ÇOK ETKİ ALANLI HAREKETLİ AĞLAR İÇİN FORMAL GÜVENLİK POLİTİKASI BETİMLEME

Devrim Ünal[1] **M. Ufuk Çağlayan**[2]

[1] Tübitak Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Kocaeli
devrimu@uekae.tubitak.gov.tr
[2] Boğaziçi Üniversitesi Bilgisayar Mühendisliği Bölümü, İstanbul
caglayan@boun.edu.tr

ABSTRACT

In this paper, we propose a method for formal specification of security policies of multi-domain mobile networks with roaming users. Multi-domain mobile networks are characterized by multiple administrative domains, roaming users and different security policies. We are interested in formal specification of authorization policies. We are especially concerned about cross-domain actions of the users, such as roaming, access and communication across domains.

The policy model covers mobility, hierarchy and role-based authorization aspects. A formal domain and inter-domain policy model is presented. Our approach is based on two integral elements: (i) a formal system model, (ii) a formal security policy specification. A novel aspect of our method is the use of ambient logic formulae to specify time and location requirements that a process must satisfy for a policy rule to be applicable.

Keywords: Security policy, formal specification, ambient calculus, process calculus, multi-domain.

1. GİRİŞ

Bir etki alanı bir güvenlik yöneticisi tarafından tanımlanır ve kullanıcılar ile bilgisayarları içerir, birbirine bağlı yerel veya geniş alan ağlar üzerinde yer alabilir. Bir etki alanının kullanıcısı olmak yalnızca bir bağlantı ile sağlanmayıp bir ağ konusundan çok bir güvenlik konusudur. Birçok ağda, güvenliğin ağ altyapısına fiziksel erişim ile ve ağa ilişkin bilgilerin bilinmesiyle sağlandığı varsayılmaktadır. Ancak hareketli kullanıcılar resme dahil oldukça bu varsayım da geçerliliğini yitirmektedir.

Çok etki alanlı ağlarda hareketlilik iki yetenek ile sağlanmaktadır. İlki, *arabağlantı*, birbirine bağlı ağlar arasında bilgi alış verişi demek olup, Internet altyapısı ile sağlanmıştır. Diğer yetenek olan *dolaşım* kullanıcıların birden fazla yönetimsel etki alanına ait ağlara bağlanabilmeleri demektir. Dolaşımda kullanıcının birden çok kuruluş tarafından tek bir kimlikle tanınması ve hareket içerisinde birden çok yönetimsel etki alanının gezilmesi söz konusudur. Dolaşan bir kullanıcının bir *ev* etki alanı olduğu ve birden fazla *yabancı* etki alanlarında dolaşabildiğini varsaymaktayız. Kullanıcı genellikle ev etki alanında bulunmakta ve burada daha fazla erişim hakkına sahip olmaktadır. Kullanıcı bir yabancı etki alanına hareket ederek bağlandığında bu etki alanının bakış açısına göre bir *yabancı kullanıcı* olarak değerlendirilecektir.

Yetkilendirme mekanizmaları bir kullanıcının erişim haklarını güvenlik politikasına dayalı olarak belirlerler. Erişim denetimi mekanizmaları daha sonra kullanıcının kaynağa erişimini bu önceden belirlenmiş erişim haklarına dayalı olarak denetlerler. Böyle bir ortamdaki güvenlik yönetimi kullanıcıların dolaştığı tüm etki alanlarında tek bir kimlikle bilinmesini, ziyaret edilen etki alanındaki kaynaklara erişim sağlarken eylemlerinin ev ve ziyaret edilen etki alanları arasında karşılıklı olarak politikaya göre denetlenmesini gerekli kılar.

Güvenlik politikaları, ziyaretçi kullanıcıların ziyaret edilen etki alanlarındaki iç güven ilişkileri nedeniyle güvenlik mekanizmalarını geçerek güvenlik politikasını delmelerine engel olmak için formal olarak denetlenmelidir. Kullanıcıların olası eylemleri hem ev hem de ziyaret edilen etki alanlarındaki güvenlik politikalarına karşı denetlenmelidir.

Burada çok etki alanlı hareketli ağların güvenlik politikalarını betimlemek için bir yaklaşım önermekteyiz. Bu yaklaşım ambient cebri, ambient modal mantığı ve yüklem mantığı kullanmaktadır. Devam eden araştırmamızda, yöntemimizin bir otomatik teorem doğrulama aracındaki gerçeklemesi üzerinde çalışmaktayız.

