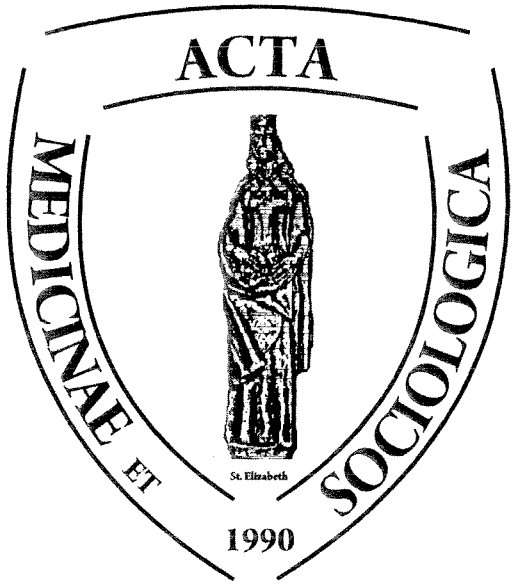
Acta

Medicinae et Sociologica



Vol .1. No.1. 2010

Debreceni Egyetem
Egészségügyi Kar, Nyíregyháza

Acta Medicinae et Sociologica

1. évfolyam 1. szám 2010
Volume 1. No.1. 2010

Alapítás éve: 2010

Főszerkesztő:
Dr. Kiss János

Szerkesztőbizottság:
DE-EK Tudományos Tanácsadó Bizottság

Felelős Kiadó:
Debreceni Egyetem
Orvos- és Egészségügyi Centrum
Egészségügyi Kar

Szerkesztőség:
4040 Nyíregyháza, Sóstói 2-4.
Tel.: (42) 404-411, Fax: (42) 408-656
e-mail: info@de-efk.hu
Nyomdai előkészítés: Dr. Takács Péter

Megjelenik félévente

HU – ISSN 2062-0284

Tartalomjegyzék

Berényi Dénes
Gondolatok az Acta Medicinae et Sociologica megjelenése alkalmából 5

Kiss János
Az első szám elé 7

Steve Drewry, Thomas R. Lawson
Operationalizing Codes of International Research Ethics: The Role of Social Work 9

András Kulja, Mariia Mudryk, Taissiya Symochko, Larysa Bugyna, Nelya Koval, Anna Tereshchenko, Nadiya Boyko
Peculiarities and statistical investigation of food consumption Ukraine 23

Jóna György, Kriszbacher Ildikó, Lukácskó Zsolt
Irányított verseny - Irányított betegellátás 33

Zolnai Erika
Az intézményi kultúra és a felelősségvállalás szerepe az értelmi sérült emberek biztonságon alapuló intézményi ellátása során 53

Szoboszlai Katalin
Hajléktalanság kialakulása az életútban 71

Takács Péter
Többcsatornás kriptográfiai protokollok formális vizsgálata - MANA III 97

Szerzőink 121

UNIVERSITY
OF DEBRECEN
FACULTY OF
HEALTH
NYÍREGYHÁZA

ACTA
MEDICINAE ET SOCIOLOGICA
1990

ACTA
MEDSOC
VOLUME 1.
2010

Többcsatornás kriptográfiai protokollok formális vizsgálata - MANA III -

Takács Péter

Debreceni Egyetem, Egészségügyi Kar,
Egészségügyi Informatika Tanszék
e-mail: vtp@de-efk.hu

Abstract. Formal verification of multi-channel cryptographic protocols - MANA III. The topic of this paper is to examine cryptographic protocols based on formal methods. As the original sources of the CSN-logic do not reflect the expected exactitude of the mathamatical logic, we present a remodelled CSN-logic. A multi-sorted modal logic and its notation is given. We modify the axiom system in a lesser degree. We apply the extended logic to verify validity of MANA III protocol.

Keywords: cryptographic protocols, formal verification, CSN-logic, MANA III protocol

Lektor: Dr. Vályi Sándor Ph.D, főiskolai docens, Nyíregyházi Főiskola

1. Bevezetés

Kommunikáló partnerek sok esetben több információs csatornát is képesek használni. A dolgozat célja többcsatornás rendszerek matematikai logikai eszközökkel történő vizsgálatának bemutatása. Munkánk során a Coffey-Saidha-Newe-féle (a továbbiakban: CSN) logikai rendszert bővítjük a többcsatornás kommunikáció leírásának és kezelésének lehetőségeivel. Az új rendszert már ismert és gyakorlatban is alkalmazott többcsatornás kriptográfiai protokollok biztonsági elemzésére használjuk fel. Jelen írásban a MANA III protokoll elemzését mutatjuk be.

