tr}$ AND $(MAX - max_t) > d_{tr}$ **then** output a_t; **endif**

else if $|x^{opt}_t - MAX| \leq d_{tr}$ OR $(MAX - max_t) \leq d_{tr}$ **then** output DENY; **endif**

Algorithm 2/b: Online auditor Auditor$^{max}_{avg}$

Inputs: $q_1, \ldots, q_t$, $a_1, \ldots, a_t$, d_{tr}, α, β;

Let $\mathcal{L}_t$ be the feasible set formed by the t queries/answers

if with $\mathcal{L}_t$ the linear equation system has unique solution **then** output DENY; **return**; **endif**

else if there is a x_i that can be uniquely determined **then**

  if $(MAX - x_i) > d_{tr}$ AND $(MAX - max_t) > d_{tr}$ **then** output a_t; **return**; **endif**

  else if $(MAX - x_i) \leq d_{tr}$ OR $(MAX - max_t) \leq d_{tr}$ **then** output DENY; **return**; **endif**

endif else output a_t;

A fenti táblázatban a $|x^{opt} - MAX|$-t az x^{opt} és MAX távolsága, valamint max_t jelöli az első t válasz maximumát. d_{tr} egy biztonsági küszöbértéket jelöli, hogy legrosszabb esetben milyen közel engedjük a kérdezőt a MAX értékéhez.

5.3.2. Szimulálható Auditor$^{max}_{avg}$ auditor a részleges felfedési modellben

3.3. Tézis. *Javasoltam egy hatékony szimulálható Auditor$^{max}_{avg}$ tipusú query auditort a probabilisztikus felfedési modellben (ami a részleges felfedési modellnek az egyik osztálya). Az általam javasolt*

auditor a [26]-ban publikált hatékony véletlen mintavételezési módszert alkalmazza, valamint a sztatisztikában ismert Chernoff bound és Union boundon alapul. Megmutattam továbbá, hogy az általam javasolt auditor szimulálható, és emiatt bizonyíthatóan biztosítja a MAX kiszivárgása elleni védelmet.

Ebben a fejezetben bemutatom az általam javasolt $\text{Auditor}_{avg}^{max}$ tipusú auditort a probabilisztikus modellben, ami rendelkezik a szimulálhatósági tulajdonsággal. Tekintsük egy tetszőleges $X = \{x_1, \ldots, x_n\}$ adathalmazt, amelyben mindegyik x_i-t egymástól függetlenül választjuk ki a $\mathcal{H}$ eloszlás mellett az $(-\infty, \infty)$ intervallumban. Legyen továbbá $\mathcal{D} = \mathcal{H}^n$ az együttes eloszlás függvény.

A probabilisztikus felfedési modellben az úgynevezett λ-Safe és AllSafe prédikátumok definiálják a biztonság fogalmát.

4. Definició. *A t kérdésből és válaszból álló $q_1, \ldots, q_t$, $a_1, \ldots, a_t$ szekvenciáról akkor mondjuk, hogy λ-Safe az $I \subseteq [\alpha, \beta]$ intervallumra vonatkozóan ha a következő logikai prédikátum* 1*-re értékelődik.*

$Safe_{\lambda,I}(q_1, \ldots, q_t, a_1, \ldots, a_t) =$

$$\begin{cases} 1 & ha\ 1/(1+\lambda) \leq \frac{P_{\mathcal{G}_{post}^t}(MAX \in I | \wedge_{j=1}^t (avg(Q_j) = a_j))}{Pr_{\mathcal{G}_{max}}(MAX \in I)} \leq (1+\lambda) \\ 0 & egyébként \end{cases}$$

ahol $\mathcal{G}_{post}^t$ a posteriori valószinüség és $\mathcal{G}_{max}$ a MAX eloszlása. Az AllSafe definiciója ezután a $[\alpha, \beta]$-n vett J ω-szignifikáns intervallumokra értelmezzük. Az ω-szignifikáns intervallumok olyan intervallumok, amelyekre a $P_{\mathcal{G}_{max}}(\text{MAX} \in J) \geq \frac{1}{\omega}$ feltétel fennáll. Az auditor megtervezése során csak a ω-szignifikáns intervallumokat veszem figyelembe.

