TASARSIZ AĞLARDA DAĞITIK ANAHTAR YÖNETİM SİSTEMİ

Elif AKTEN [1] **Bülent ÖRENCİK**[2]

[1]Tübitak-UEKAE P.K 74, 41470, Gebze-Kocaeli
[2]Bilgisayar Mühendisliği Bölümü
Elektrik-Elektronik Fakültesi
İstanbul Teknik Üniversitesi, 80626, Maslak, İstanbul

[1]e-posta: aktenel@uekae.tubitak.gov.tr [2] e-posta: orencik@cs.itu.edu.tr

Anahtar sözcükler:Tasarsız Ağlar,Açık Anahtar Altyapısı,Eşik Kriptografi

ABSTRACT

Ad hoc networks are a new wireless, decentralized communication paradigm for mobile hosts. In traditional networks nodes are interconnected through wired links and there are specialized nodes, i.e. routers that handle packet forwarding. In Ad hoc networks mobile nodes are interconnected through wireless interfaces, and nodes do not rely on any fixed infrastructure. Instead every node in the network functions as a router as well as an application node and forwards packets on behalf of other nodes. [1]

This work covers the issue of securing Ad Hoc networks, which exhibit a number of characteristics that make such a task challenging. One of the major challenges is that Ad Hoc networks typically lack a fixed infrastructure both in form of physical infrastructure such as routers, servers and stable communication links and in the form of an organizational or administrative infrastructure. Another difficulty lies in the highly dynamic nature of Ad Hoc networks since new nodes can join and leave the network at any time. The major problem in providing security services in such infrastructureless networks is how to manage the cryptographic keys that are needed. In order to design practical and efficient key management systems it is necessary to understand the characteristics of Ad Hoc networks and why traditional key management systems cannot be used. [2]

1. GİRİŞ

Güvenlik servisleri , bir ağı güvenli hala getirmek için gerekli olan tüm mekanizmaları içerir. Bu servisler:

- **Gizlilik**: İletilen verinin istenmeyen kişiler tarafından anlaşılmamasını garanti eder.
- **Bütünlük**: İletilen verinin iletim sırasında değişip değişmediğini garanti eder.
- **İnkar Edememe**: İletilen verinin iletiminin ret edilememesini garanti eder.
- **Asıllama**: İletişim yapan tarafların kimlikleri hakkında bilginin doğruluğunu garanti eder.

Güvenlik servislerini sağlamak için ağırlıklı olarak kriptolojik yöntemlere başvurulmaktadır. Açık anahtarlı sistemler ise tüm bu güvenlik mekanizmalarını sağlamak üzere geliştirilmiş kriptolojik yaklaşımlardan biridir. Güvenlik servislerinin temel öğesi olan kriptolojik anahtarların yönetimi de açık anahtar altyapısının görevlerinden biridir.

Güvenlik servislerinin hepsini sağlayan bir altyapı olan açık anahtarlı sistemler kablolu ağlarda yaygın biçimde kullanılmaktadır. Bu altyapının kablosuz ağlarda kullanılması da gittikçe yaygınlaşmaktadır. Böyle bir alt yapının Tasarsız Ağ mimarisindeki sistemlere uygulanması klasik ağlara göre çok daha zor ve karmaşıktır.

Tasarsız ağlar hareketli ve kendi kendini organize edebilen yeni bir ağ modelidir. Geleneksel ağlarda uçlar birbirlerine kablolar aracılığıyla bağlıdırlar; ayrıca ağ üzerinde özelleşmiş sunuculara gerek duyarlar (örneğin paketleri yönlendiren yönlendiriciler). Tasarsız ağlarda ise uçlar kablosuz arabirimler ile birbirlerine bağlıdırlar ve önceden ayarlanmış özel bir altyapıya gerek duymazlar.

Tasarsız ağlar savaş alanlarında, askeri personelin merkezi ve kalıcı bir altyapı olmadan haberleşebilmesi amacıyla kullanılmak üzere geliştirildiler ve basit gezgin cihazları destekleyecek şekilde tasarlandılar.