A CSN-logikai rendszer két közleményben jelent meg. Elsőr 1997-ben T. Coffey és P. Saidha tette közzé az alaprendszert. [1] Ebben a cikkben a nyilvános kulcsú titkosítást használó protokollok számára kidolgozott elmélet látott napvilágot. Ezt követően 2003-ban jelent meg a Newe és T. Coffey írása, amely kibővítette a modellt a titkos kulcsú titkosítást alkalmazó rendszerek körére. Mindezek a [11] és [12] dolgozatokban érhetők el.

Mivel az eredeti források nem tükrözik teljes mértékben a matematikai logika elvárt precizitását, itt saját átdolgozott rendszerünket mutatjuk be. Munkánk során tovább pontosítjuk az alkalmazott logikai nyelvet, a jelölésrendszert, a következtetési szabályokat. Kisebb módosításokat eszközlünk az axiómák körében is. A teljes rendszer a közlemény mellékletében kapott helyet - a továbbiakban az ott lévő jelöléseket és számozási rendszert alkalmazzuk. A szerzőkre utalva továbbra is a CSN-logika nevet használjuk.

A bővített CSN-logika alkalmazásaként vizsgált MANA III protokollról [4]-ben olvashatunk.

További kapcsolódási pontként kell megemlítenünk Wong F-L. és Stajano F. 2005-ben megjelent cikkét, amely a többcsatornás kriptográfiai protokollok körében a MANA protokollcsaládot vizsgálja. [16] Írásukban a MANA I, II és III protokollok kerülnek elemzésre valószínűségszámítási eszközök felhasználásával. A cikk végén a szerzők jelzik, hogy aktuális feladat egy olyan rendszer kidolgozása, amely lehetővé tenné a többcsatornás protokollok logikai alapú vizsgálatát. Munkánk során ezen az úton indultunk el, és alkalmaztuk eredményeinket a már említett MANA protokollcsalád egyes elemeire. Hasznos összefoglalását találja az érdeklődő még a többcsatornás kriptográfiai protokollok körének Wong és Stajano 2007-ben megjelent cikkében, amely a tudományterület aktuális helyzetét foglalja össze. [17]

2. A kriptográfiai- és a többcsatornás protokollok

A kriptográfiai protokollok olyan kommunikációs protokollok, amelyek célja a partnerek biztonságos, védett és ellenőrzött kommunikációjának biztosítása. A protokollok elmélete a támadások detektálásától kezdve a protokollok különböző eszközökkel történő vizsgálatára vállalkozik. Napjainkban erősödött meg az az irányzat, amely külön vizsgálja a protokollokban szereplő csatornák szerepét és jelentőségét. Ez a vonulat kapcsolódik a „mindenütt jelen lévő, láthatatlan számítástechnika" (*ubicomp - ubiquitous computing*, vagy *pervasive computing*) fogalmához. Az újonnan megjelenő számítástechnikai és informatikai eszközök már az egymáshoz kapcsolódás képességével, a vezetékes, vagy vezeték nélküli kommunikációval vannak felruházva. Kialakult a PAN (*Personal Area Network* - Személyes hálózat) fogalomköre és technológiája, amelynek kommunikációs protokolljai eltérnek az Internet és a mobilhálózatok eddig felépített protokolljaitól. [6][15]

Részletesen és behatóan tanulmányozva a tradicionális (titkos kulcsú) kriptográfiai rendszereket, könnyen megtaláljuk többcsatornás protokollok alapjait. Például a protokollokban szereplő titkos kulcsú kommunikáció kulcsát egy védett csatornán kell eljutatni a parnerhez, ami jelentheti egy futár alkalmazását, vagy személyes találkozáskor lebonyolított kulcscserét. Hasonló megoldások találhatók különböző elektronikus pénzkezelési megoldásokban, eBank rendszerekben is.

Elmondhatjuk tehát, hogy több csatorna használata nem jelent lényegesen új eszközt a kritptográfiában, viszont az ilyen megoldások megalapozott tudományos vizsgálata még csak napjainkban zajlik. Ahhoz, hogy részletesebben ismertessük elért eredményeinket, be kell mutatnunk a protokollok formális vizsgálatát.

