YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

TELSİZ ÖRGÜ AĞLARDA WPS TABANLI GÜVENLİ KURULUM VE DAĞITIK YÖNETİM SİSTEMİ TASARLANMASI VE GERÇEKLENMESİ

Mühendis Gürsel MUTLU

FBE Bilgisayar Mühendisliği Anabilim Dalında Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı : Yrd. Doç. Dr. A. Gökhan YAVUZ

İSTANBUL, 2010

İÇİNDEKİLER

Sayfa

KISALTMA LİSTESİ

AES	Advanced Encryption Standart
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
IEEE	Institute of Electrical and Electronics Engineering
IPTV	Internet Protocol television
ISM	Industrial, Scientific, Medical
MAC	Media Access Control
MIMO	Multiple Input - Multiple Output
OFDM	Orthogonal Frequencies Division Multiplexing
PIN	Personal Identification Number
RC4	Rivest Cipher 4
SES	Secure Easy Setup
UUID	Universally Unique Identification Number
UPnP	Universal Plug and Play
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WMN	Wireless Mesh Network
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

ŞEKİL LİSTESİ

ÇİZELGE LİSTESİ

ÖNSÖZ

Yüksek lisans eğitimi ve tez geliştirme süresince yardımlarını esirgemeyen tez danışmanım Yrd. Doç. Dr. A. Gökhan YAVUZ'a, AirTies'da bu tez çalışmasının geliştirilmesi ve gerçeklenmesi için bilgi ve deneyimlerini paylaşan Fırat BİRLİK ve Can İLHAN başta olmak üzere tüm çalışma arkadaşlarıma teşekkürü bir borç bilirim.

ÖZET

Günümüzde telsiz ağlar bir çok alanda kullanım bulmaya başlamıştır. Bu arada telsiz ağlar teknolojisi kullanıcıların ihtiyaçlarına ve yaşadıkları zorluklara göre geliştirilmeye devam etmektedir. Bu tez çalışmasında kapsama alanı arttırımı ve güvenlik ayarları kurulumu konusunda bir çalışma yürütülmüştür. Bu çalışma sonucunda telsiz ağların kapsama alanını arttırmada kullanılan telsiz örgü ağlarının kurulumu ve dağıtık olarak ayarlanması konusunda bireysel kullanıcıların yaşadıkları zorlukları aşmak amacıyla güvenli bir yöntem tasarlanmış ve gerçeklenmiştir.

Tasarlanan yöntem veri alış verişinde bireysel kullanım alanlarında güvenli ve kolay kurulum için tanımlanmış olan WPS tanımlamasını temel alır. Bu sayede sıradan bir bilgisayar kullanıcısının bile erişim noktaları üzerinde kurulum düğmelerine basmak suretiyle güvenli bir örgü ağı kurarak telsiz ağ kapsama alanını genişletmesine olanak sağlar. Ayrıca telsiz ağ ayarları ile ilgili bir değişikliğe ihtiyaç duyulduğunda kullanıcının örgü ağını oluşturan cihazlardan herhangi birinin yönetim arayüzünde bu değişikliği yapması yeterlidir. Yapılan değişiklik örgü ağının diğer üyelerine telsiz ağ üzerinden güvenli ve otomatik olarak aktarılıp örgü ağı yeni ayarlarıyla çalışmaya başlar.

Anahtar Kelimeler: Telsiz örgü ağı, WPS, dağıtık ayar yönetimi

ABSTRACT

Wireless local area networks has become ubiqitous in the last few years. Wireless local area networking technology is still under development according to the new demands and issues reported by users. In this thesis, coverage extension and security settings setup have been studied. As a result, a new, secure method was designed that addresses the difficulties of wireless mesh network setup and distributed configuration of it.

Data exchange in our proposed system is based on the secure data exchange technique documented in Wi-Fi Protected Setup (WPS) specification defined by Wi-Fi organization for personal wireless LAN's. Hence, even a regular computer user may set up a WMN in order to increase the coverage by just pressing the setup buttons on wireless access points. In addition, if any configuration modification is required for WMN during regular operation; the user needs just to configure one of the member of WMN and then the new configuration will be delivered automatically using a secure communication and whole members will start operating using the new configuration.

Keywords: Wireless mesh networks, WPS, distributed configuration management

1. GİRİŞ

Bilgisayar sistemlerinin sayısındaki hızlı artışın ardından geçtiğimiz on yılda bilgisayar sistemleri için en önemli gereksinimlerden birisi taşınabilirlik olmuştur. Ayrıca Internet'in yaygınlaşmasıyla bilgisayar ağları bilgisayarlar için vazgeçilmez hale gelmeye başlamıştır. Bu durum telsiz bilgisayar ağları konusundaki araştırmaların hız kazanmasına sebep olmuştur. Araştırma, geliştirme ve standardizasyon çalışmaları sonucunda telsiz bilgisayar ağlarının maliyetleri hızla düşerken performansları onlarca kez artmıştır. Diğer yandan telsiz ağlardaki kapsama alanı tek bir erişim noktasından sağlanacak hizmetin fiziksel kısıtları sebebiyle aynı mertebede artış gösterememiştir.

Telsiz ağların kapsama alanı kısıtlamasını aşabilmek amacıyla IEEE 802.11 standardında telsiz ağların örgü şeklinde birbirine bağlanmasıyla oluşturulacak telsiz ağ dağıtım sistemi yapısı öngörülmüştür. Örgü ağlarının kurulumu ve hizmet sürekliliği için ağı oluşturan tüm düğüm erişim noktaları bir ayar yönetim sistemine ihtiyaç duyar. Bu ihtiyaç kurumsal kullanım alanlarında teknik yetkinliğe sahip kişilerce veya merkezi yönetim yazılımlarınca karşılanabilirken bireysel kullanım alanlarında son kullanıcılar için sorun teşkil etmektedir.

Telsiz ağların güvenlik ayarları sıradan bireysel kullanıcılar için karmaşık olduğundan bu ayarlamalar yanlış veya eksik yapılmaktadır. Seçilen güvenlik seviyesi ve şifresinin ağa dahil olacak tüm cihazlarda ayarlanmış olması gerekir. Bu durum özellikle kullanıcı ekranı olmayan veya ayarlanması teknik bilgi gerektiren telsiz ağ cihazlarında ilgili ayarların hiç yapılmadan çalıştırılması şeklinde sonuç verebilmektedir.

Bu tez çalışması kapsamında, telsiz örgü (mesh) ağı kurulumunu kolaylaştırmak ve düğüm noktalarını dağıtık olarak yönetmek amacıyla bir yöntem önerilmiş ve gerçeklenmiştir. İlgili yöntem, düğüm noktalarının yanı sıra telsiz ağa dahil tüm cihazlara ayar bilgisi dağıtımı ve eşleştirilmesi amacıyla da kullanılabilir. İlgili yöntem sayesinde bireysel kullanım alanlarında örgü ağı oluşturmak için düğüm noktalarında fiziksel bir düğmeye basmak yeterli olacaktır. Ayrıca, herhangi bir ayar değişliği ihtiyacında düğüm noktalarından birinde yapılan ayar değişikliği bu değişikliğin ağa dahil diğer tüm düğümlere aktarılmasını sağlayacaktır.

