Policy keretrendszer dinamikus hálózatkompozíciók automatizált tárgyalási folyamatához

ERDEI MÁRK, WAGNER AMBRUS

Budapesti Műszaki és Gazdaságtudományi Egyetem, Híradástechnikai Tanszék
{merdei, awagner}@hit.bme.hu

Kulcsszavak: policy keretrendszer, adatmodell, policy-kezelő algoritmusok

Az utóbbi években a vezetéknélküli hálózati technológiák széleskörű elterjedésének köszönhetően intenzív kutatás indult az Ambient Network (AN) témakörében. Az AN-ek célja az, hogy a felhasználó számára átlátszó módon biztosítson kapcsolatot többféle hálózati technológiát felhasználva. Ezen cél elérése érdekében az AN-ek automatikusan konfigurálják az egyes hálózati elemeket, így egy AN a tartalmazott elemek management domainjeként szolgál. A vezetéknélküli hálózatok dinamizmusa szükségessé teszi az AN-ek folyamatos karbantartását elemek hozzáadása és eltávolítása, illetve AN-ek kompozíciója és dekompozíciója révén. Ideális esetben ez a karbantartási tevékenység a háttérben, emberi beavatkozás nélkül, önszervező módon történik. Az AN-ekkel kapcsolatos kutatás az Európai Közösség „Wireless World Initiative – Ambient Networks" projektje keretében zajlik [1,2]. A cikk az AN-ek kompozícióját irányító, úgynevezett policy keretrendszert mutatja be.

1. Bevezető

A széles körben használt hálózati technológiák sokfélesége rugalmas konfigurációs és karbantartási megoldások létrehozását teszi szükségessé. Egy természetes megközelítés az alacsonyszintű konfiguráció származtatása a felhasználó és a hálózat adminisztrátor igényeit és szándékait leíró magasszintű definíciókból.

Ezen szándékok kifejezésének egyik lehetséges módja a policy-k használata. Az irodalomban több különböző felhasználást, értelmezést és megvalósítást találunk. Policy-kat használnak például a DiffServ erőforrásgazdálkozásban [3], a hierarchikus IP menedzsmentben a hálózatmenedzsment viselkedés futásidejű kiterjesztéséhez [4], szolgáltatás elemek magasszintű kontextus információ alapján történő adaptációjához [5], és emberi beavatkozás nélküli hozzáférésvezérléshez [6].

A policy-k szabványos tárolása és kezelése iránti igényre reagálva az IETF kidolgozott egy információs modellt [7,8], és meghatározta a policy menedzsment terminológiáját [9]. Az ezen cikkben bemutatott policy keretrendszer nagy vonalakban szintén az IETF terminológiát követi. Mivel a legtöbb létező megoldás specifikus alkalmazásokhoz készült, dinamikus hálózatkompizícióval kapcsolatos kutatásunkhoz egy új policy keretrendszert dolgoztunk ki, melynek kidolgozásakor fontos szempont volt a széleskörű alkalmazhatóság.

Cikkünkben bemutatjuk a policy adatmodell felépítését és szemantikáját, a policy-k és a kontextusok kapcsolatát, végül a kapcsolódó algoritmusokat tárgyaljuk.

2. A policy-k szerepe a dinamikus hálózatkompozícióban

Az AN koncepcióban a peerek (felhasználók) hierarchikus overlay (csoport) struktúrákat alkotnak, melyek menedzsment tartományoknak felelnek meg. Egy csoportot hasonló tulajdonságú és igényű peerek alkotnak. Magasabb szintről szemlélve egy csoport egyetlen olyan peernek tekinthető, amely egyesíti magában a csoport tagjainak jellemzőit. A csoportok így hierarchikus struktúrákba rendezhetők.

A hierarchia legalsó szintjén lévő peerek csoportokba, majd felsőbb szinteken csoportok csoportjaiba szerveződnek.

Ha két csoport megközelíti egymást, kompozíciót hajthatnak végre, ha tulajdonságaik és szándékaik (melyeket policy-k fejeznek ki) elegendően hasonlóak.

Minden peernek van policy-ja, melyek egy csoport policy-ba egyesíthetők. A csoport-policy a csoportban lévő policy-k esszenciáját hivatott kifejezni. Az alábbiakban definiált policy keretrendszer a policy adatmodellt, a kapcsolódó algoritmusokat, illetve a kontextusok és policy-k közötti kapcsolatot definiálja.