5. Definició. $AllSafe_{\lambda,\omega}(q_1, \ldots, q_t, a_1, \ldots, a_t) =$

$$\begin{cases} 1 & ha\ Safe_{\lambda,J}(q_1, \ldots, q_t, a_1, \ldots, a_t) = 1, \forall\ J \\ 0 & egyébként \end{cases}$$

A probabilisztikus felfedési modellben a randomizált auditorok definicióját veszük figyelembe.

6. Definició. *A randomizált auditor a $q_1, \ldots, q_t$ kérdéseknek, az X adathalmaznak, és a D eloszlásnak olyan randomizált függvénye, amely akár válaszolhat akár megtagadhatja a válasz.*

A következőben a (λ, ω, T)-privacy játék és a (λ, δ, ω, T)-private auditor fogalmát részletezem. Egy támadó és egy auditor között definiált (λ, ω, T)-privacy játék a következő:

1. A támadó kiadja a $q_t = (Q_t, f_t)$ kérdést.
2. Az auditor eldönti, hogy válaszol-e a q_t-re, majd ha igen akkor visszaküldi a $a_t = f_t(Q_t)$-t, egyébként elutasítja.
3. A támadó nyer ha $\text{AllSafe}_{\lambda,\omega}(q_1, \ldots, q_t, a_1, \ldots, a_t) = 0$.

7. Definició. *Azt mondjuk, hogy egy auditor (λ, δ, ω, T)-private ha tetszőleges A támadóra igaz, hogy*

$$P\{A \text{ megnyeri a } (\lambda, \omega, T)\text{-privacy játékot}\} \leq \delta.$$

Az általam javasolt probabilisztikus $\text{Auditor}_{avg}^{max}$ auditor a disszertációm 4.7. fejezetében levő 3-as és 4-es algoritmusok valósítják meg. Az auditorról bebizonyítottam (a disszertáció 4.7. fejeztében), hogy a fent tárgyalt 7-es definiciónak megfelel.

6. Konklúzió

A disszertációmban a vezeték nélküli szenzor hálózatokra (WSN) vonatkozó különböző biztonsági kérdésekkel foglalkozom. Új formális és automatizált ellenőrzési módszereket javasoltam WSN-nekre tervezett protokollok biztonsági ellenőrzéséhez, valamint új query auditálási algoritmusokat érzékeny adatok kiszivárgása elleni védelmére. A disszertációm három téziscsoportból áll, amelyek három különböző kutatási témához kapcsolódnak.

Az első téziscsoport tartalmazza a következő fő kontribúciókat: Javasoltam egy új processz algebrai variánst, az *sr*-kalkulus, amely nagy kifejező erejű szintaxist és szemantikát biztosít a (i) kriptográfiai primitivek és műveletek, (ii.) a broadcast kommunikáció jellemzőit, (iii.) a szomszédság definicióját, amik szükségesek a biztonsági útvonal-választó protokollok modellezéséhez és ellenőrzéséhez. Ezekivül javasoltam egy szisztematikus és kimerítő bizonyítási technikát, a BDSR-t, amelyet kombinálva az *sr*-kalkulussal a bonyolutabb útvonal-választó protokollokat is tudom analízálni formálisan.

Továbbá, javasoltam egy teljesen automatizált ellenőrzési módszert, az *sr-verif*t, biztonsági útvonal-választó protokollok ellenőrzésére. Az *sr*-verif az általam javasolt BDSR technikának a logikai dedukciós megvalósítása. A módszeremnek a biztonsági útvonal-választó protokollokra optimalizált és kifejező szintaxisa és szemantikája van. Másik előnye a kapcsolódó munkákkal szemben, hogy specifikus hálózati topológia helyett tetszőleges topológiát feltételez.

Felhasználva a javasolt módszereimet bebizonyítottam, hogy az *DSR*, *SRP*, *Ariadne* és *endairA* ismert útvonal-választó protokollok sérülékenyek az útvonal hamisító támadásra. Bebizonyítottam, hogy az *endairA* biztonságos egy darab támadó csomópont esetén.