Tasarsız ağlar yapıları gereği çeşitli özelliklere sahiptir. Bu özellikler:

Dinamik ağ topolojisi: Tasarsız ağlardaki düğümler genelde gezgin yapılı olduklarından ağ içinde hareket ederler ve ağ topolojisi sıklıkla değişebilir.
Kısıtlı Bant Genişliği: Kablosuz iletişim kullanımı geleneksel ağlardan daha düşük iletim kapasitesine sahiptir. Kısıtlı bant genişliği protokolde iletilecek olan mesaj boyutunun kısıtlanmasına sebep olur.
Kısıtlı Enerji : Tasarsız ağdaki düğümler genellikle güç kaynağı olarak pillerle çalışmaktadır. Düğümlerin bu özelliği karmaşıklığı yüksek algoritmaların çalıştırılmasını zorlaştırabilmektedir.
Kısıtlı Fiziksel Güvenlik: Kablosuz iletişim hattının kullanılması ağın saldırılara açık olmasına yol açar. Düğümlerin hareketli olması geleneksel ağlardan daha fazla risk getirmektedir.

Tasarsız ağlara güvenlik yöntemleri geliştirilirken bu karakteristikleri göz önünde bulundurulmalıdır. Ayrıca tasarsız ağlar için geliştirilen güvenlik çözümlerinin zorluğu tasarsız ağların şu özelliklerinden ileri gelmektedir.

- Tasarsız ağlar pasif ve aktif her türlü saldırıya açıktır.
- Hareketli düğümler her zaman ve her yerde servis talep ederler.
- Geniş ölçekli ağlar için ölçeklenebilir bir çözüm gerekmektedir.

Tasarsız ağlar özellikle haberleşmeyi dinleme, ikinci kere tekrarlama ve araya girip değiştirme saldırılarına karşı tam bir hedef durumundadırlar. Dolayısıyla kablosuz ağlar bu tip saldırılara karşı koyacak mekanizmaları içinde barındıracak şekilde yapılandırılmalıdırlar.

Tasarsız ağlar için tasarlanan pek çok uygulama sağlam güvenlik yapıtaşlarına ve gizlilik koruma yöntemlerine ihtiyaç duymaktadırlar. Sabit yapıları ve kablolu uçları olan ağlarda bu ihtiyaçları karşılayabilmek için merkezi güvenlik çözümleri kullandılar (örneğin güvenilir üçüncü partiler, güvenlik duvarları). Ancak tasarsız ağların sabit bir yapıları olmadığından ve kaotik karakteristiklerinden dolayı bu tür mekanizmaların etkinliği önemli ölçüde kısıtlanmıştır.

Bir iletişim sisteminin başarısı iletilen bilginin güvenliğinden emin olunmasıyla ölçülür. İletişim kuran her hangi iki birimin etkin olarak haberleşebilmeleri için karşılıklı güven kurmaları gerekmektedir. Asıllama böyle bir güven kurmanın temel yoludur. İletişimin herhangi iki uç arasında olabileceği büyük ve dinamik ağlarda her düğümün diğer tüm düğümleri asıllayabilmesini varsaymak olanaksızdır. Bu yüzden doğrulama servisi ayrıca sağlanmalıdır. Bunun geleneksel yöntemlerinden biri de ortak güvenilir üçüncü tarafların devreye sokulmasıdır. Açık Anahtar Altyapılarındaki sertifika otoritesi böyle bir yaklaşımın en başarılı örneklerinden biridir.

Açık anahtar altyapısı iletişim kuran düğümlerin sertifika otoritesi aracılığıyla birbirlerini doğrulayabildikleri herhangi bir ağda kullanılabilir. Ancak böyle bir yapının tasarsız kablosuz ağlarda kullanılması doğası gereği oldukça güçtür.

Açık anahtar altyapısı geleneksel ağlarda başarıyla uygulanmasına rağmen, kablosuz tasarsız ağlarda kabul görüp görmeyeceği belli değildir.

2.KULLANILAN TEMEL YÖNTEMLER VE TASARSIZ AĞLAR

2.1. Eşik Kriptografi

Eşik kriptografi paylaşılması gereken bir sırrın dağıtılması prensibine dayanmaktadır. Tek bir tarafın tüm sırra sahip olmaması gerektiği durumlarda sırrın taraflar arasında paylaşılması gerekir (Örneğin sistem özel anahtarı). Bunu için özel anahtar SK ağda bulunan tüm düğümlere dağıtılır. Özel anahtarı dağıtmak için kullanılan k-1 dereceli fonksiyon,

$f(x) = SK + f_1 x + \ldots\ldots + f_{k-1} x^{k-1}$ {1} şeklindedir.

f_1, f_2, …. ,f_{k-1} katsayıları rastgele üretilmektedir. Bu fonksiyondan her düğüm için bir değer elde edilir ve bu değer,

$Pvi = f(v_i) \bmod N$ {2}

güvenli bir şekilde ilgili düğüme iletilir. SK böylece hiçbir düğümde tek başına bulunmaz; fakat herhangi k-1 düğüm bir araya gelerek Lagrange interpolasyonu ile özel anahtar SK'yı elde edebilir.