Tez kapsamında düğüm noktaları arasındaki veri alışverişi için telsiz ağlarda kolay ve güvenli kurulum amacıyla Wi-Fi organizasyonu tarafından geliştirilen Wireless Protected Setup (WPS) tanımlamasını kullanılmıştır. WPS'teki yeni hizmet geliştirmeye açık protokol yapısı sayesinde düğümler arası ayar alışverişi için güvenli bir iletişim kanalı oluşturulmuştur. Ayar değişikliklerinin otomatik dağıtılması için ise düğüm noktası olarak hizmet veren gömülü

bilgisayar sistemleri üzerinde ayar sıra numarası takibi yapısı geliştirilmiştir. Geliştirilen sistem, iletişim kanalının güvenli kabul edilmesi nedeniyle bu kanal üzerinden telsiz ağ güvenlik ayarlarının dahi aktarılmasına imkan tanımaktadır.

Tezin 2. bölümünde telsiz bilgisayar ağlarının gelişimi başlığı altında telsiz örgü ağları ile bu ağların kurulum, güvenlik ve yönetim gereksinimleri incelenmiştir. 3. bölümde WPS tanımlaması, kullanım alanları ve sağladığı güvenlik değerlendirilmiştir. 4. bölümde telsiz örgü ağlarının otomatik ayar güncelleme ihtiyacı ve bu ihtiyacın karşılanması için bu tez kapsamında önerilen uygulama açıklanmıştır. 5. bölümde tasarlanan yöntemin gerçeklenmesiyle ilgili detaylar aktarılmıştır. Altıncı ve son bölümde sonuç ve bundan sonraki çalışmalar için önerilere yer verilmiştir.

2. TELSİZ BİLGİSAYAR AĞLARININ GELİŞİMİ

Geçen yüzyılın en büyük buluşlarından birisi olan bilgisayarlar özellikle bilgiye çok kolay erişmemize olanak sağlayan Internet teknolojisinin geliştirilmesiyle bir çok uygulama alanı bulmuştur. Öyle ki; günümüzde sadece kurumsal alanlarda değil evlerde de birden çok bilgisayar ve bunları kapsayan bir yerel bilgisayar ağı bulunmaktadır. Bilgisayar ağlarının bu kadar önem kazanması, bu ağları kolay kurmayı ve bu ağlara rahat erişmeyi zorunlu hale getirmiştir. Bu ihtiyaç tellerin kullanıldığı ağlar yerine telsiz bilgisayar ağı teknolojisinin gelişmesine olanak tanımıştır. Elektrik, elektronik ve bilgisayar teknolojilerinde bir çok standardın sahibi olan Institute of Electrical and Electronics Engineers (IEEE), yerel bilgisayar ağları konusunda çalışmalar yürüten 802 adlı grubunun bir alt grubu olarak 802.11 adı verilen telsiz bilgisayar ağları standardından sorumlu bir görev grubu oluşturmuştur. İlgili görev grubu tarafından geliştirilen standart 1997 yılında taslak, 1999 yılında da ilk sürüm olarak yayınlanmıştır [1]. Bu ilk sürüm günümüzde kullanım dışıdır [2]. Standart, fiziksel katmanda ve MAC katmanında tanımlı olup 2.4 GHz Endüstriyel, Bilimsel, Tıbbi (Industrial, Scientific, Medical - ISM) frekans bandını kullanmaktadır (Ritz, 2003). 802.11 görev grubu, ortaya çıkan ihtiyaçlara göre eklemeler yaparak standardı geliştirmeye devam etmektedir. Standarda yapılan eklemeler, 802.11x adı ile tanımlanmış olup x bir harf veya harf grubunu temsil etmektedir (Köksal, 2007). Standarda veri akış hızı ve modülasyon konusunda yapılan eklentiler Çizelge 2-1'de gösterilmiştir.

Çizelge 2-1 IEEE 802.11 hız ve modülasyon eklentileri [2]

802.11 Protokolleri							
Adı	**Eklenme Tarihi**	**Frekans (GHz)**	**Bant Genişliği (MHz)**	**Veri akış hızı (Mbit/s)**	**MIMO Akış Sayısı**	**Modü-lasyon**	**Kapsama alanı (Kapalı - Açık) (m)**
	06/1997	2.4	20	1, 2	1	DSSS	20 – 100
a	09/1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	35 – 120
		3.7					-- - 5,000
b	09/1999	2.4	20	1, 2, 5.5, 11	1	DSSS	38 – 140
g	06/2003	2.4	20	1, 2, 6, 9, 12, 18, 24, 36, 48, 54	1	DSSS, OFDM	38 – 140
n	10/2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	4	OFDM	70 – 250
			40	15, 30, 45, 60, 90, 120, 135, 150			70 – 250

Standarda ekleme yapılan diğer konu başlıklarından ikisi de güvenlik ve örgü ağlarıdır. Bu tez çalışması kapsamında güvenlik ve örgü ağı ayarlarını bireysel kullanıcılar için kolaylaştırıcı bir yöntem tasarlanmıştır.

2.1. Telsiz Ağlarda Güvenlik

Telsiz bilgisayar ağları iletim ortamı olarak elektromanyetik dalgaları kullanır. Elektromanyetik sinyallerin doğası gereği sinyallerin algılanma kapsamında bulunan tüm cihazlar, birbirlerinin iletişimlerini algılayabilir durumdadır. Ancak bu özellik yüzünden telsiz ağ bağlantısı üzerinden haberleşen iki cihazın arasındaki veri akışının içeriğini aynı ortamda bulunan diğer cihazlar da ilgili frekanstaki elektromanyetik sinyalleri dinleyerek öğrenebilir. Hatta kötü niyetli kullanıcılar, herhangi bir kullanıcı onaylama sistemi kullanmayan bilgisayar ağlarına izinsiz olarak dahil olup etkin bir saldırı da düzenleyebilirler. Bu sebeple gizlilik gerektiren telsiz ağ uygulamaları için iletişim ortamındaki veri paketlerinin şifrelenmesine ve ağa dahil olacak kullanıcıların onaylanmasına ihtiyaç duyulmuştur.