3. A kriptográfiai protokollok formális vizsgálata

A kriptográfiai kutatások napjainkra két fő irányzatot alakítottak ki. Az egyik a számításelméleti megközelítés (főleg valószínűségelméleti és komplexitáselméleti eszközök alkalmazása), a másik pedig a formális megközelítés (főleg modális logikai eszközök). [5] A formális módszerek kriptográfiai protokollok tervezésének és ellenőrzésének különböző szakaszaiban használhatók. A leginkább kutatott az ellenőrzés (verifikáció) szakasza. A bővített CSN logika a modális logika alkalmazását jelenti a verifikáció során. A modális logika alkalmazásának sémája a kriptográfiai protokollok ellenőrzése során a következő: 1. lépésben a vizsgált protokollt kell formalizálni. 2. lépés a kezdeti feltételek meghatározása. 3. lépésként a protokoll céljait kell megfogalmazni. 4. lépés a logikai posztulátumok alkalmazását jelenti. 5. lépés a negyedik lépés esedményeinek és a protokoll céljainak (harmadik lépés) összevetését jelenti.

4. A CSN-logika és bővítése

A CSN-logika egy többtípusú, multi-modális elsőrendű levezetési rendszer. A többtípusú logika akkor használatos, ha a vizsgált objektumok nem alkotnak homogén halmazt. Többtípusú logikák lefordíthatók egytípusú, hagyományos elsőrendű logikává. A modális operátorok alkalmazásával az állítások eredeti jelentése módosítható. Egy modális logika eredetileg egy klasszikus logikai rendszer bővítése a *„szükségszerű"* és a *„lehetséges"* kifejezésekkel.[1] A CSN-rendszer többek között a

[1] Jelekben: a *szükségszerűség* operátora: $\Box$ a *lehetségesség* operátora: $\Diamond$. $\Box$ és $\Diamond$ egymásból kifejezhetők: $\Box\alpha \leftrightarrow \neg\Diamond\neg\alpha$ és $\Diamond\alpha \leftrightarrow \neg\Box\neg\alpha$ (α formula). A $\Box$ operátornak többféle értelmezése

K-val (*knowledge* - tud, ismer) és a B-vel (*belief* - hisz, bízik) jelölt operátorokat vezeti be, amivel egy multi-modális logikát hoz létre.

A levezetési rendszer egy klasszikus elsőrendű levezetési rendszerből indul ki, bővítve azt többek között az új operátorokra vonatkozó levezetési szabályokkal (például: $R2(a)$, $R2(b)$) és axiómákkal (például: $A1(a)$, $A1(b)$, $A2(a)$).

Egy másik osztályozás szerint a CSN-rendszer episztemikus-doxatikus[2] rendszer. [9] E szemléletmód szerint a rendszer kidolgozói abból indultak ki, hogy két tendencia figyelhető meg a kriptográfiai protokollok logikai vizsgálatában. Az egyik a bizalom/megbízhatóság fejlődésének vizsgálata a protokoll lépései során (*logics of belief*), a másik a protokollok működésére alapozott tudás (protokoll szereplőinek ismerete) elemzése (*logics of knowledge*). A CSN-logika célja a kétféle megközelítés ötvözése, lehetővé téve ezáltal a kriptográfiai protokollok szélesebb körű és mélyebb vizsgálatát.

A logikai modellünk egyik kiinduló célja a partnerek közötti védett kommunikáció leírása (formalizálás). Ennek során legelőször a modell típusait kell megadnunk. [10]

A legegyszerűbb kommunikációs kapcsolat során a küldő fél üzenetet küld a fogadó fél felé. Ez alapján külön típusnak kell tekintenünk a szereplő partnereket (EGYED típus) és az átküldött üzenetet (ÜZENET típus). A védett kommunikáció a küldött üzenet titkos voltát jelenti, amelyet kriptográfiai algoritmusok alkalmazásával érünk el. Az algoritmusok titkosító és visszafejtő kulcsokat használnak a működés során (KULCS típus). Le kell írnunk a vizsgálandó protokollok időbeli viselkedését, ami külön típust jelent (IDŐ típus). Szintén le kell írnunk a partnerek által használt csatornákat és azok tulajdonságait is (CSATORNA típus).

A típusok megadása után a *Mellékletben* megadjuk az alkalmazható nyelvi elemeket, a következtetési szabályokat, az axiómarendszert, és azokat a megjegyzéseket, amelyek a rendszer pontosabb értelmezését szolgálják.