$SK = f(0) = \Sigma^{k}_{i=1} \; l_{vi} P_{vi}$, {3}

$l_{vi} = \Pi^{k}_{j=1\, j\neq i} \; v_j/(v_j - v_i)$ {4}

k-1'den az birliktelik ile özel anahtarın elde edilmesi mümkün değildir [3].

Eşik kriptoloji tasarsız ağlara pek çok yönden çok uygundur. Tasarsız ağlar için geliştirilecek anahtar yönetim sisteminde özel anahtarın güvenliğini sağlamak için dağıtmak en uygun yöntemdir. Eğer özel anahtar dağıtılmaz ve tek bir uca teslim edilirse bu ucun güvenliği tüm ağın güvenliği anlamına gelecek ve eğer bu uç kapsama alanına çıkar veya anahtarını çaldırırsa tüm ağın güvenliği kaybedilmiş olacaktır.

Tasarsız ağın oluşturulması zamanında dağıtılan özel anahtar parçaları hem dağıtık bir açık anahtar yönetim sistemi sağlayacak hem de her zaman ve her yerde sertifika servisi sağlayacaktır. Gezgin düğümlerin hareket etmeleri, kapsama dışına çıkmaları veya ele geçirilmeleri, sertifika servisinin tamamının güvenliğine zarar vermeyecektir. Özel anahtarın gerektiği durumlarda ise eşik değeri (k) kadar ucun birlikteliği ile özel anahtar ile yapılabilecek tüm işler yapılabilecektir.

2.2. Kısmi İmzalama

Her düğüm kendisine verilen kısmi anahtar ile (Pv_i) kendisine ait parça özel anahtarını (SKv_i) oluşturur.

$$SK_{v_j} = P_{v_j} l_{v_j}(0) = P_{v_j} \prod_{r=1, r\neq j}^{k} \frac{v_r}{v_r - v_j} \mod N$$

{5}

Düğüm kendi kısmi özel anahtarı ile kısmi olarak imza oluşturabilir. Eğer sisteme yeni katılan düğüm için sertifika, CERT, oluşturulmak isteniyorsa her düğüm ürettiği sertifika istek yapısını, cert , kısmi özel anahtarı SK_{vj} ile imzalar.
Bu imza:

$$CERT_{v_j} = (cert)^{SK_{v_j}} \mod N$$

{6}

Sisteme yeni katılan düğüm kendisi için bir sertifika elde etmek istediğinde sertifikasını oluşan kısmi imzalardan şu şekilde elde eder:

$$CERT' = \prod_{j=1}^{k} CERT_{vj} = (cert)^{\sum_{j=1}^{k} SK_{vj}} = (cert)^{t.N+SK} = \mathrm{CERT}.(\mathrm{cert})^{t.N} \mod N$$

{7}

Herbir uç kendisine gelen kısmi sertifikalardan elde ettiği sertifikanın geçerliliğini daha önceden sahip olduğu sistem açık anahtarı ile kontrol eder.

Sistem özel anahtarı ile imzalı bir sertifikaya sahip olmak ucun sistem kaynaklarına erişebilmesini, haberleşebilmesini sağlayacaktır.

2.3 . Anahtar Güncelleme

Eşik kriptolojide özel anahtar SK'nın güvenliği K tane özel anahtar parçasının düşman tarafından ele geçirilmesine kadardır. k tane ucun düşman tarafından ele geçirilmesi belirli periyotlar dahilinde gerçekleşebilir. Bunun için kısmi anahtarların belirli periyotlarla güncellenmesi gerekmektedir.
Bunun için her uç sabit terimi 0 olan rastgele katsayılı bir fonksiyon üretir ve bu fonksiyonda her düğüm için elde ettiği değerleri ilgili uçlara gönderir. Uçlar elde ettikleri bu değerleri aşağıdaki formüle göre birleştirir.

$$s'_j = s_i + \sum_{i=1}^{n} s_{ij}$$

{8}

Bu yöntem ile sistem konfigürasyonu (n,k) dan (n',k') sistemine geçebilecektir.

Kısmi anahtarların güncellenmesi sistem özel anahtarı değişmeden gerçekleşecek ve sistem başka bir değişiklik olmadan, sertifikalar tekrar imzalanmadan, çalışmaya devam edecektir.