IEEE'nin 802.11 telsiz ağlar standardizasyon süreci on yılı aşkın süre önce başlamasına rağmen güvenlik problemi ciddi anlamda ancak son birkaç yılda ele alınmıştır. Standardın ilk halinde güvenlik için önerilen ilk yöntem telli ağdaki güvenliğe denk bir güvenliğin amaçlandığı Wired Equivalent Privacy (WEP) şifreleme yöntemidir [1]. Ne var ki; WEP şifreleme protokolü güvenlik ve şifreleme uzmanları tarafından tasarlanmamıştır. Bu sebeple kısa süre içerisinde, kullandığı Rivest Cipher (RC4) kodlama tekniğinde WEP'in tasarlanmasından 4 yıl öncesinde tespit edilmiş olan güvenlik açığı yüzünden, saldırıya açık olduğu ispatlanmıştır (Lehembre, 2005). Yıllar içerisinde protokolde tespit edilen güvenlik açıkları WEP güvenliğini kırmayı birkaç dakikalık basit bir işlem haline getirmiştir. IEEE802.11 çalışma grubu, ortaya çıkan bu güvenlik açıkları üzerine telsiz ağlarda güvenlik konusunu yeniden ele almak ve standarda güvenlik konusunda ilaveler yapılması için 2001 yılının ocak ayında IEEE802.11i adında bir alt çalışma grubu kurmuştur (Chandra, 2005).

802.11i grubunun çalışmalarıyla biri kısa vadeli diğeri ise uzun vadeli olmak üzere iki aşamalı bir çözüm üretilmiştir (Gürkaş, 2005). Bu çalışmalar esnasında öncelikle sektörün WEP algoritmasındaki güvenlik zaaflarından etkilenmemesi için telsiz ağ donanımı üreticilerinin üyesi olduğu Wi-Fi [3] topluluğu ve IEEE tarafından Wi-Fi Güvenli Erişim (Wi-Fi Protected Access - WPA) [4] adı verilen güvenlik protokolü geliştirilmiş ve bu sayede sektör için geçici bir çözüm üretilmiştir. WPA, mevcut donanımlarda sadece yazılım güncellemesi yapılarak kullanılabilir hale gelmiştir. Mevcut donanımın kullanımına imkan sağladığından daha kolay

ve daha hızlı bir şekilde kullanım bulması sağlanmıştır. 802.11i çalışma grubu tarafından telsiz ağların güvenliği için uzun vadeli çözüm olarak düşünülen WPA2 (IEEE802.11i) [5] ise 2004 yılı Mayıs ayında standart haline gelmiş ve aynı yılın Ekim ayından itibaren bu protokolü destekleyen ürünler üretilmeye başlanmıştır. WPA, WEP tabanlı bir yapı olduğu ve RC4 kaynaklı zaaflarının çıkabileceği şüphesinden ötürü IEEE tarafından geliştirilen WPA2, WPA'nın aksine WEP üzerine kurulmamış, yeni ve farklı bir güvenlik protokolü olarak geliştirilmiştir. WPA2'nin WPA ve WEP'ten en büyük farkı ağ trafiğini şifrelemek için RC4 algoritması yerine AES algoritmasını kullanmasıdır (Gürkaş, 2005).

Tüm bu güvenlik geliştirmelerine rağmen geçtiğimiz yıllarda yapılan araştırmalara göre bir çok kullanıcının pratikte şifreleme yapmadan telsiz ağ kullandığı tespit edilmiştir. Örneğin, 2006 yılında Amerika Birleşik Devletleri'nin Indianapolis eyaletinde yapılan bir araştırmaya göre özellikle telsiz ağ güvenlik ayarları için kolay bir yöntem sunmayan cihazların kullanıldığı durumda kullanıcı onaylama ve şifreleme anlamında güvenlik kullanınımının sadece % 54,5 oranında olduğu tespit edilmiştir (Hottell vd., 2006). Çizelge 2-2, ilgili çalışma kapsamında elde edilen telsiz ağ güvenlik ayarları kullanım miktarını göstermektedir. Bu çizelgede cihaz kurulumu esnasında yardımcı bir uygulama ile güvenlik ayarlarını yapmaya zorlayan üreticinin modeli 2Wire, güvenlik ayarlarını tek bir düğmeye basma işlemine indirgeyen model ise Linksys SecureEasySetup (SES)[6] olarak belirtilmiştir. Bu araştırma telsiz ağlarda güvenlik ayarlarının pratikte kolay bir yolu olmadığında yeterli ölçüde kullanım bulamadığına işaret etmektedir.

Çizelge 2-2 Telsiz ağ güvenlik ayarlarının kullanım oranı örneklemesi (Hottell vd., 2006)

Cihaz modeli	**Toplam ölçüm sayısı**	**Güvenliği ayarlanmış cihazların sayısı**	**Güvenliği ayarlanmış cihazların oranı**
2Wire	340	330	% 97,1
Linksys SES	57	50	% 87,7
Diğer	2046	1116	% 54,5
Toplam	**2443**	**1496**	**% 61,2**

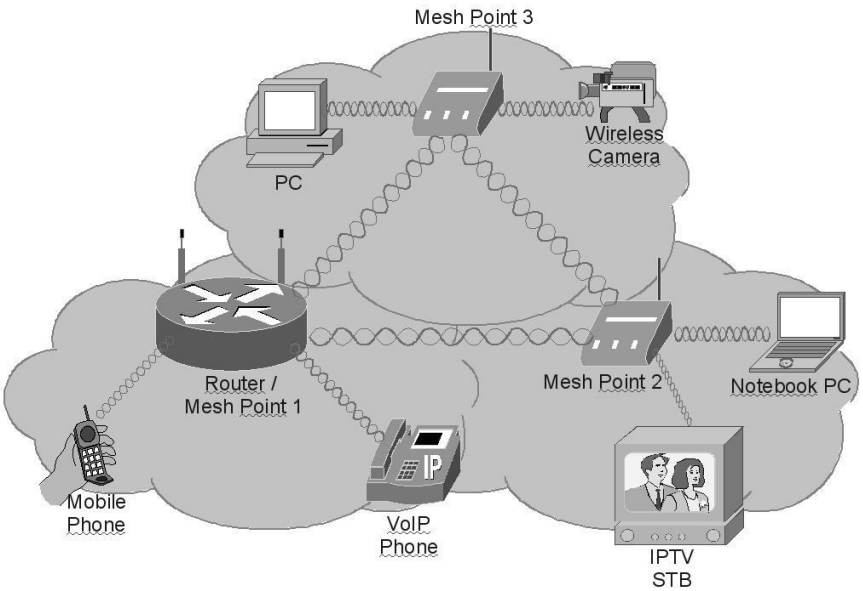
2.2. Telsiz Örgü Ağları

Telsiz ağların yaygınlaşmasıyla, sağladığı faydalardan daha geniş kapsama alanında faydalanabilmek için telsiz ağların kapsama alanının arttırılması konusunda büyük bir talep doğmuştur. Telsiz bilgisayar ağlarının kapsama alanı büyüklüğünü, özellikleri 802.11 standardında belirlenmiş olan elektromanyetik sinyallerin gücünden kaynaklanan erişim mesafesi belirlemektedir. İlgili frekans bandında izin verilen en yüksek sinyal gücü seviyesini ise ülkeye özgü elektromanyetik yayın düzenleme yetkisine sahip kurumlar belirlemektedir.