5. A bővített CSN-logika alkalmazása - A MANA protokollcsalád

A MANuális Authentikáció (MANA protokollcsalád) főleg vezeték-nélküli (wireless) eszközök hitelesítésére lett kialakítva. Ez a hitelesítés egy nem biztonságos vezeték-nélküli csatornát egészít ki manuális adatátvitellel (mint második csatorna), így biztosítva a megfelelő szintű védelmet. Négy protokoll tartozik jelenleg a MANA protokollcsaládba. Ezek között az alapvető különbség a protokoll során felhasznált eszközök tulajdonságaiban van (alkalmazható az eszközön billentyűzet, LED, kijelző képernyő, beviteli gomb, nyomógomb, stb.). A nyilvános csatorna általában gyors és szélessávú; míg a nem nyilvános csatorna általában a manuális

lehetséges. Ezek közül néhány: $\Box\alpha$ igaz, ha ... α *szükségszerűen* igaz; *tudom*, hogy α igaz; *ismeretes*, hogy α igaz; *hiszem*, hogy α igaz; α igaz *most, és a jövőben mindig* igaz lesz; stb. [3]

[2] angolul: *epistemic-doxastic*

csatorna kis kapacitással - a felhasználók olvassák és/vagy írják a csatornajeleket. [17]

A továbbiakban csak a MANA III protokollal foglalkozunk. A MANA I és II protokollok vizsgálatának eredményei a [13] és [14] közleményekben jelentek meg.

5.1. MANA III

A protokollban két eszköz (A és B) és az eszközöket kezelő felhasználó (U - user) vesz részt. Mindkét eszköz rendelkezik egy-egy input egységgel (billentyűzet), és egy-egy output egységgel (világító dióda - LED). A protokoll célja az, hogy mindkét eszköz bizonyítottan rendelkezzen ugyanazzal a kezdeti paraméterrel (n_A), amelyet a későbbi védett kommunikáció során használhat fel.

A MANA III protokoll lépései

1. Az A eszköz generál egy n_A számot. Ezt és azonosítóját (A) átküldi a B eszköznek a ch_1 csatornán. B egy n_B számot és Σ azonosítót kap a ch_1 csatornán (a ch_1 csatorna nem védett, feltételezzük, hogy egy támadó képes megváltoztatni az üzeneteket (fennállhat $n_A \neq n_B$ és $\Sigma \neq A$)).
2. A B eszköz a ch_1 csatornán elküldi az B azonosítóját. Az A eszköz Ψ számot (azonosítót) fogad a ch_1 csatornán (hasonlóan fennállhat, hogy $\Psi \neq B$).
3. Az U user egy r_U véletlenszámot generál, és ezt a védett ch_2 és ch_3 csatornákon eljuttatja az A és a B félhez.
4. A egy k_A véletlenszámot (kulcs) generál és kiszámítja az $m_1 = h(\{A, n_A, r_U\}, k_A)$ értéket.
5. Az A eszköz elküldi m_1-t B-nek a ch_1 csatornán. B m_{11}-t kap üzenetként (fennállhat, hogy $m_1 \neq m_{11}$).
6. B egy k_B véletlenszámot (kulcs) generál és kiszámítja az $m_2 = h(\{B, n_B, r_U\}, k_B)$ értéket.
7. B elküldi m_2-t A-nak a ch_1 csatornán. A m_{22}-t kap üzenetként (fennállhat, hogy $m_2 \neq m_{22}$).
8. Miután A fogadja m_{22}-t B-től (és nem előbb), A átküldi a k_A kulcsot B-nek a ch_1 csatornán (B k_Σ-et kap, fennállhat, hogy $k_\Sigma \neq k_A$).
9. Amikor B megkapja az m_{11} értéket A-tól (és nem előbb), B átküldi a k_B számot A-nak a ch_1 csatornán (A k_Ψ-t kap, fennállhat, hogy $k_\Psi \neq k_B$).
10. A újraszámítja m_2-t, m_{222}-t kap eredményül. Amennyiben ez megegyezik a B-től kapott m_{22} értékkel, úgy A erről egy jelet küld (világító LED) U-nak a ch_2 csatornán. $m_{222} = h(\{\Psi, n_A, r_U\}, k_\Psi)$ a kapott üzenetek alapján.
11. B újraszámítja m_1-t, m_{111}-t kap eredményül.

Amennyiben ez megegyezik az A-tól kapott m_{11} értékkel, úgy B erről egy jelet küld (világító LED) U-nak a ch_3 csatornán. $m_{111} = f_{\mathcal{H}}(\{\Sigma, n_B, r_U\}, k_\Sigma)$ a kapott üzenetek alapján.