Minden peer rendelkezik egy policy adatbázissal, amely egy, vagy több policy-t tartalmaz. Minden pillanatban ezen policy-k egyike az aktív policy. Az aktív policy kiválasztása a peer kontextusa alapján történik. A peer egy policy halmazzal rendelkezik, az alkalmazható policy-k halmazát több tényező határozza meg:

– hardver és szoftver környezet,
– hálózati környezet,
– hely információ stb.

A peer az aktív policy-t az alkalmazható policy-k halmazából választja ki.

3. Adatmodell

Az adatmodell némiképp hasonló az irodalomban leírtakhoz [10,11]. A policy-t három elem határozza meg *(1. ábra)*:

– profil, állítások, szabályok.

3.1. Profil

A profil olyan tulajdonságok halmaza, amelyeket a peer fontosnak tekint a többi peerrel történő tárgyalás során. Minden tulajdonságot egy-egy kulcs-érték pár ír le. Sem a kulcsokra, sem az értékekre nincs semmiféle típus-, vagy értékbeli megkötés, tetszőleges szövegek. Előre definiált kulcsok létezhetnek, de definiálhatnak kulcsokat a peerek is.

Példák:
– „memory-capacity” = „10M”
– „company-meeting-participant” = „yes”
– „nationality” = „Hungarian”

3.2. Állítások

Az állítások az adott peer és a tárgyalópartner profilja közötti relációkat fogalmaznak meg. Egy állítás három részből áll:
– a tárgyalópartner profiljából származó kulcs,
– relációs operátor,
– az adott peer profiljából származó kulcs, vagy konstans.

Példák:
– „software-version” >= „software-version”
– „company-meeting-participant” = „yes”

A tárgyalás kimenetelére gyakorolt hatás		Az állítás értéke	
		igaz	hamis
Minősítő	MUST	nincs	kudarc
	SHOULD	nincs	nincs
	DON’T CARE	nincs	nincs
	SHOULD NOT	nincs	nincs
	MUST NOT	kudarc	nincs