2. PROBLEM TANIMI

Kullanıcıların farklı yönetimsel etki alanları arasında dolaşabildiği bir ortamdaki güvenlik politikalarının formal betimlemesi ve doğrulamasıyla ilgilenilmektedir. Bu problem aşağıdaki soruya indirgenebilir: "Hareketli kullanıcıların işlemleri, içerisine geldikleri yönetimsel etki alanlarının güvenlik politikalarına ve etki alanları arasındaki güvenlik politikalarına uygun mudur?"

Bir *güvenlik politikası* etkin öğelerin pasif öğeler üzerinde gerçekleştirebilecekleri *eylemleri* ve

bunların gerçekleştirilebileceği *koşulları* tanımlar. Etkin öğeler aynı zamanda güvenlik politikasında *yetkilendirme özneleri* (veya sadece *özneler*) olarak adlandırılır. Özneler *yetkilendirme nesneleri* (veya sadece *nesneler*) olarak adlandırılan pasif öğeler üzerinde işlemler gerçekleştirebilirler. Özneler kullanıcılar, roller veya sunucu ya da istemci bilgisayarlar olabilir. Nesneler ağ kaynakları olup uygulamalar, dosyalar, veri tabanları veya mesajlar olabilir. Etki alanları ve bilgisayarlar aynı zamanda pasif öğeler şeklinde davranarak yetkilendirme nesneleri olabilirler.

Bir *yönetimsel etki alanı* alanı bir öğeler kümesi tanımlar. Eylemler bir özne tarafından bir etki alanında gerçekleştirilebilecek işlevleri tanımlar. Bir eyleme izin verilmesi için zaman, kimlik, rol üyeliği, kullanıcı grubu üyeliği, konum ve hareketlilik gibi koşullar olabilir. Tüm bu öğelere bağlı kurallar kümesi bir etki alanındaki güvenlik politikasını oluşturmaktadır.

Bu tanımların sonucu problem tanımını şu şekilde formalize edebiliriz: "Bir sistem modelinde, hareketli kullanıcılar farklı yönetimsel etki alanlarını gezmektedir. Etki alanı güvenlik politikaları ve etki alanları arasında bir güvenlik politikası mevcutken, kullanıcıların eylemleri bu güvenlik politikalarına uygun olup olmadığının ve bu güvenlik politikaları birbirleriyle uyumlu olup olmadığının formal olarak doğrulanması hedeflenmektedir."

3. İLGİLİ ÇALIŞMALAR

Güvenlik politikalarının mantık tabanlı betimlenmesi evrensel yapıtaşlarına dayanır ve formal cebir yöntemlerini destekler. Mantık kullanımı aynı zamanda model doğrulama ve teorem ispatı yöntemleri için otomatik araç desteği sağlar.

Flexible Authorization Framework (FAF) [1], [2] yetkilendirme politikalarının tanımlanması, türetilmesi ve çelişkilerin çözülmesi için mantık programlamasına dayalı bir yöntemdir.

Mantığa dayalı olarak açık izin reddini, hiyerarşileri, politika çıkarımını ve çelişki çözümlemeyi destekleyen başka bir önemli çalışma [3]'tür. Woo ve Lam [4] yarı tutarlı bir formal dil ile yetkilendirmeleri mantıksal yapıtaşlarına dayalı olarak betimlemeyi seçmişlerdir. [5] çalışmasında deontik mantık kullanılarak *izin*, *zorunluluk* ve *yasaklama* unsurları sorumluluk, delegasyon ve zaman yapıları gibi yönetsel kavramları modellemek için kullanılmıştır. Küme ve fonksiyonlara dayalı bir güvenlik politikası dili [6]'da sunulmuştur.

Her konumda kullanılabilecek uygulama katmanı güvenlik politikalarında uzaysal yapılandırmalarla ilgili çıkarımda bulunmak [7] çalışmasında göz önüne alınan konulardan biridir. Bu çalışmada ambient cebri ve ambient mantığının basitleştirilmiş bir sürümü bir güvenlik politikasındaki politika kurallarında kullanılmıştır. Süreç cebirlerinin güvenlik politikası betimlemesinde kullanımına bir örnek ise Sπ cebrinin formal dil olarak kullanıldığı ve gerçeklemede Datalog kullanılan [8]'dir.