12. Amennyiben mindkét eszköz sikeres számítást jelez (és csak ekkor), U visszajelzi ezt mindkét eszköznek. □

Kezdeti feltételek rögzítése

I301. $CH(ch_1, pub)$; $CH(ch_2, sec)$; $CH(ch_3, sec)$.

I302. $ENT_{ch_2} = \{A, U\}$; $ENT_{ch_3} = \{B, U\}$.

I303. $K_{\mathcal{A},t_{17}}(m_{22} = m_{222}) \rightarrow S(ch_2, A, t_{17}, \text{"1"})$.

I304. $K_{\mathcal{A},t_{19}}(m_{11} = m_{111}) \rightarrow S(ch_3, B, t_{19}, \text{"1"})$.

I305. $K_{\mathcal{A},t_{17}}(m_{22} \neq m_{222}) \rightarrow S(ch_2, A, t_{17}, \text{"0"})$.

I306. $K_{\mathcal{A},t_{19}}(m_{11} \neq m_{111}) \rightarrow S(ch_3, B, t_{19}, \text{"0"})$.

I307. $K_{U,t_{21}}(R(ch_2, U, t_{18}, \text{"1"}) \wedge R(ch_3, U, t_{20}, \text{"1"}))$
$\rightarrow S(ch_2, U, t_{21}, \text{"1"}) \wedge S(ch_3, U, t_{23}, \text{"1"})$

I308. $K_{U,t_{21}}(R(ch_2, U, t_{18}, \text{"0"}) \vee R(ch_3, U, t_{20}, \text{"0"}))$
$\rightarrow S(ch_2, U, t_{21}, \text{"0"}) \wedge S(ch_3, U, t_{23}, \text{"0"})$

I309. $R(ch_2, A, t_{22}, \text{"1"}) \rightarrow K_{A,t_{22}}(n_A = n_B)$.

I310. $R(ch_3, B, t_{24}, \text{"1"}) \rightarrow K_{B,t_{24}}(n_A = n_B)$.

I311. $R(ch_2, A, t_{22}, \text{"0"}) \rightarrow K_{A,t_{22}}(n_A \neq n_B)$.

I312. $R(ch_3, B, t_{24}, \text{"0"}) \rightarrow K_{A,t_{24}}(n_A \neq n_B)$.

A MANA III protokoll formális alakja

1. $S(ch_1, A, t_1, \{n_A, A\})$; $R(ch_1, B, t_2, \{n_B, \Sigma\})$
2. $S(ch_1, B, t_3, B)$; $R(ch_1, A, t_4, \Psi)$
3. $S(ch_2, U, t_5, r_U)$; $R(ch_2, A, t_6, r_U)$
4. $S(ch_3, U, t_7, r_U)$; $R(ch_3, B, t_8, r_U)$
5. $S(ch_1, A, t_9, m_1)$; $R(ch_1, B, t_{10}, m_{11})$
6. $S(ch_1, B, t_{11}, m_2)$; $R(ch_1, A, t_{12}, m_{22})$
7. $S(ch_1, A, t_{13}, k_A)$; $R(ch_1, B, t_{14}, k_\Sigma)$

8. $S(ch_1, B, t_{15}, k_B)$; $R(ch_1, A, t_{16}, k_\Psi)$
9. $S(ch_2, A, t_{17}, x)$; $R(ch_2, U, t_{18}, x)$
10. $S(ch_3, B, t_{19}, y)$; $R(ch_3, U, t_{20}, y)$
11. $S(ch_2, U, t_{21}, z)$; $R(ch_2, A, t_{22}, z)$
12. $S(ch_3, U, t_{23}, z)$; $R(ch_3, B, t_{24}, z)$

A protokoll céljai - tételek és bizonyítások

Tétel 5.1. *Tegyük fel, hogy a n_A és n_B paraméterek nem egyenlők a protokoll végrehajtása során (egy illetéktelen felhasználó módosítja a kommunikációt). Ekkor a MANA III protokoll lefutásának a végén az A és B partnerek (eszközök) mindketten tudják azt, hogy $n_A \neq n_B$. Formálisan:*

$$n_A \neq n_B \rightarrow K_{A,t_{22}}(n_A \neq n_B) \wedge K_{B,t_{24}}(n_A \neq n_B).$$

Bizonyítás Az első lépés és az $A5(a)$ és $A6(a)$ axióma alapján

$$L_{A,t_1}\{n_A, A\}\,, \quad (1)$$
$$L_{B,t_2}\{n_B, \Sigma\}\,. \quad (2)$$

(M3) alapján

$$L_{A,t_1} n_A\,, \quad (3)$$
$$L_{A,t_1} A\,, \quad (4)$$
$$L_{B,t_2} n_B\,, \quad (5)$$
$$L_{B,t_2} \Sigma\,. \quad (6)$$