Bu sebeple tek bir erişim noktasının oluşturduğu telsiz ağ hizmetinin kapsama alanı belirli bir seviyenin üstüne çıkamamaktadır. Bu kısıtlar altında telsiz ağların kapsama alanını arttırmanın yolu 802.11 standardında atıfta bulunulan telsiz dağıtım sistemini (Wireless Distribution System - WDS) kullanmak olmuştur. Telsiz dağıtım sistemi, kapsama alanları örtüşen erişim noktaları arasında telsiz haberleşmenin sağlanmasıyla oluşturulur. Şekil 2-1'de telsiz dağıtım sistemi modellenmiştir.

Telsiz dağıtım sistemi genel olarak telsiz ağ üzerinde birden çok erişim noktasından atlayarak aktarılacak bir paketin başlığındaki adres bilgisine, aracılık yapacak erişim noktasının MAC adresinin eklenmesiyle çalışır [1]. Bu sebeple aracılık yapacak her erişim noktasının önceden yönlendirme bilgilerine sahip olması gerekir. Kapsama alanının arttırılması için eklenen erişim noktalarına tekrarlayıcı adı da verilmektedir. Sadece bir iki tekrarlayıcının kullanıldığı bir sistemde bu işlem her bir erişim noktasına karşılıklı olarak sabit yönlendirme bilgisi tanımlayarak gerçekleştirilebilir. Örgü ağı topolojisinde bir çok tekrarlayıcının yer aldığı bir telsiz bir ağ için ise yönlendirme bilgisinin dinamik olarak cihazlar tarafından bulunabilmesi hem kurulum kolaylığı hem de çalışma sürekliliği açısından gereklidir.

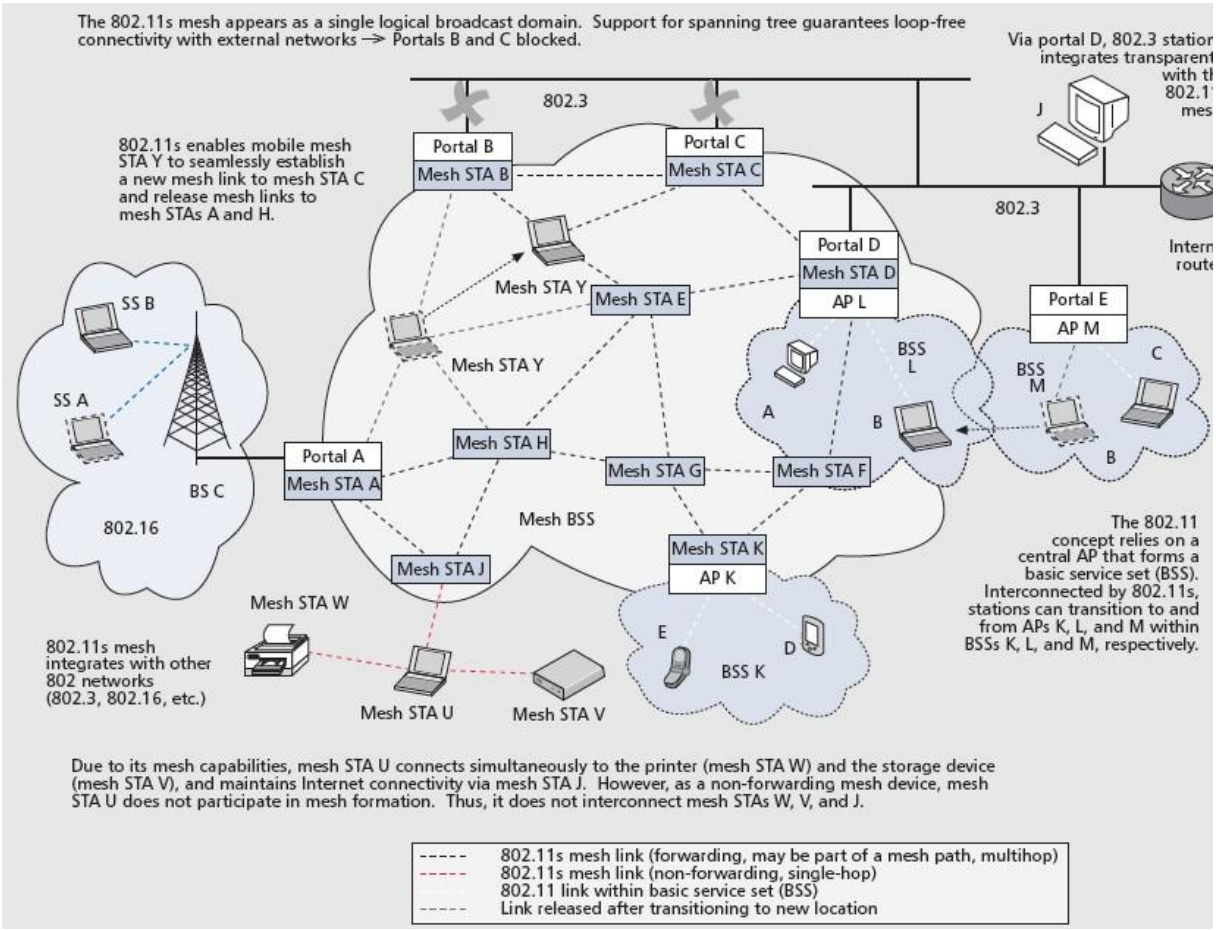
Bu sebeple telsiz örgü ağları genellikle dinamik yönlendirme kabiliyetine sahip erişim noktalarının düğüm olarak görev aldığı ağlar olarak kabul edilirler (Hiertz vd., 2006).



Şekil 2-1 Telsiz dağıtım sistemi modeli

Telsiz örgü ağları, tasarsız gezici ağlar gibi çok atlamalı yönlendirme yapısını kullanarak sıradan telsiz ağların sağladığı faydaları arttırırken altyapı masraflarını da azaltan bir ağ yapısı sağlamaktadır. Bu çoklu atlamalı yönlendirme yapısının kullanımı telsiz ağın hizmet alanını genişletmesinin yanı sıra ağın kendi kendisini onarıcı özelliğini de kazanmasını sağlar (Glass vd., 2008). Örgü ağlarının bu özellikleri, bu teknolojinin çok geniş kapsama alanlı kurulumlar için kablolu bir omurga ağına olan ihtiyacı da ortadan kaldırmaktadır. Bu sayede geniş kapsamlı ağ kurulumu masrafları azaltılırken, kablo altyapısı kurulumu ihtiyacı tamamen ortadan kalktığı için kurulum da kolaylaşmaktadır. Ancak geniş kapsamlı örgü ağı kurulumlarında tüm erişim noktalarının sadece tek bir kanalda hizmet verebilir özellikte olursa ilgili kanalın tüm erişim noktaları tarafından paylaşılarak kullanılmasına sebep olacağından kullanıcı başına düşen veri akış hızı oldukça düşer. Pratikte 8 erişim noktasından daha fazla erişim noktasının kullanımında veri hızlarının sıradan kullanıcıların ihtiyacını karlaşayamacak seviyeye düştüğü görülmüştür. Bu sorunu aşmak için çoklu kanal desteğine sahip erişim noktaları ve bu erişim noktalarının uygun kanal seçimini yönetecek bir sisteme ihtiyaç duyulur.