A második téziscsoport illetően a legfontosabb eredményeim a következőek: Javasoltam egy probabilisztikus időzített kalkulust, a $crypt_{time}^{prob}$-t, amelynek kifejező szintaxisa és szemantikája lehetővé teszi olyan rendszerek és protokollok modellezését és ellenőrzését amik tartalmazzák a következő három tulajdonság egyikét vagy mindegyiket: (i) kriptográfiai műveletek, (ii) probabilisztikus viselkedés, (iii) órai időzítések. A legjobb tudomásom szerint ez az első olyan algebrai nyelv, amely

támogatja mind ezt a három tulajdonságot egyszerre. Demonnstráltam a $crypt_{time}^{prob}$ használhatóságát WSN transzport protokollok ellenőrzésére. Modelleztem és ellenőriztem a más szerzők által javasolt DTSN és SDTP protokollokat. Formálisan bebizonyítottam, hogy (i) a DTSN protokoll sebezhető az üzenetet modósító és hamisító támadásokkal;(ii) az SDTP protokoll biztonságos az üzenetet modósító és hamisító támadásokkal szemben, ha egy támadó csomópontot feltételezünk; (iii) az SDTP protokoll sérülékeny két támadó csomópontot esetén. Figyelembe véve az DTSN és SDTP-ben található biztonsági lyukakat, javasoltam egy új biztonsági WSN transport protokoll, az SDTP$^+$-t, és bebizonyítottam, hogy a sikeres támadások a DTSN és SDTP protokollok ellem nem mükönek az SDTP$^+$ esetében.

Továbbá javasoltam egy automatizált ellenőrzési módszert, amely a több egyéb területen használt PAT process analysis toolkit használatán alapul. Tudomásom szerint a PAT toolkitet még nem használták WSN transzport protokollok elemzésére. A PAT toolkitet használva specifikáltam a DTSN és a SDTP protokollok müködését és a PAT segítségével automatizáltan elemeztem a két protokollt különböző támadási forgatókönyvük szerint.

Végül a harmadik téziscsoportban a következő eredményeket értem el: Egy újszerű query auditálási beállítást vizsgálom, ahol az érzékeny adat amit megakarunk védeni egy adathalmazban levő elemeknek vmilyen aggregált értéke. Konkrétan a kérdező bizonyos tárolt adatokra kiszámolt átlagra kérdezhet rá, és a cél, hogy az adathalmaz maximuma (minimuma) ne szivárogjon ki. Ez a beállítás például a kórházi környzetben lehet fontos ahol betegektől mért adatoknak szélső értékei valamilyen betegségekre utalhatnak, ami érzékeny információ. Ebben a modellben javasoltam három fajta query auditort, az offline, az online és a probabilisztikus auditorokat.

Hivatkozások

[1] M. Abadi and A. Gordon. A calculus for cryptographic protocols: the Spi calculus. Technical Report SRC RR 149, Digital Equipment Corporation, Systems Research Center, January 1998.

[2] G. Acs, L. Buttyan, and I. Vajda. Provable security of on-demand distance vector routing in wireless ad hoc networks. In *In In Proceedings of the Second European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS 2005*, pages 113–127, 2005.

[3] G. Acs, L. Buttyan, and I. Vajda. Provably secure on-demand source routing in mobile ad hoc networks. In *IEEE Transactions on Mobile Computing*, volume 5, 2006.

[4] G. Acs, L. Buttyan, and I. Vajda. The security proof of a link-state routing protocol for wireless sensor networks. In *IEEE Workshop on Wireless and Sensor Networks Security*, 2007.

[5] Charu C. Aggarwal and Philip S. Yu, editors. *Privacy-Preserving Data Mining - Models and Algorithms*, volume 34 of *Advances in Database Systems*. Springer, 2008.

[6] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury. A survey on wireless multimedia sensor networks. *Computer Networks*, 51(4):921–960, 2007.

[7] Todd R. Andel and Alec Yasinsac. Automated evaluation of secure route discovery in manet protocols. In *SPIN '08: Proceedings of the 15th international workshop on Model Checking Software*, pages 26–41, 2008.

[8] J. Bengtsson and F. Larsson. Uppaal a tool for automatic verification of real-time systems. *Technical Report,Uppsala University, (96/67)*, 1996.

[9] Bruno Blanchet. Automatic Proof of Strong Secrecy for Security Protocols. In *IEEE Symposium on Security and Privacy*, pages 86–100, Oakland, California, May 2004.

[10] L. Buttyan and L. Csik. Security analysis of reliable transport layer protocols for wireless sensor networks. In *Proceedings of the IEEE Workshop on Sensor Networks and Systems for Pervasive Computing (PerSeNS)*, pages 1–6, Mannheim, Germany, March 2010.

[11] L. Buttyan and A. M. Grilo. A Secure Distributed Transport Protocol for Wireless Sensor Networks. In *IEEE International Conference on Communications*, pages 1–6, Kyoto, Japan, June 2011.