A második lépésben $A5(a)$ és $A6(a)$ alapján

$$L_{B,t_3} B\,, \quad (7)$$
$$L_{A,t_4} \Psi\,. \quad (8)$$

A harmadik és negyedik lépésben $A5(a)$ és $A6(a)$ alapján

$$L_{U,t_5} r_U\,, \quad (9)$$
$$L_{A,t_6} r_U\,, \quad (10)$$
$$L_{B,t_8} r_U\,. \quad (11)$$

Az ötödik lépésben $A5(a)$ és $A6(a)$ alapján

$$L_{A,t_9} m_1\,, \quad (12)$$
$$L_{B,t_{10}} m_{11}\,. \quad (13)$$

$(m_1 = h(\{A, n_A, r_U\}, k_A))$
A hatodik lépésben $A5(a)$ és $A6(a)$ alapján

$$L_{B,t_{11}} m_2 \ , \tag{14}$$
$$L_{A,t_{12}} m_{22} \ . \tag{15}$$

$(m_2 = h(\{B, n_B, r_U\}, k_B))$
A hetedik lépésben $A5(a)$ és $A6(a)$ alapján

$$L_{A,t_{13}} k_A \ , \tag{16}$$
$$L_{B,t_{14}} k_\Sigma \ . \tag{17}$$

A nyolcadik lépésben $A5(a)$ és $A6(a)$ alapján

$$L_{B,t_{15}} k_B \ , \tag{18}$$
$$L_{A,t_{16}} k_\Psi \ . \tag{19}$$

A protokoll szerint t_{16} után A újraszámítja m_2-t és m_{222}-t kap eredményül. m_{222} formailag, az A rendelkezésére álló, fogadott üzenetek alapján: $m_{222} = h(\{\Psi, n_A, r_U\}, k_\Psi)$. Eredetileg $m_2 = h(\{B, n_B, r_U\}, k_B)$. Ha $m_2 = m_{22}$, $\Psi = B$ és $k_\Psi = k_B$ ($A17(a)$ alapján), még akkor sem lehet $m_{22} = m_{222}$, mivel a tétel feltételei szerint $n_A \neq n_B$. Így $K_{A,t_{17}}(m_{22} \neq m_{222})$, amivel $I305$. alapján $S(ch_2, A, t_{17}, \text{"0"})$. A védett csatornák miatt (M5) U az $R(ch_2, U, t_{18}, \text{"0"})$ üzenetet kapja, ami alapján az $I308$. kezdeti feltétel érvényes. Ez azt jelenti, hogy $S(ch_2, U, t_{21}, \text{"0"}) \wedge S(ch_3, U, t_{23}, \text{"0"})$. Védett csatornák miatt (M5), $I311$. és $I312$. érvényes: $R(ch_2, A, t_{22}, \text{"0"})$ és $R(ch_3, B, t_{24}, \text{"0"})$.
Tehát $K_{A,t_{22}}(n_A \neq n_B)$ és $K_{B,t_{24}}(n_A \neq n_B)$, ami a keresett állítás egyik fele. Hasonló gondolatmenettel belátható, hogy a B egyed által elvégzett $m_{11} = m_{111}$ összehasonlítás is a $K_{B,t_{24}}(n_A \neq n_b)$-t adja. A két rész a keresett állításhoz vezet. □

Tétel 5.2. *Tegyük fel, hogy n_A és n_B paraméterek egyenlők a protokoll végrehajtása során. Ekkor a MANA III protokoll nem garantálja, hogy lefutásának a végén az A és B partnerek mindketten tudják azt, hogy $n_A = n_B$.*
Formálisan: $n_A = n_B \rightarrow K_{A,t_{22}}(n_A \neq n_B) \wedge K_{B,t_{24}}(n_A \neq n_B)$ nem levezethető.