IEEE, 2004 yılında telsiz örgü ağları mimarisi için ortak bir standart oluşturması amacıyla 802.11s adında bir görev grubu oluşturmuştur. Ancak tamamlanma tarihi pek çok kez ertelenen standart hala taslak aşamasındadır (Glass vd., 2008; Camp ve Knightly, 2008). Standardın kurumsal ve bireysel kullanım alanlarında yerel ve uzak mesafe bilgisayar ağları oluşturacak şekilde geniş kapsamlı olması amaçlanmaktadır (Hiertz vd., 2006). Şekil 2-2'de 802.11s standardında amaçlanan ağ yapısı örneklenmiştir. Örgü ağı topolojisi dağıtık bir sistem olduğu için oldukça karmaşık ihtiyaçlar doğurmaktadır. Geliştirme sürecinde özellikle güvenlik konusunda pek çok tartışma süregelmiş ve tamamlanma zamanı ertelenmiştir.[7]



Şekil 2-2 802.11s standardında önerilen örnek ağ yapısı (Hiertz vd., 2010)

Bu tez çalışması kapsamında geliştirilen uygulamada 802.11s standardında tanımlanan seviyede bir kapsama alanına ihtiyaç duyulmadığı ve standart henüz tamamlanıp uygulama bulamadığı için ilgili standartta önerilen yöntemler doğrudan kullanılmamıştır.

3. GÜVENLİ WI-FI KURULUMU TANIMLAMASI

IEEE 802.11 standardına uygun cihazlar geliştiren önde gelen teknoloji şirketleri 1999 yılında ilgili standart için denetim ve belgelendirme işlemlerini yürütmesi amacıyla Wi-Fi Allience isimli bir organizasyon kurmuştur [3]. Bu organizasyon özellikle üreticiler arası cihaz uyumluluğunun denetlenmesi ve standardın yaygınlığının artması için ticari anlamla önem taşımaktadır. Wi-Fi Allience organizasyonu aynı zamanda telsiz ağlar standardını kullanan cihazlarda pratikte karşılaşılan sorunların çözümüne yönelik teknoloji tanımlamaları (specification) geliştirir ve bunlar için belgelendirme (certification) programlarını yürütür.

Tez kitapçığının 2.1 başlığı altında değinildiği üzere, telsiz ağlarda güvenlik konusunda sürekli iyileştirmeler olsa da kullanıcılar için oluşturduğu ayar zorluğu nedeniyle kullanım oranı ihtiyaç duyulan seviyeye ulaşamamıştır. Buna karşın telsiz ağ yongası üreticileri en azından bireysel kullanım alanlarında güvenlik ayarlarının basitleştirilmesi için kendilerine özgü çözümler geliştirme yoluna gitmişlerdir. Örneğin ilk olarak 2005 yılı Ocak ayında Broadcom ve Atheros isimli telsiz ağ yongası üreticileri, güvenlik ayarlarını tek bir düğme veya kısa bir PIN kullanımı ile sağlayacak uygulamalar duyurmuşlardır [8]. Ancak bunun gibi üreticiye özgü uygulamalar birbiriyle uyumlu olmadığı gibi tek bir üretici tarafından analize kapalı bir ortamda geliştirildiğinden güvenlik seviyesinin analizi kolay olmamaktadır. Wi-Fi organizasyonu bu aşamada devreye girerek muhtemel uyumsuzluk ve güvenlik sorunlarına karşı üreticiler çapında ortak bir sertifika programı kurulmasına karar vermiştir. 2007 yılı Ocak ayında yayınlanan Güvenli Wi-Fi Kurulumu (Wi-Fi Protected Setup-WPS) [9] tanımlaması, kullanıcıların karmaşık güvenlik ayarlarının yapılmasındaki zorluğu aşmaları için geliştirilmiştir. Özellikle cihazlar arası uyumluluk sağladığı için bu tez çalışması kapsamında bu tanımlama ile belirlenen teknolojinin kullanılması tercih edilmiştir.

3.1. WPS Kayıt Protokolü

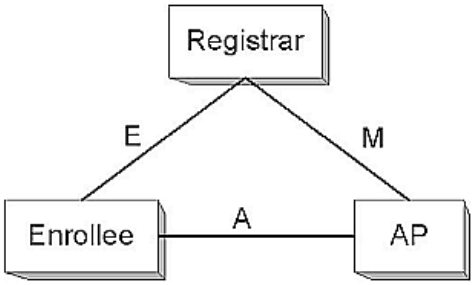
WPS'te veri aktarımı kayıt protokolüyle sağlanır. WPS işlemlerinde rol alan cihazlar için 3 tip rol tanımlanmıştır. Bu roller:

- Ağa yeni kayıt olan birim (Enrollee), bu çalışmada "E" harfiyle ifade edilecektir.
- Ağa kayıt edici birim (Registrar), bu çalışmada "R" harfiyle ifade edilecektir
- Telsiz ağ erişim noktası (AP), bu çalışmada "AP" kısaltmasıyla ifade edilecektir

olarak sıralanabilir. Ayrıca ilgili rolde görev alan birimler arasında iletişim arayüzlerine özel isimler verilmiştir. WPS tanımlamasına göre R ve E rolündeki cihazlar arasındaki arayüz E, R ve AP rolündeki cihazlar arasındaki arayüz M, E ve AP rolündeki cihazlar arasındaki arayüz

ise A olarak isimlendirilmiştir. Şekil 3-1'de ilgili birimler ve aralarındaki iletişim arayüzleri gösterilmiştir.

Kaydedici rolü doğrudan erişim noktası rolünde çalışan cihazda yer alabileceği gibi M iletişim arayüzü kullanılmak suretiyle ağ üzerindeki başka bir cihazda da yer alabilir. Kaydedici ve erişim noktası ayrı cihazlar ise UPnP [10] protokolüne göre haberleşirler.



Şekil 3-1 WPS'te kullanılan birimler ve iletişim arayüzleri (Wi-Fi Alliance, 2006)

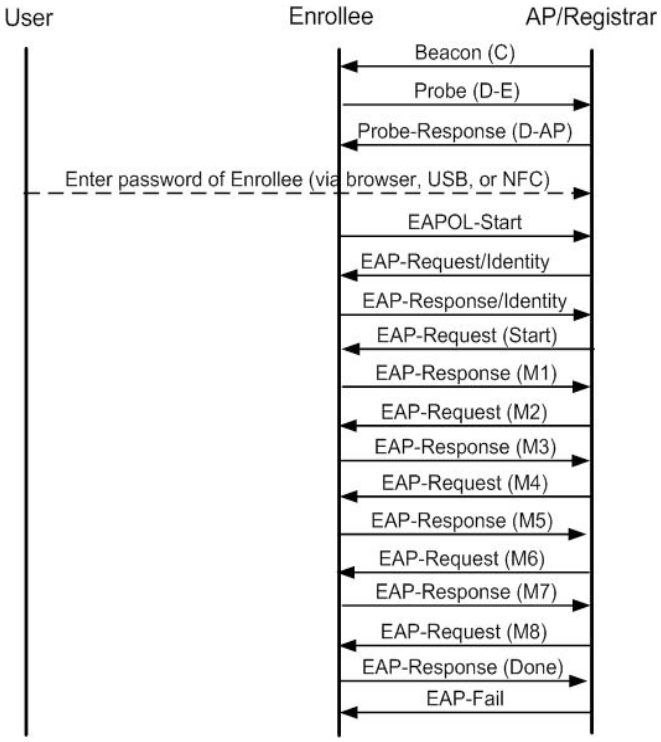
WPS'de kurulum ve ayar aktarımı için "PIN girme", "düğmeye basma" ve "kanal dışı aktarım" olmak üzere 3 farklı seçenek sunulmuştur. (Kuo vd., 2007)