3. ÖNERİLEN DAĞITIK ANAHTAR YÖNETİM SİSTEMİ

Bu çalışmada geleneksel ağlar için kullanılan açık anahtarlı sistemlerin tasarsız ağlar için uygulanabilir olup olmadığının araştırılmış ve bu sistem tasarsız ağlara uyarlanmaya çalışılmıştır. Bu çalışmada temel güvenlik servisleri olan gizlilik, bütünlük, inkar edememe ve asıllama fonksiyonları gerçeklenmiştir.

Bu fonksiyonları sağlamak için gerekli olan sertifikaların imzalanması görevi geleneksel ağlardaki yöntemlerin aksine dağıtık olarak yapılmaktadır. Sertifikalar sistemin güven noktaları olduğu anahtarların yönetilmesi sorumluluğu ağın tüm düğümleri arasında paylaşılmıştır.

Sisteme yeni katılmak isteyen düğüm ağ kaynaklarından faydalanabilmek için sistem özel anahtarı ile imzalanmış bir sertifikaya sahip olmalıdır. Bunun için sertifika talebini bildirir ve k-1 düğüm tarafından kısmi imzalı olarak aldığı cevapları birleştirip "k-bounded offsetting" algoritmasından geçirip geçerli bir sertifika elde eder.

Tasarsız ağlar için önerilen dağıtık anahtar yönetim sisteminde homojen bir yapı vardır ve tüm uçlar benzer yetkilerle donatılmıştır.

Bunun için sisteme sonradan dahil olan uçlarında anahtar yönetimin bir parçası olması gerekmektedir.

Sisteme yeni katılan düğümün diğer düğümler gibi yetkilendirilmesi ve yeni düğüm içinde özel anahtar parçası verilmesi gerekmektedir. Bu anahtar şu şekilde

$$P_{vx} \equiv f(v_x) \equiv \sum_{j=1}^{K} P_{v(x,j)} . l_{v(x,j)}(v_x) \equiv \sum_{j=1}^{K} SS_{(x,j)} (\mathrm{mod}\ N)$$

hesaplanır:

{9}

Böylece sisteme yeni katılan düğüm de sertifika servisinin bir parçası olabilecektir.

4. BENZETİM

Temel güvenlik servislerini gerçekleyen bir sistem olan açık anahtar altyapısının tasarsız ağlara uygunluğunun araştırıldığı bu çalışmada bir benzetim programı yazılmış ve çeşitli parametrelerle tasarsız ağ gerçeklenmiştir.

Benzetim ortamında tasarsız ağda kaç uç olacağı,eşik değeri, ağın genişliği ve uçların kapsama alanları parametriktir. Buna göre sistemin ilk ayağa kalktığı durumda sisteme ait olan özel anahtar SK üretilmekte ve eşik değerine göre rastgele katsayılı fonksiyonda her uç için bir değer elde edilmektedir. Bu ilk değer uçlara güvenli bir şekilde teslim edilmektedir. Ayrıca daha sonra yapılacak olan doğrulamalarda kullanılacak olan sistem sertifikası da verilmektedir. Bu aşamada ayrıca her uç için kendi ürettikleri anahtarlar için sistem özel anahtarıyla imzalı birer sertifika üretilmektedir.

Sistem bundan sonra işleyişini tek başına sürdürebilecektir. Eğer sisteme yeni bir düğüm katılacak olursa bu düğümün yetkilendirilmesi yapıldıktan sonra bu uç içinde sistem özel anahtarı ile imzalı bir sertifika oluşturulur. Bu imza yeni katılan düğümde kısmi imzaların birleştirilmesi ve geçerli bir imza elde edilmesi şeklinde olacaktır.

Sistem anahtar yönetiminden de sorumludur. Bu amaçla periyodik anahtar güncelleme ve suçlu düğümlerin ilan edilmesi gibi mekanizmaları da içinde bulundurmaktadır.

Benzetim ortamı ile ilgili şekil bildirinin sonunda yer almaktadır (Şekil 1).

5. SONUÇ

Teknolojide meydana gelecek gelişmelerin paralelinde tasarsız ağlar kendilerine daha fazla uygulama alanı bulabileceklerdir. Sahip olduğu özellikler dolayısıyla yaygınlaşacak olan tasarsız ağlar için çeşitli güvenlik mekanizmalarına ihtiyaç duyulacaktır. Bu mekanizmaların tüm ihtiyaçları sağlaması ve tam olarak tasarsız ağların yapısına ve ihtiyaçlarına uyması çok zordur. Tasarlanan dağıtık anahtar yönetim sistemi tasarsız ağların yapısına uygundur ve açık anahtarlı sistemlerin sağladığı tüm güvenlik çözümlerini içinde barındırır. Açık ağların yönetimi ve anahtarların güvenliğinin korunması problemi de eşik kriptoloji ile aşılmıştır.