Bizonyítás Az előző tétel bizonyításához hasonlóan az A és B felhasználók eljutnak a fogadott m_{22} és számított m_{222} (m_{11} és m_{111}) összehasonlításához. Ez abban az esetben, ha a támadó aktívan nem avatkozik a protokollba, a keresett állításhoz vezet. Amennyiben a protokollt támadás éri, az $n_A = n_B$ feltételt megtartva, de az A vagy k_A értékek közül bármelyiket változtatva, a protokoll az $m_{22} = m_{222}$ vagy $m_{11} = m_{111}$ állítások bármelyikének elvetéséhez vezet. Így $K_{A,t_{22}}(n_A \neq n_B)$ és $K_{B,t_{24}}(n_A \neq n_B)$. Ez azt jelenti, hogy hiába lett helyesen átküldve az n_A üzenet, mégsem fogadják el a felhasználók ezt. □

Ebben az esetben elmondható, hogy a felek hiába rendelkeznek a helyes n_A értékkel, annak közös elfogadhatóságát a protokoll nem tudja garantálni. Mivel az A, B egyednevek és a k_A, k_B kulcsok nyilvános csatornán kerülnek továbbításra, egy támadó fél módosítani tudja értéküket, megzavarva így a protokollt. A fenti két tétel elemzése megmutatja, hogy a javítás a MANA II protokollához hasonló módon nem oldható meg (lásd [13][14]). Kulcshasználat nélküli $H(m)$ egyirányú függvények alkalmazása az összetett m üzenet miatt nem jelent megoldást. n_A, illetve n_B részeket tartalmaznia kell az átküldött üzeneteknek, de r_U elhagyása már megszemélyesítő támadást tesz lehetővé. A protokoll ezen hiányosságainak javítása új protokoll kidolgozását igényli.

5.2. Összefoglalás

Összefoglalva elmondhatjuk, hogy CSN-logika pontosítása és bővítése alkalmas a többcsatornás protokollok vizsgálatára. Nyilvánvaló, hogy nem ez lehet az egyetlen lehetséges megoldás a problémkörben. A bemutatott példa evidensnek és egyszerűnek tűnhet, viszont megnyithat olyan vizsgálati utakat, amelyek komolyabb protokoll-hibákra is rámutathatnak.

Többcsatornás protokollokat a vizsgált három protokollon (MANA család) kívül más körben is alkalmaznak. Szaporodik azoknak az alkalmazásoknak a köre, amelyek összekapcsolják az Internetet és a személyes kommunikációs eszközöket. A mobiltelefonra küldött SMS, amely a banki szolgáltatások elérését teszi védettebbé; a mobiltelefonokkal történő hang- és képátvitel (2D-s BAR-kódok, biometriai azonosítás, stb.) összekapcsolva más kommunikációs csatornákkal (Internet, fax, stb.), mind azt erősítik, hogy a többcsatornás protokolloknak jogosultsága van a kommunikációs fejlődésben.

Hivatkozások

[1] T. Coffey and P. Saidha. Logic for verifying public-key cryptographic protocols. *IEEE Proceedings Computers and Digital Techniques*, 144(1):28–32, 1997.

[2] D. Dolev and A. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, IT-29(2):198–208, March 1983.

[3] M. Ferenczi. *Matematikai logika.* Műszaki Könyvkiadó, 2002.

[4] C. Gehrmann, C. J. Mitchell, and K. Nyberg. Manual authentication for wireless devices. *Cryptobytes*, 7(1):29–37, 2004.

[5] Á. Gergely. Biztonságos útvonalválasztás ad hoc hálózatokban. Master's thesis, Budapesti Műszaki és Gazdaságtudományi Egyetem, Villamosmérnöki és Informatikai Kar, Híradástechnikai Tanszék, 2005.

[6] S. Goeman. Specification of prototypes - D11, IST - 2000 - 25350 - SHAMAN, Public Report. http://www.isrc.rhul.ac.uk/shaman/docs, March 2003. D11v2.pdf.

[7] J. Hintikka. *Knowledge and Belief. An Introduction to the Logic of the Two Notions.* Cornell University Press, 1962.

[8] J. Hintikka. *Részletek Jaakko Hintikka Tudás és Hit (Bevezetés a két fogalom logikájába) című művéből. A hiedelmek természete, szerveződése és szerepe a mindennapi tudatban című munkaértekezlet segédanyaga 7.* Fordítási részek. Forclította: Berkes Ildikó, 1975.

[9] S. Kramer. Logical concepts in cryptography. http://citeseer.ist.psu.edu/759062.html.

[10] T. Mihálydeák. *Az informatika logikai alapjai.* University of Debrecen, 2007. Egyetemi jegyzet.

[11] T. Newe and T. Coffey. Formal verification logic for hybrid security protocols. *International Journal of Computer Systems Science & Engineering*, pages 17–25, 2003.

[12] P. Takács. The additional examination of the Kudo-Mathuria time-release protocol. *Journal of Universal Computer Science*, 12(9):1373–1384, 2006.