PIN girme ve düğmeye basma senaryoları ilerleyen alt başlıklarda incelenecektir. Kanal dışı aktarım yöntemi ise veri alışverişi için harici bir depolama birimi veya telsiz haberleşme için RFID gibi ek bir donanımın kullanımını gerektirdiğinden bu çalışma kapsamında kullanılmamıştır.

3.2. PIN ile Kurulum Senaryosu

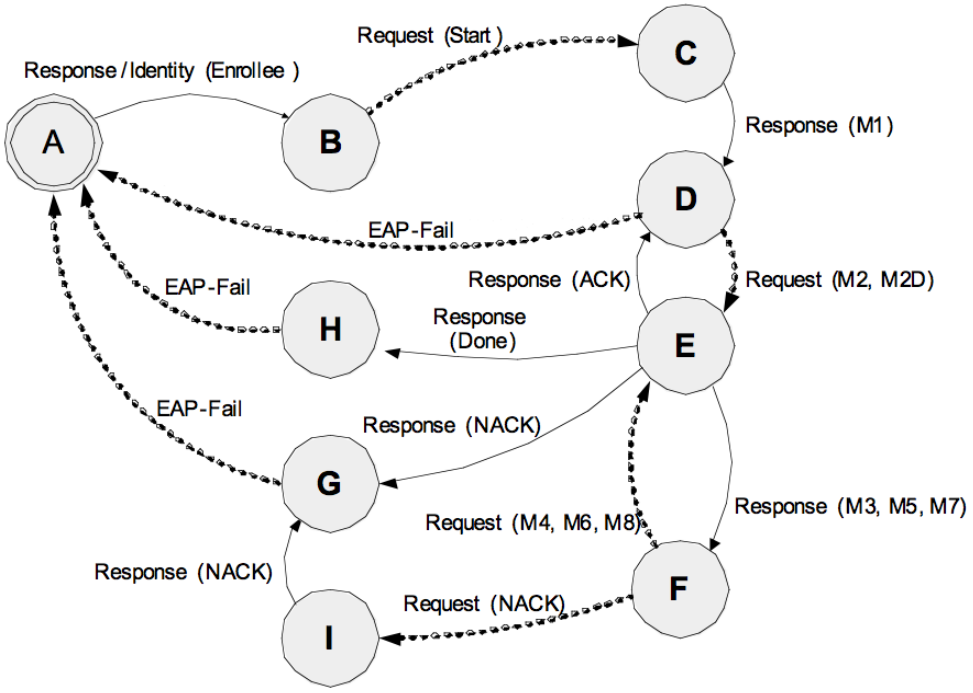
PIN girme yöntemi WPS için varsayılan yöntemdir. Yeni kaydedilecek (E) cihazda 4 veya 8 rakamdan oluşan PIN'in kaydedici (R) cihaza girilmesini gerektirir. Bu yöntemde PIN değeri, iki cihaz arasındaki Diffie-Hellman alışverişinin izinsiz girişlerden korunması amacıyla onaylama anahtarı olarak kullanılır. Rastgele oluşturulmuş 8 rakamlık PIN, 10^8 ($2^{26.65}$) farklı PIN değerine imkan sağlar. PIN protokolü PIN değerini 2 tane dört rakama bölerek kullanır. Eşleştirilecek iki cihaz PIN değerinin ilgili yarısını bilir ve tamamını doğrulamak için veri alışverişi yapar. İletişim esnasında araya girebilecek bir saldırgan (man-in-the-middle) PIN değerinin her iki yarısını da ayrı ayrı tahmin etmeye çalışabilir. Bu durumda saldırganın PIN değerini tespit etme ihtimali en az $2^{-14'}$ olarak hesaplanır. Deneme yanılma yoluyla PIN değerini elde etmeye çalışacak bir saldırgan olabileceğinden her işlemdeki PIN değeri sadece bir kez kullanılmalıdır. (Kuo vd., 2007)

WPS PIN yöntemine göre kayıt protokolünün işleyişi Şekil 3-2'de gösterilmiştir.



Şekil 3-2 WPS PIN yöntemi kayıt protokolü paket akışı (Wi-Fi Alliance, 2006)

WPS kayıt protokolü, mesajlarının telsiz ağ üzerinde aktarımı için 802.1x ve Extensible Authentication Protocol (EAP) protokollerini kullanır. 802.1x ve EAP, IEEE802.11i güvenlik eklentisinde de kullanılmış olup geliştirme ve güncellemelere açık bir güvenlik protokolü sağlar. EAP, ağa dahil olacak yeni kullanıcıların erişimine izin verme esnasında bir sonlu durum makinası kullanır. WPS kayıt protokolünde kullanılan EAP sonlu durum makinası Şekil 3-3'te gösterilmiştir. Buna göre işlemlerler başarısız olduğunda kullanıcı ağa dahil olamazken başarılı durumda ağa erişimine izin verilir.



Şekil 3-3 WPS kayıt protokolü sonlu durum makinası (Wi-Fi Alliance, 2006)

3.3. Düğmeyle Kurulum Senaryosu

Düğmeye basma yöntemi kullanıcı açısından en kolay kurulum seçeneğidir. Kullanıcı hem ağa kaydedici (R) cihazda hem yeni kaydedilecek (E) cihazda kurulum için ayarlanmış düğmeye basarak iki cihaz arasında "onaylanmamış Diffie-Hellman aktarımı" olarak tanımlanmış yönteme göre belirli bir süre aralığı için haberleşme başlatır.

WPS tanımlamasına göre düğmeyle kurulum yöntemi kolay olması yanında güvenli olma özelliğini de koruması için belirli şartlara göre çalışabilir. Bu bölümde düğmeyle kurulum senaryosu açıklanmıştır.