1. táblázat Minősítők

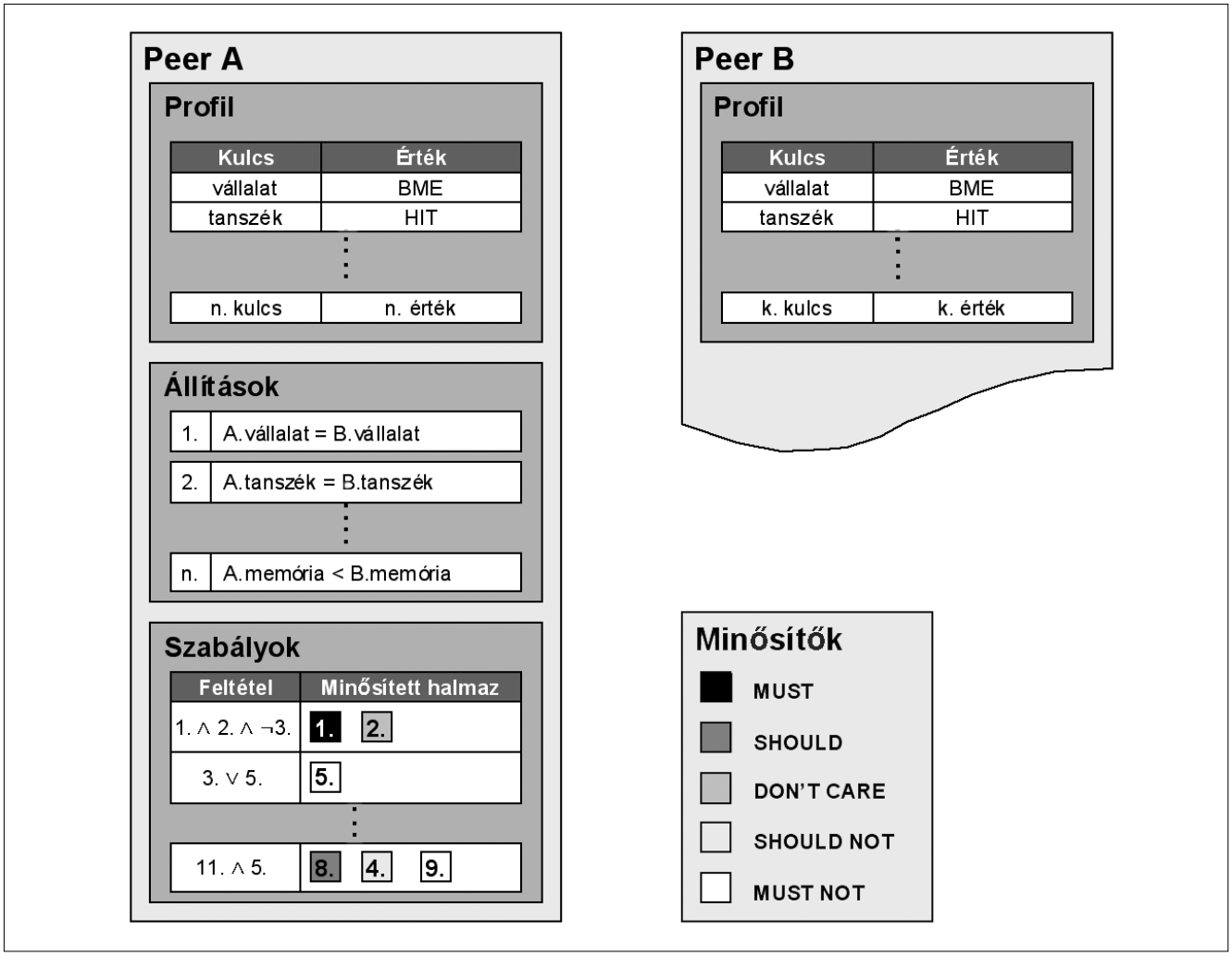
3.3. Szabályok

A szabályok a tárgyalási algoritmus paraméterei és két részből állnak:
– feltétel,
– minősített halmaz.

A feltétel egy logikai kifejezés. Ez a kifejezés állításokra való hivatkozásokat és logikai operátorokat tartalmaz. Behelyettesítve a tárgyalópartner profil információját, a feltétel kiértékelése igaz vagy hamis eredmény ad.

A feltétel határozza meg, hogy a szabályt alkalmazzuk-e a tárgyalás során, vagy nem.

1. ábra A policy adatmodell



A minősített halmaz állításokra vonatkozó minősített hivatkozások halmaza. A minősített halmaz minden hivatkozott állítást az alábbi minősítőkkel lát el:

– MUST (ragaszkodom hozzá),
– SHOULD (előnyben részesítem),
– DON'T CARE (érdektelen),
– SHOULD NOT (hátrányban részesítem),
– MUST NOT (nem fogadom el).

A minősítők a kiértékelt állítás sikeres tárgyaláshoz szükséges logikai értékét határozza meg. Az *1. táblázat (előző oldalon)* definiálja a minősítők jelentését.

A SHOULD és SHOULD NOT minősítők egyenértékűek a DON'T CARE minősítővel a tárgyalás során, a policy karbantartó algoritmusok azonban másként kezelik őket. Annak érdekében, hogy a policy konzisztens legyen önmagával, a szabályok közötti ellentmondásokat fel kell deríteni új szabály létrehozásakor.

Két szabály ellentmond, ha létezik az állítások olyan kiértékelése, hogy mindkét szabály feltétele igaz, és van olyan állítás, amelyet a két szabály ellentmondóan minősít. A meglévő szabályoknak ellentmondó szabályt nem lehet hozzáadni a policy-hoz.