[12] L. Buttyán and I. Vajda. Towards provable security for ad hoc routing protocols. In *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pages 94–105, 2004.

[13] Francis Chin. Security problems on inference control for sum, max, and min queries. *J. ACM*, 33:451–464, May 1986.

[14] Francis Chin and Gultekin Ozsoyoglu. Auditing for secure statistical databases. In *Proceedings of the ACM '81 conference*, pages 53–59, New York, NY, USA, 1981.

[15] D. Coppersmith and M. Jakobsson. Almost optimal hash sequence traversal. In *Fourth Conference on Financial Cryptography*, pages 102–119, Southampton, Bermuda, March 2002.

[16] PedroR. D'Argenio and Ed Brinksma. A calculus for timed automata. In Bengt Jonsson and Joachim Parrow, editors, *Formal Techniques in Real-Time and Fault-Tolerant Systems*, volume 1135 of *Lecture Notes in Computer Science*, pages 110–129. Springer Berlin Heidelberg, 1996.

[17] C. Fournet and M. Abadi. Mobile values, new names, and secure communication. In *In Proceedings of the 28th ACM Symposium on Principles of Programming, POPL'01*, pages 104–115, 2001.

[18] Jens Chr. Godskesen. A calculus for mobile ad hoc networks. In *COORDINATION*, pages 132–150, 2007.

[19] Jens Chr. Godskesen. A calculus for mobile ad-hoc networks with static location binding. *Electron. Notes Theor. Comput. Sci.*, 242(1):161–183, 2009.

[20] Jean Goubault-Larrecq, Catuscia Palamidessi, and Angelo Troina. A probabilistic applied piâcalculus. In Zhong Shao, editor, *Programming Languages and Systems*, volume 4807 of *Lecture Notes in Computer Science*, pages 175–190. Springer Berlin Heidelberg, 2007.

[21] Y. C. Hu, D. B. Johnson, and A. Perrig. Secure efficient distance vector routing in mobile wireless ad hoc networks. *Ad Hoc Networks*, 1(1):175–192, July 2003.

[22] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: a secure on-demand routing protocol for ad hoc networks. *Wirel. Netw.*, 11(1-2):21–38, 2005.

[23] Krishnaram Kenthapadi, Nina Mishra, and Kobbi Nissim. Simulatable auditing. In *In ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, PODS*, pages 118–127, 2005.

[24] M. Kwiatkowska, G. Norman, and D. Parker. PRISM 4.0: Verification of probabilistic real-time systems. In G. Gopalakrishnan and S. Qadeer, editors, *Proc. 23rd International Conference on Computer Aided Verification (CAV'11)*, volume 6806 of *LNCS*, pages 585–591. Springer, 2011.

[25] Ruggero Lanotte, Andrea Maggiolo-Schettini, and Angelo Troina. Weak bisimulation for probabilistic timed automata. In *PROC. OF SEFMdž˝03, IEEE CS*, pages 34–43. Press, 2003.

[26] László Lovász and Santosh Vempala. The geometry of logconcave functions and sampling algorithms. *Random Struct. Algorithms*, 30:307–358, May 2007.

[27] John D. Marshall, II, and Xin Yuan. An analysis of the secure routing protocol for mobile ad hoc network route discovery: Using intuitive reasoning and formal verification to identify flaws. Technical report, THE FLORIDA STATE UNIVERSITY, 2003.

[28] R. C. Merkle. Protocols for Public Key Cryptosystems. In *Symposium on Security and Privacy*, pages 122–134, California, USA, April 1980.

[29] Robin Milner, Joachim Parrow, and David Walker. A calculus of mobile processes, parts i and ii. *Inf. Comput.*, 100(1):1–77, September 1992.

[30] Shubha U. Nabar, Bhaskara Marthi, Krishnaram Kenthapadi, Nina Mishra, and Rajeev Motwani. Towards robustness in query auditing. In *International Conference on Very Large Data Bases (VLDB)*, pages 151–162, 2006.

[31] P. Papadimitratos and Z.J. Haas. Secure routing for mobile ad hoc networks. In *In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, pages 1–13, 2002.

[32] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar. SPINS: security protocols for sensor networks. In *ACM MobiCom*, Rome, Italy, July 2001.

[33] Mayank Saksena, Oskar Wibling, and Bengt Jonsson. Graph grammar modeling and verification of ad hoc routing protocols. In *Proceedings of the Theory and practice of software, 14th international conference on Tools and algorithms for the construction and analysis of systems*, TACAS'08/ETAPS'08, pages 18–32, Berlin, Heidelberg, 2008. Springer-Verlag.