KAYNAKLAR

[1] **Konrad Wrona ,** 2002. Distributed Security in Ad hoc Networks.

[2] **Klas Fokine,** 2003. Key Management in Ad Hoc Networks.

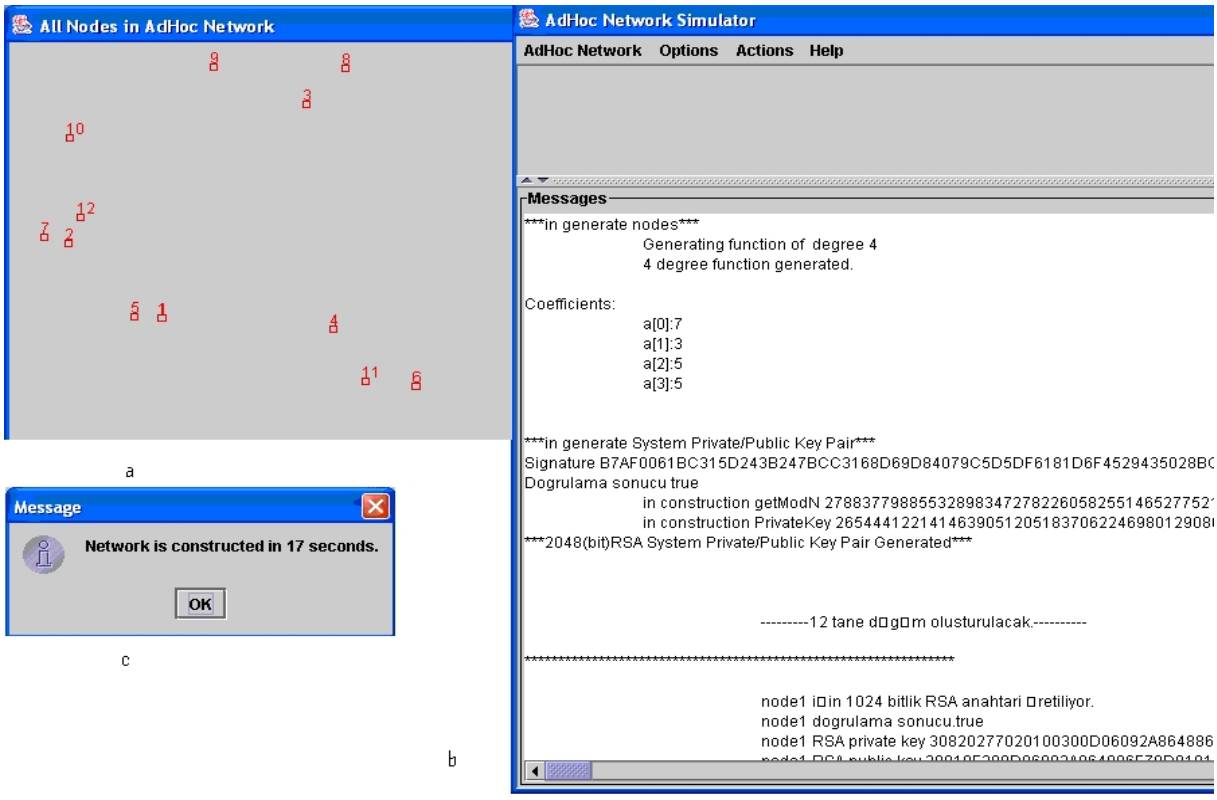
[3] **Charlie Khaufman, Radia Perlman, Mike Speciner**, "Network Security - PRIVATE Communiction in a PUBLIC World", Prentice Hall Series in Computer Networking and Distributed Systems, Upper Saddle River, NJ.

[4] **ZHOU, L., AND HAAS,** Z. J. Securing Ad Hoc Networks. *IEEE Network 13*, 6 (1999), 24–30.

[5] **H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang,** IEEE ISCC 2002. Self-securing Ad hoc Wireless Networks.

[6]**Vesa Kärpijoki**, Helsinki University of Technology Telecommunications Software and Multimedia Laboratory 2002**.**Security in Ad hoc Networks.

[7] **PERKINS, C. E., Ed**. 2001. Ad hoc networking.



Şekil 1 Tasarısız ağın oluşturulması