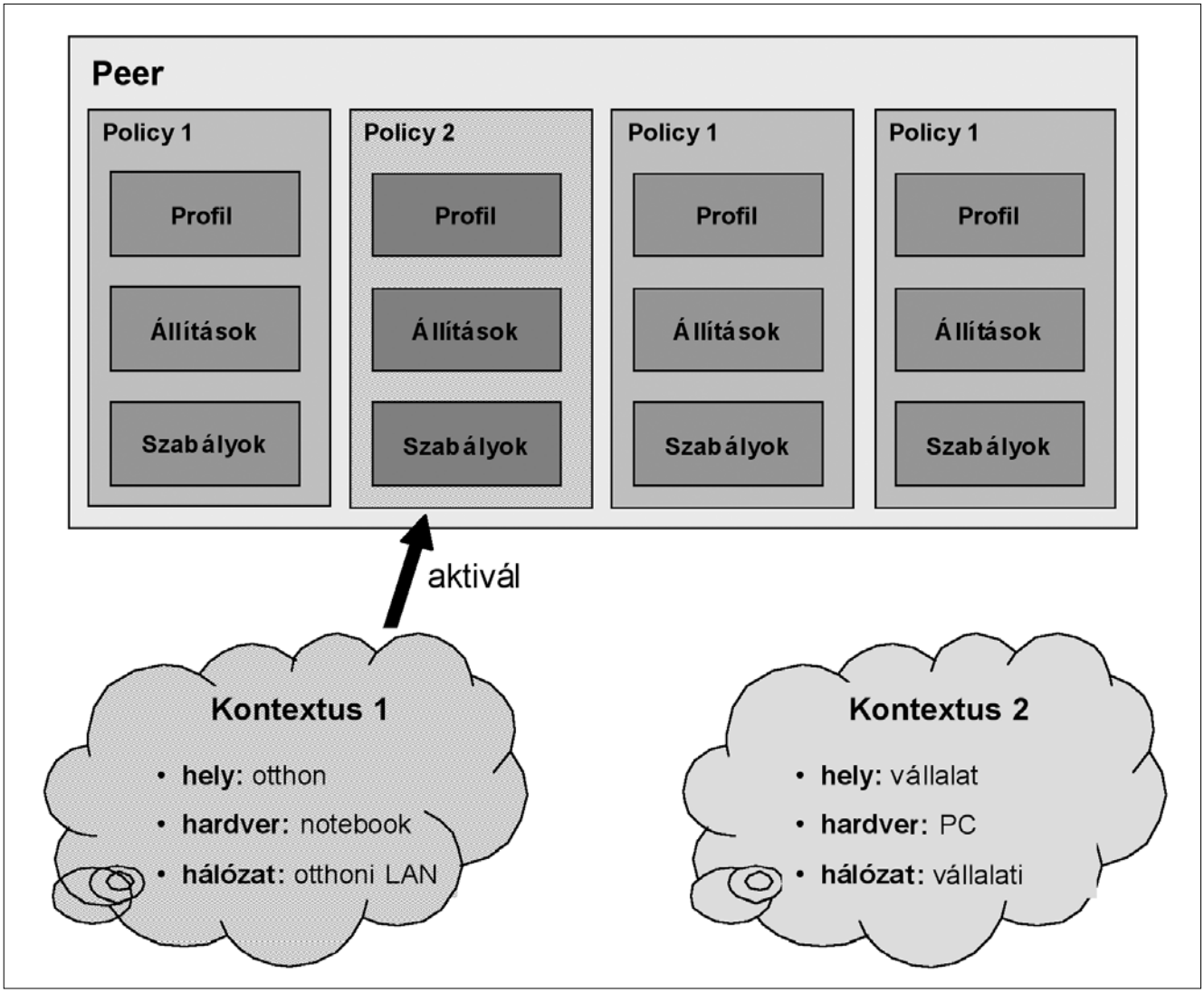
4. Összefüggés a policy-k és a kontextusok között