E cihazı üzerinde düğmeye basıldığında veya buna denk bir tetikleme gerçekleştiğinde cihaz düğmeyle kurulum modundaki bir R cihazı aramaya başlar. Arama işlemine, bir R bulunana kadar değil tüm telsiz ağ kanalları taranıp birden fazla R cihazın düğmeyle kurulum modunda olmadığından emin olunana kadar devam edilir. (Wi-Fi Alliance, 2006)

E, öncelikle etraftaki erişim noktalarını taramada kullanılan “Probe Request” paketlerini düğmeyle basma modunda olduğunu duyuracak şekilde gönderir. Etraftaki erişim noktaları (AP) cevap olarak Probe Response paketleri gönderirler. E, ilgili cevaplar içinde etkin R bilgisi olup olmadığına bakar. Tarama işleminde birden fazla R’ye rastlanırsa tüm işlem iptal edilip kullanıcı kayıt oturumu çakışması (session overlap) hakkında bilgilendirilmelidir. Böyle bir çakışma durumunda kullanıcı düğmeyle kurulum işlemini bir süre bekledikten sonra

yeniden denemesi veya PIN yönetimi kullanması için yönlendirilmelidir. Tarama işlemi sonunda tek bir R bulunduğundan emin olunduğunda E derhal kayıt protokolünü başlatabilir. (Wi-Fi Alliance, 2006)

R, üzerinde düğmeye basıldığında veya buna denk bir tetikleme gerçekleştiğinde öncelikle 120 saniye içerisinde birden fazla yeni kayıt isteği gelip gelmediğini kontrol eder. Bu süre aralığına izleme süresi (monitor time) veya yürüme süresi (walking time) adı verilir. İzleme süresi içerisinde birden fazla yeni kayıt isteği alınırsa R kullanıcıyı oturum çakışması hakkında bilgilendirip aşağıdaki şartların tamamı karşılanmadığı sürece yeniden düğmeyle kurulum işlemine başlanmasına izin vermemelidir:

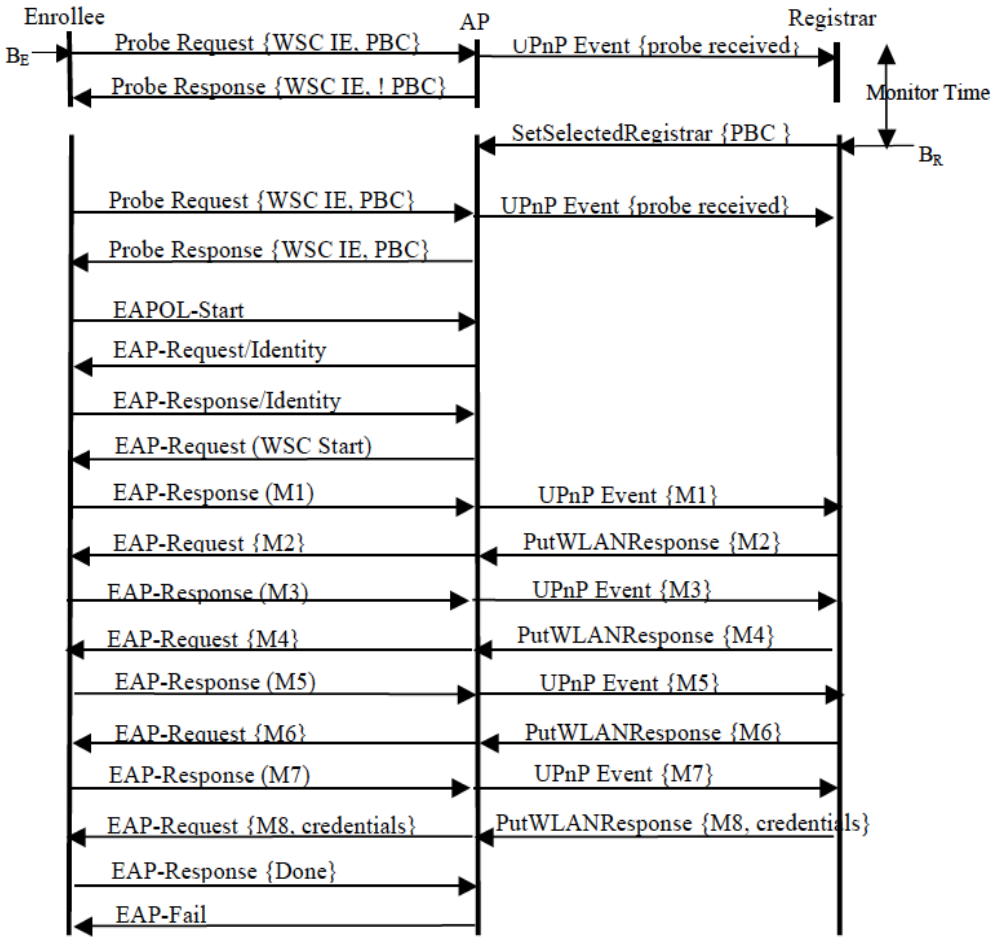
- kullanıcı, R'nin düğmesine yeniden basmıştır
- İzleme süresi içerisinde sadece bir kayıt isteği görülmüştür

R'nin çalışma süresi, izleme süresinden kısaysa (cihazın yeni çalıştırıldığı durum) izleme süresinin sonuna kadar beklemesine gerek olmaz.

R düğmeyle kurulumun başarıyla sonuçlanması durumunda, E'nin probe request bilgisini bir sonraki izleme süresi kontrolünden kaldırır. Bu sayede birden çok yeni cihazın 120 saniyelik gecikmeye ihtiyaç duymaksızın ardarda kaydedilmesi sağlanır. (Wi-Fi Alliance, 2006)

R ve E cihazları düğmeye basıldıktan sonra sadece izleme süresi kadar düğmeye basma modunda kalıp daha sonra düğme modundan çıkmalıdır. Düğmeye birden fazla basılmasına izin verilir. R veya E'de düğmeye yeniden basıldığında izleme süresi sayacı başa alınmış olur. (Wi-Fi Alliance, 2006)

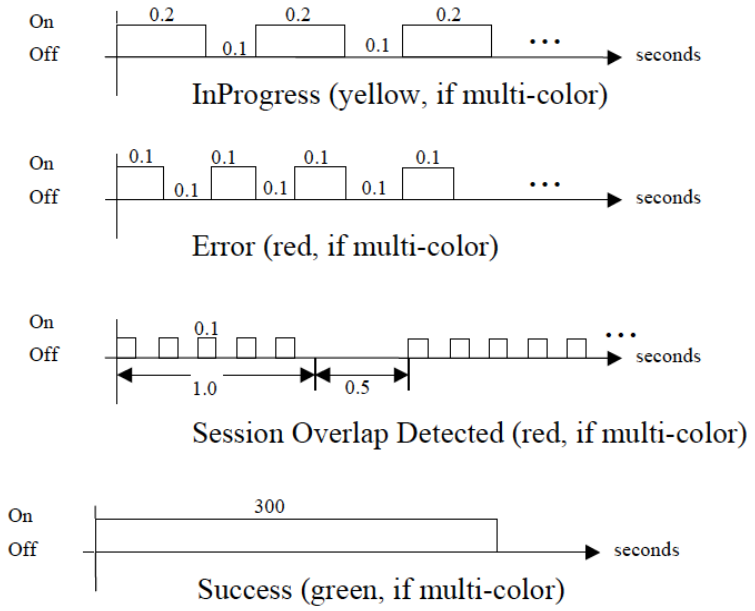
Şekil 3-4'te WPS kayıt protokolünün düğmeyle kurulum senaryosundaki işleyişi gösterilmiştir.