Bunlara benzer olarak bizim yaklaşımımızda da süreç cebri ve onunla ilişkili modal mantık kullanılmaktadır. [8]'in aksine Ambient cebri [9] kullanılacak ve gerçeklemede bir otomatik teorem doğrulama aracı kullanılacaktır. [7]'nin aksine uygulama düzeyi politikalarından ziyade ağ düzeyi politikaları kapsanacak ve fiziksel konum değil, etki alanları ve bilgisayarlardan oluşan mantıksal konumlar göz önüne alınacaktır.

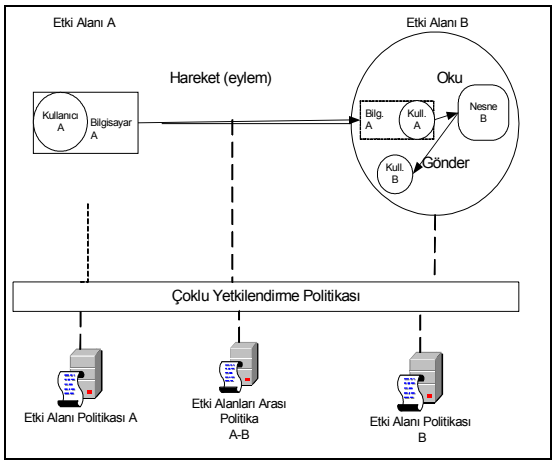
4. MODELLEME YAKLAŞIMI

Tüm formal model aslında iki alt modelden oluşmaktadır. Bunlardan ilki dinamik bir sistem modeli, diğeri ise bir güvenlik politikası modelidir. Sistem modelinde sisteme özgü ve dinamik öğeler bulunmaktadır: etki alanları, ağ üzerindeki kullanıcılar ve kaynaklar ile kullanıcıların mümkün eylemleri. Güvenlik politikası yönetimsel yapıya özgü ve durağan öğeleri modeller: sistem tarafından sağlanması gereken kurallar ve kullanıcıların eylemleri üzerindeki kısıtlamalar. Birden çok yetkilendirme politikasından oluşan güvenlik politikası modeli, dinamik sistem modelindeki eylemler için bir denetleyici konumundadır.

Dinamik ve sisteme özgü öğelerin durağan ve yönetimsel yapıya özgü öğelerden ayrılması daha etkin bir betimlemeye olanak tanımaktadır. Tüm olası sistem yapılandırmaları ve eylemlerin statik olarak doğrulanması gerekmez, yalnızca bir çoklu etki alanlı hareketli ağ modelinin belirli bir örneğinde ortaya çıkanların doğrulanması yeterlidir.

Şekil 1'de gösterilen örnekte, Etki Alanı A'daki Kullanıcı A, Bilgisayar A'ya oturum açmıştır. Daha sonar Etki Alanı B'ye hareket eder, bir dosya okur ve bunu Etki Alanı B'deki Kullanıcı B'ye gönderir. Bu türden bir senaryo Kullanıcı A'nın eylemlerinin birden çok politika uygulama noktasında denetlenmesini gerektirir. Bu uygulama noktalarındaki cihaza özgü güvenlik politikaları genellikle bir yönetici tarafından yönetimsel politikalara bağlı olarak yapılandırılır, örneğin etki alanı politikaları ve etki alanları arasındaki politikalar. Bu çalışmada, politika uygulama noktalarındaki politikalardan ziyade etki alanı ve

etki alanları arasındaki politikaları modelleme ele alınmaktadır.

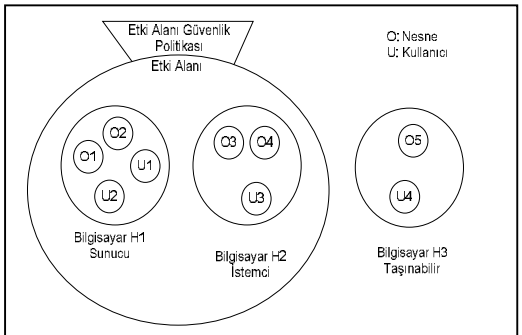


Şekil 1. Modelde sistem öğeleri, birden fazla politika ve kullanıcıların eylemleri vardır.