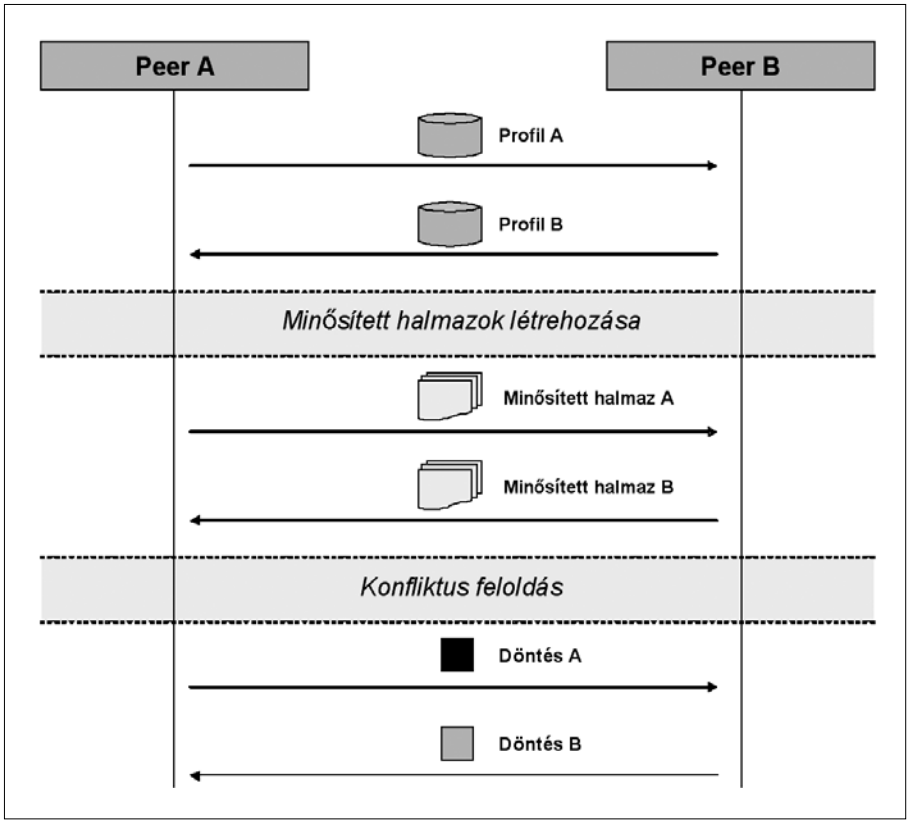
Egy peernek több policy-ja is lehet. A rendelkezésre álló policy-k közül egyik az aktív policy. Minden pillanatban pontosan egy aktív policy-nak kell lennie. A megfelelő policy kiválasztásában a felhasználót a kontextus fogalma segíti.

A kontextus a felhasználó környezetének különböző szempontjairól tartalmaz információt. Néhány a lehetséges szempontok közül:

- **Hely információ.** Információ a felhasználó tartózkodási helyéről. Lehetőségek: otthon, iroda, közlekedés stb. Ha hozzáférhető, a vezeték nélküli hálózatok vagy egy GPS vevő által adott információ tovább finomíthatja a kontextust.
- **Hardver/szoftver konfiguráció.** Információ az aktuálisan használt számítógépes platformról. Lehetséges értékek: asztali gép, notebook, PDA, mobiltelefon stb.
- **Hálózati kapcsolatokra vonatkozó információk.** Otthoni vagy irodai hálózat, vezetékes, vagy vezeték nélküli kapcsolat, rendelkezésre álló sávszélesség, ár stb.

2. ábra Kontextusok és policy-k





3. ábra Tárgyalási algoritmus

A fenti információk alapján a használható policy-k köre szűkíthető. A felhasználó a szűkített körből választja ki az aktív policy-t (illetve a kiválasztás automatikusan megtörténik, ha a szűkített kör már csak egy elemből áll). Ahhoz, hogy meghatározhassuk, egy adott kontextusban aktiválható-e egy policy, a policynak definiálnia kell a minimális, kontextussal szembeni elvárásait.

Az alábbi szituáció egy példa kontextusok használatára *(2. ábra)*. Egy dolgozó otthon és a munkahelyén is a notebookját használja. Hazaérkezik, bekapcsolja a notebookot, a megváltozott kontextus pedig két policyra szűkíti a használható policy-k körét:

– személyes, amely elérhetővé teszi számára a családi levelezést, és a családdal és barátokkal történő chat-elést, illetve
– otthoni iroda, amely összeköti őt a vállalati hálózattal a rendelkezésre álló szélessávú kapcsolaton keresztül.

A felhasználónak ekkor egy párbeszédablakban kell választania a fenti két lehetőség közül.

5. Policy-kezelő algoritmusok

5.1. Tárgyalási algoritmus

A tárgyalási algoritmus feladata, hogy a két kommunikáló peer policy-ját összehasonlítsa, és eldöntse, hogy azok kölcsönösen elfogadhatóak-e egymás számára. A peerek nem specifikus tárgyalási algoritmust használnak, hanem mindketten ugyanazt a szabványos algoritmust különféleképpen felparaméterezve. A rendszer felépítésétől függően, az alábbinál komplexebb tárgyalási algoritmusokra is szükség lehet [12].