[34] Steve Schneider. *Concurrent and Real Time Systems: The CSP Approach*. John Wiley & Sons, Inc., New York, NY, USA, 1st edition, 1999.

[35] Anu Singh, C. R. Ramakrishnan, and Scott A. Smolka. A process calculus for mobile ad hoc networks. *Sci. Comput. Program.*, 75(6):440–469, 2010.

[36] Jun Sun, Yang Liu, and Jin Song Dong. Model checking csp revisited: Introducing a process analysis toolkit. In *In ISoLA 2008*, pages 307–322. Springer, 2008.

[37] O. Wibling, J. Parrow, and A. Pears. Automatized verification of ad hoc routing protocols. *Formal Techniques for Networked and Distributed Systems FORTE*, pages 343–358, 2004.

[38] J. Yicka, B. Mukherjeea, and D. Ghosal. Wireless sensor network survey. *Computer Networks*, 52(12):2292–2330, Aug. 2008.

Publications

[Th01] Levente Buttyán and Ta Vinh Thong. Biztonsági API analízis a spi-kalkulussal. *Híradástechnika*, LXII(8):16–21, July 2007. (in Hungarian).

[Th02] Levente Buttyán and Ta Vinh Thong. Security API analysis with the spi-calculus. *Híradástechnika*, LXIII(1):43–49, April 2008.

[Th03] Frank Kargl, Panagiotis Papadimitratos, Levente Buttyán, Michael Mueter, Elmar Schoch, Bjorn Wiedersheim, Ta Vinh Thong, Gorgio Calandriello, Albert Held, Antinio Kung, and Jeanpierre Hubaux. Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges. *IEEE Communications Magazine*, 46(11):110–118, November 2008.

[Th04] Levente Buttyán, Gábor Pék, Ta Vinh Thong. Consistency verification of stateful firewalls is not harder than the stateless case. *Infocommunications Journal*, LXIV(2009/2-3):2–8, March 2009.

[Th05] Levente Buttyán and Ta Vinh Thong. Formal verification of secure ad-hoc network routing protocols using deductive model-checking. In *IFIP Wireless and Mobile Networking Conference (WMNC 2010)*, IFIP, pp 1–6, Budapest, 2010.

[Th06] Levente Buttyán and Ta Vinh Thong. Formal verification of secure ad-hoc network routing protocols using deductive model-checking. *Periodica Polytechnica Electrical Engineering Journal*, Vol. 1245, pp 1–20, 2011.

[Th07] Ta Vinh Thong and Levente Buttyán. On automating the verification of secure ad-hoc network routing protocols. *Telecommunication Systems Journal, Springer*, ISSN 1572-9451, pp 1–28, August 2011.

[Th08] Ta Vinh Thong. Formal verification of secure ad-hoc network routing protocols using deductive model-checking. *Cryptology Eprint Archive, IACR*, 1–77, March 2012.

[Th09] Ta Vinh Thong and Levente Buttyán. Query Auditing for Protecting Max/Min Values of Sensitive Attributes in Statistical Databases. In *9th International Conference on Trust, Privacy, Security in Digital Business (Trustbus 2012)*, Springer LNCS, Volume 7449, pp 192–206, July 2012, Wien.

[Th10] Ta Vinh Thong and Levente Buttyán. Query Auditing for Protecting Max/Min Values of Sensitive Attributes in Statistical Databases. *Technical Report, pp. 1–15, 2012, CrySyS Lab., BME*

[Th11] Amit Dvir, Levente Buttyán, Ta Vinh Thong. SDTP+: Securing a Distributed Transport Protocol for WSNs using Merkle Trees and Hash Chains. In *IEEE International Confenrence on Communications (ICC 2013)*, *Communication and Information Systems Security Symposium*, IEEE, pp 1–6, June 2013, Budapest.

[Th12] Ta Vinh Thong and Amit Dvir. On Formal and Automated Security Verification of WSN Transport Protocols. *Cryptology Eprint Archive, IACR*, 1–81, January 2013.

[Th13] Ta Vinh Thong and Levente Buttyán and Amit Dvir. On Formal and Automated Security Verification of WSN Transport Protocols. *International Journal of Distributed Sensor Networks, Hindawi*, 1–28. (submitted on May 3, 2013).