5. ÇOK ETKİ ALANLI HAREKETLİ AĞ MODELİ

Bir çok etki alanlı hareketli ağa ilişkin sistem modeli beş kümeden oluşmaktadır: etki alanları, kullanıcılar, nesneler, güvenlik hizmetleri ve eylemler.

1. Etki alanları kümesi (D): Bir etki alanı belirli bir hareketli ağı tanımlar. Etki alanı aynı zamanda diğer ağ öğeleri için bir taşıyıcı görevi görür; bir etki alanındaki özneler, nesneler ve güvenlik politikasını tanımlar.
2. Bilgisayarlar kümesi (H): Bilgisayarlar bilgi işlem uçları ve nesneler için taşıyıcı olarak görev alırlar. Her bir kullanıcının sistemdeki nesnelere erişebilmek için bir etki alanında oturum açması gerekir.
3. Kullanıcılar kümesi (U): Kullanıcılar ana etki alanı olarak tek bir etki alanına üye olabilirler. Ayrıca bir etki alanından diğerine gezebilirler. Kullanıcının tüm etki alanlarında aynı kimlikle tanındığını varsayıyoruz.
4. Nesneler Kümesi (O): Nesneler bir etki alanındaki kaynaklardır. Nesneler veritabanlarını, dosyaları ve iletileri modellemektedir. Nesneler bilgisayarlar içerisinde yer alır ve bilgisayarlar ile etki alanlarına girebilir ve oradan çıkabilirler. İletiler ağda dolaşabilir.
5. Eylemler Kümesi (A): Eylemler özne ve nesneler arasında erişim, hareketlilik ve iletişim için kullanılır. Sistem modeli içerisindeki eylemler kümesi Ambient Calculus yetenekleri olarak modellenmiştir. Özneler diğer özne ve nesnelerle eylem sırası olarak etkileşimde bulunmaktadır.



Şekil 2. Tek bir etki alanı, farklı bilgisayarlar, kullanıcılar ve nesneler içeren bir ağın sistem modeli

6. GÜVENLİK POLİTİKASI

Güvenlik politikası, güvenlik mimarisi öğelerinin kullanımını belirleyen kurallar kümesidir. Tenek kural kümesi aşağıdaki gibidir:

Yetkilendirme terimi $at = (as, ao, sa, fo, co)$
$as \in \mathbf{AS}$: yetkilendirme öznesi
$ao \in \mathbf{AO}$: yetkilendirme nesnesi
sa: işaretli (+/-) eylem, eylem $\in \mathbf{A}$
fo: formül, bir ambient mantık formülü
co: koşul, bir önekli mantık formülü
UG: Kullanıcı grupları, **OT:** Nesne türleri, **R**: Roller, $\mathbf{AS} = \mathbf{U} \cup \mathbf{UG} \cup \mathbf{R} \cup \mathbf{H}$, $\mathbf{AO} = \mathbf{O} \cup \mathbf{OT} \cup \mathbf{H} \cup \mathbf{D}$, $\mathbf{A}$ = {read, write, execute, move, enrol, leave, connect, disconnect, login, logout, control}. **SP**: Güvenlik politikası = Yetkilendirme terimleri kümesi *at*.

Yetkilendirme teriminin öğeleri süreç modelindeki belirli bir eylemi güvenlik politikası kuralındaki belirli bir kurala eşleştirmek için gerekli kriterleri temsil eder. Her bir kural bir koşula bağlı olup bir formül ile konum ve hareketlilik kısıtlarını tanımlar.

Yetkilendirme öznesi bir eylem gerçekleştirebilecek bir öğedir. Etkin bir öğe olduğundan bir kullanıcı, kullanıcı grubu, bilgisayar ya da rol olabilir. Bir kullanıcı grubu ya da rol doğrudan bir eylem gerçekleştiremez; bir eylemin gerçekleştirilmesini isteyen bir öğenin bunu gerçekleştirmesine izin verilip verilmeyeceği belirlenirken kullanılırlar.

Yetkilendirme nesnesi bir eylemin üzerinde gerçekleştirileceği öğedir. Nesneler, bilgisayarlar ve etki alanları yetkilendirme nesneleri olarak kullanılabilirler. İki ana nesne türü grubu olarak Uygulama nesneleri ve Ağ nesneleri model içerisinde tanımlanmıştır. Bu gruplara ait olan nesne türleri kullanıcı tarafından tanımlanabilirler.