Az alapvető algoritmus lépései az alábbiak *(3. ábra)*:

1) Minden policy állítás minősítésének semlegesre (DON'T CARE-be) állítása.
2) A peerek kicserélik egymás között a profiljukat.
3) Minden szabály feltétele kiértékelésre kerül. Ha a feltétel teljesül, a szabályban szereplő állítások a megadott minősítőkkel bekerülnek az összevont minősített halmazba.
4) A peerek összehasonlítják egymás minősített halmazait.
5) Ha a minősített halmazok között ellentmondás van, a peerek ezt megpróbálhatják feloldani a konfliktus-feloldó algoritmus segítségével.
6) A peerek a tárgyalást sikeresnek tekintik, ha a folyamat végén nincs ellentmondás a minősített halmazok között.

5.2. Csoport policy

Egy csoport policy-ja a csoportban lévő entitiások policy-jainak aggregátuma. Az egyes peerek személyes policy-jaiból a csoport policy kezelő algoritmus képezi a csoport policy-ját. A csoport policy-ja a csoportot alkotó felhasználói halmaz változásának és az egyes felhasználók policy-jai változásának megfelelően folyamatosan alkalmazkodik a csoport pillanatnyi állapotához, a csoport pillanatnyi képét tükrözi.

A csoport policy azokban a helyzetekben kerül felhasználásra, amikor egy szituáció során a csoportot egyetlen kommunkáló félként kell reprezentálni (például amikor egy újabb csomópont szeretne a csoporthoz csatlakozni, akkor a tárgyalási algoritmus az új csomópont és a csoport policy-ja felett fog lefutni, hasonlóképpen két AN kompozíciójakor is a tárgyalási algoritmus a két csoport policy-t fogja használni).

5.2.1. A csoport policy működése

A csoport policy ugyanazokból a főbb elemekből épül fel, mint egy felhasználói policy (profil, állítások, szabályok). Az adatszerkezet ezen felül még ki van egészítve a profil tulajdonságainak, az állításoknak és a szabályoknak a kardinalitásával.

A kardinalitás azt írja le, hogy a csoporton belül hány felhasználó rendelkezik ugyanazokkal a profiltulajdonságokkal, állításokkal illetve szabályokkal. Ez kifejezi az adott leíró fontosságát is a csoporton belül.

Tehát a csoport policy kismértékben eltér az egyszerű felhasználói policy-tól. Ennek következtében vagy a tárgyalási algoritmust kell módosítani úgy, hogy kezelni tudja a kardinalitásokat is (a felhasználói policyban ebben az esetben minden elem kardinalitása egy), vagy a csoport policy-t le kell képezni egy egyszerű felhasználói policy-ra mielőtt a tárgyalásra sor kerülne. Ebben az esetben a csoport policy-ban előforduló kis kardinalitású elemeket el kell távolítani (ezek ugyanis nem a csoport jelentős részének álláspontját képviselik), valamint az egymásnak ellentmondó elemek között fel kell oldani a konfliktust (például egyszerű többségi döntés elvén).

A második esetben nem elegendő a leképzést egyszer elvégezni, hiszen ebben az esetben elvesztenénk a számossági információkat, melyekre szükség lehet, ha csomópontok lépnek ki a csoportból, vagy csatlakoznak a csoporthoz (ebben az esetben ugyanis megváltozhatnak az erőviszonyok amit a csoport policy-nak is tükröznie kell), hanem minden tárgyalás elindulása előtt, vagy minden csoportbeli változás után újra el kell végezni a leképzést.

5.2.2. Csoport policy kezelő algoritmus

A csoport policy kezelő algoritmus feladatai az alábbiak:

– az újonnan csatlakozó felhasználó policy-jának a csoport policy-ba való beolvasztása,
– a csoport policy állapotának frissítése, ha egy felhasználó távozik a csoportból, és
– a csoport policy folyamatos közelítése a csoportot alkotó felhasználók közösen megfogalmazható álláspontjához.