[13] P. Takács. The extension of CSN-logic for multi-channel protocols. In *Proceedings of the 7th ICAI Conference, Eger*, pages 147–154, 2007.

[14] P. Takács and S. Vályi. An extension of protocol verification modal logic to multi-channel protocols. *Tatra Mountains Mathematical Publications*, 41:153–166, 2008.

[15] P. Windirsch. Security for mobile systems beyond 3G - Presentations and posters of the IST - 2000 - 25350 - SHAMAN Worshop, 2002. http://www.isrc.rhul.ac.uk/shaman/docs, 2002.

[16] F-L. Wong and F. Stajano. Multi-channel protocols. In *Proceeding of Security Protocols, 13th International Workshop, Cambridge, UK*, volume 4631 of *Lecture Notes in Computer Science*. Springer-Verlag, April,20-22 2005.

[17] F. L. Wong and F. Stajano. Multichannel security protocols. *IEEE Pervasive computing*, VI.:31–39, October-December 2007.

Melléklet
A bővített CSN-logika[3]

A CSN-logikai rendszerhez tartozó nyelv a következő

$$L^{(CSN)} = \langle Sort, LC, Var, Con, Term, Form \rangle$$

rendezett hatos, ahol
Sort $= \{U, E, K, T, C\}$
A típusok (fajták) halmaza: U üzenet-típus; E egyed-típus; K kulcs-típus; T időtípus; C csatorna-típus.
LC $= \{\neg, \rightarrow, \leftrightarrow, \wedge, \vee, \equiv, =, \forall, \exists, (,)\}$
A nyelv logikai konstansainak halmaza, amelyeket az elsőrendű logikában megszokott módon használunk.
Var $= Var_U \cup Var_E \cup Var_K \cup Var_T \cup Var_C$
A nyelv változóinak megszámlálhatóan végtelen halmaza. Minden változónak meghatározott típusa van. Var_δ a δ típusú változók halmazát jelöli.
Con $= Con_U \cup Con_E \cup Con_K \cup Con_T \cup Con_C$
A nyelv nemlogikai konstansainak legfeljebb megszámlálhatóan végtelen halmaza. Minden nemlogikai konstansnak meghatározott típusa van. Con_δ a δ típusú nemlogikai konstansok halmazát jelöli, egyes típusok esetén üres is lehet a halmaz. $F(0)_\delta$ a névkonstansok, $F(n)_\delta$ az n argumentumú függvényjelek halmaza. Az argumentumban szereplő szám a paraméterek számát jelöli. Függvényjelek esetén szokás megadni egy véges $\langle \delta_1, \delta_2, \ldots, \delta_n, \delta \rangle$ indexsorozatot is, amely rendre megadja a konkrét függvényjel n darab argumentumának típusát ($\delta_i \in Sort$) és a függvényjel típusát ($\delta \in Sort$). $P(0)$ az állításkonstansok, $P(n)$ az n argumentumú predikátumkonstansok halmaza. Itt szintén szokás megadni az egyes predikátumkonstansok argumentumában szereplő $\langle \delta_1, \delta_2, \ldots, \delta_n \rangle$ ($\delta_i \in Sort$) indexsorozatot.
Term $= Term_U \cup Term_E \cup Term_K \cup Term_T \cup Term_C$
A nyelv terminusainak, termjeinek halmaza, típusonként induktív definícióval megadva. $Term_\delta$ a δ típusú Termek halmazát jelöli, egyes típusok esetén üres is lehet a halmaz.
Az induktív definíció általános formája minden δ típus esetén:
(a) $Var_\delta \cup F(0)_\delta \subseteq Term_\delta$.

[3] Az eredeti CSN-logika két cikkben jelent meg: T. Coffey, P. Saidha. Logic for verifying public-key cryptographic protocols. IEEE Proceedings Computers and Digital Techniques, 144(1):28-32, 1997. és T. Newe, T. Coffey. Formal verification logic for hybrid security protocols. International Journal of Computer Systems Science and Engineering, 17-25, 2003. Ezt a rendszert egészítette ki M. Kudo, A. Mathuria. Az entended logic for analyzing timed-release public-key protocols. In Proceedings Information and Communication Security, Second International Conference, ICICS'99, Sydney, 1999. A többcsatornás jelölésrendszert első alakját Takács P. és Vályi S. dolgozta ki. An extension of protocol verification modal logic to multi-channel-protocols. Tatra Mountains Mathematical Publications - TATRACRYPT 2007. Vol.41. 2008. A melléklet ezen rendszer lényegesen átdolgozott változatát tartalmazza.