İşaretli eylem bir eyleme açık olarak izin verildiğini ya da reddedildiğini belirler. (+) işareti bir eyleme izin verildiğini gösterirken (-) işareti reddedildiğini gösterir. Politikalar tam olarak tanımlı olmayabilir, bu durumlarda belirtilmeyen erişim izinlerinin red veya kabul şeklinde ele alınacağı politikanın bir parçası olarak tanımlanmalıdır.

7. GÜVENLİK POLİTİKASININ FORMAL BETİMLEMESİ

Güvenlik politikasının formal betimlemesi önekli ambient modal mantığına dayalı olup 6. bölümde tanıtılmış olan yetkilendirme terimi yapısına dayalıdır. Burada gerçekçi güvenlik politikası örneklerine dayalı olarak formal betimleme sürecini sunmaktayız. Günlük dilde tanımlanan güvenlik politikası tümceleri karşılık gelen formal betimleme ile eşleştirilecektir.

İki tür politika betimlemesi mevcuttur. Bunlardan ilki tüm ağ modellerinde geçerli olan soysal politika tümceleridir. İkincisi ise modele özgü güvenlik politikası tümceleri olup system veya güvenlik yöneticisi tarafından tanımlanır. İlk olarak soysal politika betimlemelerine örnek sunmaktayız.

1. "Bilgisayarlar bir etki alanına bağlanmadan önce kayıt olmalıdırlar.": (*as* = host, *ao* = domain, *sa* = (+) connect, *fo* = ✧(domain [T] | host [T] | T), *co* = ∀host∈H ∃domain∈D EnrolledDomainHost (domain, host))
2. "Kullanıcılar oturum açmadan once bir etki alanında kayıt olmalıdırlar.": (*as* = user, *ao* = domain, *sa* = (+) login, *fo* = ✧(domain [T] | user [T] | T), *co* = ∀user∈U ∃domain∈D EnrolledDomainUser (domain, user))
3. "Kullanıcılar bir etki alanında herhangi bir işlem yapmadan önce bir bilgisayarda oturum açmalıdırlar.": (*as* = user, *ao* = domain, *sa* = (+) A\{login}, *fo* = ∃host ∃domain ✧domain[✧host[user]], *co* = ∀user∈U ∃domain∈D ∃host∈H)
4. "Kullanıcılar bir bilgisayarda oturum açma dışında herhangi bir işlemi, yalnızca oturum açmışlarsa yapabilirler.": (*as* = user, *ao* = host, *sa* = (-) A\{login}, *fo* = ✧host [user [T] |T]|T, *co* = ∀user∈U ∃host∈H)
5. "Kullanıcılar bir bilgisayarda bulunan nesne üzerinde eğer o bilgisayarda oturum açmadılarsa işlem yapamazlar.": (*as* = user, *ao* = object, *sa* = (-) A, *fo* = ✧host [object [T] |T]|user[T]|T, *co* = ∀user∈U ∃object∈O ∃host∈H)
6. "Bir bilgisayar tarafından herhangi bir işlem yapılmadan once bilgisayar etki alanına bağlanmış olmalıdır.": (*as* = host, *ao* = domain, *sa* = (+) A\{connect}, *fo* = ∃domain ✧domain[✧host], *co* = ∀host∈H ∃domain∈D)
7. "Bir öğeyi bir etki alanına kaydetmek yalnızca yönetici tarafından yapılabilir.": (*as* = admin_user, *ao* = domain, *sa* = (+) enrol, *fo* =T, *co* = ∀domain∈D ∃admin_user∈U Administrator (admin_user))

Aşağıda modele özgü politika tümcelerinin formal betimlenmesine bazı örnekler bulunmaktadır.