5.2.3. Beolvasztási algoritmus

A beolvasztási algoritmus az egyes felhasználói policy-kat olvasztja be a csoport policy-ba. Az algoritmus lépései az alábbiak:

1. A felhasználói profil elemeit hozzáadja a csoport profilhoz. Az újonnan létrejövő elemek kardinalitása egy, a már létező elemek kardinalitását eggyel növeli.
2. A csoport profilból eltávolítja az egymással ütköző profil elemeket. E célból kiszámítja az egymással ütköző profil elemek kardinalitásának arányát (0 és 1 közötti érték). A kapott értéktől függően kétféleképpen kerülhet sor a profil elem eliminálására:
   a) Ha az arány kisebb mint egy megadott küszöbérték, akkor a kisebb kardinalitású profil elemet törli a profilból (a kevésbé fontosat),
   b) Egyébként mindkettőt törli (egymásnak ellentmondóak, és mindkettő a csoport jelentős hányadát reprezentálja, tehát egyiket sem lehet felhasználni a csoport leírására).
3. Az állítások fontossági súlyát két tényező határozza meg: egyrészről a saját kardinalitásuk, valamint azoknak a profil elemeknek a kardinalitása, melyekre hivatkoznak. A konfliktusban lévő állításokat az algoritmus eltávolítja a csoport profilból a profil elemeknél használt algoritmushoz hasonló eljárással.
4. A szabályok esetében szintén a fontosság szerinti kiemelésre, valamint letisztításra van szükség, hogy az eredményül kapott szabályhalmaz minél jobban tükrözze a csoport közös álláspontját. A szabályok letisztítása az alábbi lépésekben történik:
   a) Az egyes szabályok fontossága a bennük szereplő állítások fontosságából származik.
   b) A szabályok feltételrészéből a kis fontosságú illetve esetlegesen a korábbi lépések során már törölt állításokat eltávolítja az algoritmus.
   c) Hasonlóképpen a kis fontosságú illetve korábban törölt állításokat a szabály minősített halmazából is törli.
   d) A szabályok között fennálló ellentmondások feloldása a minősített halmazukban szereplő minősítők alapján történik. Két szabály potenciális konfliktusban van, ha a feltételrészüknek létezik olyan kiértékelése mely esetén mindkettő szabály életbe lép. Valódi konfliktus akkor lép fel, ha a két szabály minősített halmazában ugyanaz az állítás szerepel eltérő minősítéssel. Ekkor az ellentmondó minősítésekből eredő eltérést fel kell oldani. A feloldás a *2. táblázat* alapján történik.
   e) Azok a szabályok, amelyek a folyamat végére üresek lettek, törlésre kerülnek.

5.2.4. A csoportot elhagyó felhasználók kezelése

Ha egy vagy több felhasználó elhagyja a csoportot, akkor ezt a csoport policy-nak tükröznie kell. Mivel a felhasználói policy-k nem vonhatók ki a csoport policy-ból, ezért ebben az esetben a csoport policy-t újra fel kell építeni a bent maradt felhasználók policy-jaiból.

2. táblázat Policy beolvasztási szabályok (= többféle feloldás lehetséges)*

Feloldás	MUST NOT	SHOULD NOT	DON'T CARE	SHOULD	MUST
MUST	szabály eldobása	*	*	*	N/A
SHOULD	*	*	SHOULD	N/A	
DON'T CARE	MUST NOT	SHOULD NOT	N/A		
SHOULD NOT	*	N/A			
MUST NOT	N/A				

6. Összefoglalás

A fentiekben bemutattunk egy policy keretrendszert, melyet dinamikus hálózatkompozícióval kapcsolatos kutatásainkhoz dolgoztunk ki. A keretrendszer egy adatmodellből, és a hozzá kapcsolódó algoritmusokból áll.

Ez a policy keretrendszer lehetővé teszi, hogy közvetlen felhasználói beavatkozás nélkül – a magasabb szintű felhasználói szándékok alapján –, automatikusan menjenek végbe a hálózat-kompozíciós döntések. Továbbá, a csoport policy bevezetésével lehetővé válik ezen döntési folyamatok automatikus kiterjesztése magasabb hierachia szintekre is.

Az ismertetett policy keretrendszer egy az Ambient Networks projektben [1,2] megvalósított Ambient Networks hálózatmenedzsment [14] rendszer prototípus részeként került megvalósításra [15].

A kutatási célok között szerepel az adatmodell kiterjesztése és altalánosítása (például hierarchikus profilok kezelésével). A profiltulajdonságokra adattípusok és típusspecifikus operátorok definiálása (ez jelentősen növelni fogja a tárgyalási és beolvasztási algoritmusok mozgásterét és az adatok kezelését is kifinomultabbá fogja tenni) [13].