8. "Bilgisayar 2'deki dosyalar taşınabilir bilgisayarlar tarafından okunamazlar.": (*as* = Portable, *ao* = Portable, *sa* = (-) read, *fo* = ✧ (Portable [] | Host2 [file[]]), *co* = T)
9. "Kullanıcı 1 Kullanıcı 2'ye ileti gönderemez.": (*as* = User1, *ao* = User2, *sa* = (-) send, *fo* = ✧ User1 [message[] | T] ∧ ✧ User2[T], *co* = T)
10. "Taşınabilir 1 Etki Alanı B'ye bağlanabilir.": (*as* = Portable1, *ao* = DomainB, *sa* = (+) connect, *fo* = ✧ (Portable1 [T] | DomainB [T]), *co* = T)
11. "Kullanıcı 1, Bilgisayar 2'ye oturum açabilir (önceden oturum açmadıysa)": (*as* = User1, *ao* = Host2, *sa* = (+) login, *fo* = ✧ (Host2 [T] | User1 [T]), *co* = T)

Bu betimleme örneğinde, User1, User2 ∈ **U**, Portable1 ∈ **H**, DomainA, DomainB ∈ **D**. Bu betimlemede kullanılan mantık önekleri aşağıda açıklanmaktadır:

- EnrolledDomainUser (*d*, *u*), *d*∈**D**, *u*∈**U**, kullanıcı *u*'nun etki alanı *d*'ye kayıt olup olmadığını belirler.
- EnrolledDomainHost (*d*, *h*), *d*∈**D**, *h*∈**H**, bir bilgisayar *h*'nin etki alanı *d*'ye kayıt olup olmadığını belirler.
- ActiveDomainUser (*d*,*u*), *d*∈**D**, *u*∈**U**, kullanıcı *u*'nun etki alanı *d*'ye oturum açıp açmadığını belirler.
- Administrator (*u*), *u*∈**U**, bir kullanıcı *u*'nun yönetici hakları olup olmadığını belirler.

8. SONUÇ

Çok etki alanlı hareketli ağlardaki güvenlik politikalarının formal olarak betimlenmesi ve doğrulanması için bir yöntem önermiş bulunuyoruz. Yaklaşımınızın kökünde ambient cebri ve mantık tabanlı yetkilendirme çerçeveleri bulunmaktadır. Bu çalışmanın katkıları şunlardır: (i) esnek süreç cebri tabanlı güvenlik politikası betimlemesi, (ii) hareketlilik ve konum tabanlı formal güvenlik politikası betimlemesi. Aşağıdaki konular süregelen araştırma problemleri olarak ele alınmaktadır:

- Etki alanları arasındaki güvenlik politikalarının modellenmesi,

- Süreç eylemlerinin güvenlik politikasına karşı otomatik olarak denetlenmesi,
- Yöntemimizin bir otomatik doğrulama aracıyla gerçekleştirilmesi.

KAYNAKLAR

1. Jajodia, S., Samarati, P., Subrahmanian, V. S.: A Logical Language for Expressing Authorizations, Proceedings of the 1997 IEEE Symposium on Security and Privacy, IEEE (1997) 31-43
2. Jajodia, S.: "Flexible Support for Multiple Access Control Policies", ACM Trans. Database Systems, Vol. 26, No: 2, (2001) 214-260.
3. Bertino, E., Ferrari, E., Buccafurri, F., and Rullo, P: A Logical Framework for Reasoning on Data Access Control Policies. In Proceedings of the 1999 IEEE Computer Security Foundations Workshop. CSFW. IEEE Computer Society, Washington, DC, 175 (1999).
4. Woo T. Y. C. and Lam S. S.: Authorizations in distributed systems: A new approach. Journal of Computer Security, 2 (1993) 107--136.
5. Cuppens, F., Saurel,C.: Specifying a Security Policy: A Case Study, 9th IEEE Computer Security Foundations Workshop, Kenmare, Ireland, IEEE Computer Society Press, (1996) 123-134.
6. Ryutov, T., Neuman, C.: Representation and Evaluation of Security Policies for Distributed System Services, Proc. DARPA Information Survivability Conference, DARPA (2000)
7. Scott D.J., Abstracting application-level security policy for ubiquitous computing. UCAM-CL-TR-613, Cambridge University (2005)
8. Fournet, C., Gordon,A.D., Maffeis,S.: A Type Discipline for Authorization Policies, Lecture Notes in Computer Science, Volume 3444. Springer-Verlag,(2005) Pages 141 – 156
9. Cardelli, L., Gordon, A.D., Mobile Ambients, Theoretical Computer Science 240 (2000) 177-213
10. Charatonik W., Dal Zilio S., Gordon A.D., Mukhopadhyay S., Talbot J. M.: Model Checking Mobile Ambients, Proc. FOSSACS 2001, LNCS 2030, (2001) 152-167
11. Luca Cardelli, Andrew D. Gordon, Ambient Logic, Mathematical Structures in Computer Science, basılacak.