Ezen felül a dinamikus karbantartási feladatok (például távozó felhasználók esetén a csoport policy frissítése) további vizsgálata és optimalizálása szükséges teljesítőképesség, érvényesség és koherencia szempontjából.

Irodalom

[1] N. Niebert, H. Flinck, R. Hancock, H. Karl, C. Prehofer, "Ambient Networks – Research for Communication Networks Beyond 3G", 13th IST Mobile & Wireless Communications Summit, Lyon, France, June 2004.

[2] N. Niebert, A. Schieder, H. Abramowicz, G. Malmgren, J. Sachs, U. Horn, C. Prehofer, H. Karl, "Ambient Networks: An Architecture for Communication Networks Beyond 3G", IEEE Wireless Comm., pp.1536–1584., April 2004.

[3] P. Flegkas, P. Trimintzios, G. Pavlou, A. Liotta, "Design and Implementation of a Policy-Based Resource Management Architecture", Proceedings of IEEE/IFIP Integrated Management Symposium (IM'2003), Colorado Springs, USA, pp.215–229., Kluwer, March 2003.

[4] P. Flegkas, P. Trimintzios, G. Pavlou, I. Andrikopoulos, C.F. Cavalcanti, "On Policy-based Extensible Hierarchical Network Management in QoS-enabled IP Networks", Proceedings of the IEEE Workshop on Policies for Distributed Systems and Networks (Policy 2001), Bristol, UK, M. Sloman, J. Lobo, E. Lupu, eds. pp.230–246., Springer, January 2001.

[5] J. Keeney, V. Cahill, "Chisel: A Policy-Driven, Context-Aware, Dynamic Adaptation Framework", Proceedings of IEEE 4th International Workshop on Policies for Distributed Systems and Networks, Lake Como, Italy, pp.3–15., June 2003.

[6] V. G. Bharadwaj, J. S. Baras, "Towards Automated Negotiation of Access Control Policies", Presented at the IEEE 4th International Workshop on Policies for Distributed Systems and Networks (POLICY 2003), Lake Como, Italy, June 2003.

[7] B. Moore, E. Ellesson, J. Strassner, A. Westerinen, "Policy Core Information Model – Ver.1 Specification", IETF RFC 3060

[8] B. Moore ed., "Policy Core Information Model (PCIM) Extensions", IETF RFC 3460

[9] A. Westerinen, J. Schnizlein, J. Strassner, M. Scherling, B. Quinn. S. Herzog, A. Huynh, M. Carlson, J. Perry, S. Waldbusser, "Terminology for Policy-Based Management", IETF RFC 3198

[10] G. Patz, M. Condell, R. Krishnan, L. Sanchez, "Multidimensional Security Policy Management for Dynamic Coalitions", DARPA Information Survivability Conference and Exposition 2001 (DISCEX II), Anaheim, CA, USA, June 2001.

[11] A. Di Ferdinando, P. McKee, A. Amoroso, "A Policy Based Approach for Automated Topology Management of Peer To Peer Networks and a Prototype Implementation", IEEE 4th International Workshop on Policies for Distributed Systems and Networks (POLICY 2003), Lake Como, Italy, June 2003.

[12] K. C. Feeney, D. Lewis, V. P. Wade, "Policy Based Management for Internet Communities", IEEE 5th International Workshop on Policies for Distributed Systems and Networks (POLICY 2004), Yorktown Heights, New York, June 2004.

[13] A. Sahai, S. Singhal, V. Machiraju, R. Joshi, "Automated Generation of Resource Configurations through Policies", IEEE 5th International Workshop on Policies for Distributed Systems and Networks (POLICY 2004), Yorktown Heights, New York, June 2004.

[14] M. Brunner, et al, "Ambient networks management challenges and approaches", In Proceedings of the First International Workshop on Mobility Aware Technologies and Applications (MATA2004), Florianopolis, Brazil, 2004.

[15] R. Szabó, P. Kersch, B. Kovács, Cs. Simon, M. Erdei, A. Wagner, "Dynamic network composition for ambient networks: A management view", In Eurescom Summit 2005: Ubiquitous Services and Applications Exploiting the Potential, Heidelberg, 2005.