Şekil 3-4 WPS düğmeye basma yöntemi ile kurulum senaryosu paket akış diyagramı (Wi-Fi Alliance, 2006)

Düğmeyle kurulum, PIN girme ihtiyacını ortadan kaldırdığından özellikle tuş takımı ve kullanıcı ekranı olmayan cihazlar için tercih edilmektedir. Ne varki, düğmeye basma senaryosunun detaylarında açıklandığı üzere kullanıcıyı işlem durumu hakkında bilgilendirmek gerekir. Bu amaçla düğmeyle kurulum yapacak cihazların en azından bir durum ışığı ile kullanıcıyı hatalı ve başarılı kurulum hakkında bilgilendirmesi gerekir.

Düğmeyle kurulumda durum bilgisini sadece ışıkla bildirecek cihazların Şekil 3-5'te tanımlanan zamanlama ve mümkünse renkle sağlaması gerekir.



Şekil 3-5 WPS kullanıcı bilgilendirme ışıklarının kullanımı (Wi-Fi Alliance, 2006)

4. OTOMATİK AYAR DAĞITIM YÖNTEMİ

Bireysel kullanıcılar için telsiz bir ağın kurulumu ve yönetimi tek bir erişim noktası olan ağlar için bile karmaşıktır. Bu karmaşıklık özellikle kapsama alanını genişletmek için ihtiyaç duyulan örgü ağlarında daha da artmaktadır. Orijinal 802.11 standardına göre hizmet veren örgü ağı düğümlerinin örgü ağı olarak çalışabilmeleri için her birinin elle ayarlanması gerekir. Bu durum bu tip örgü ağlarının tamamı için ortak bir yönetim yöntemi ihtiyacı doğurur. Örneğin, örgü ağının telsiz ağ şifresinin değiştirilmesine ihtiyaç duyulduğunda tüm düğüm noktaları tek tek yeni şifre için ayarlanmalıdır. Bu ayarlamanın telsiz ağ üzerinden yapılması da pratikte uygun değildir çünkü yeni şifre ayarını uygulayan düğüm noktası bu şifreyi düğümler arasındaki haberleşmede de kullanıyorsa artık diğer düğümlerle olan haberleşmesini kaybetmiş olacaktır. Bu yüzden herhangi bir toplu yönetim özelliğine sahip olmayan örgü ağlarında tüm düğümlerin telli bağlantı kurularak ayarlanması gerekecektir. Oysa örgü ağındaki düğüm noktalarına ayar değişikliklerini otomatik dağıtacak bir yöntem kullanılırsa özellikle bireysel kullanıcıların bu ağları ayarlamasına imkan tanınmış olacaktır.

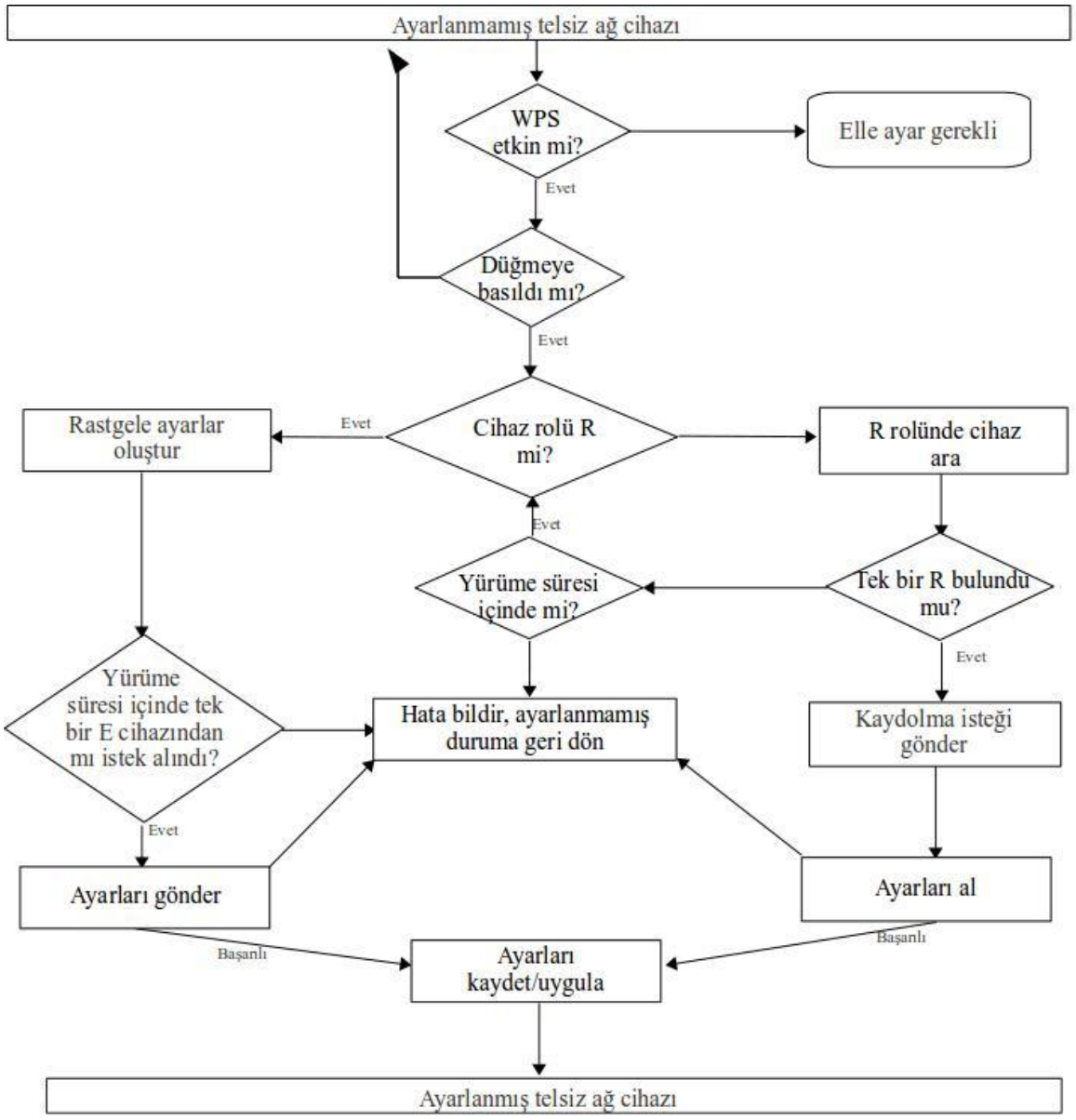
Bu tez çalışması kapsamında, Wi-Fi Allience tarafından tariflenen WPS PIN ve/veya düğmeye basma yöntemleri kullanılarak örgü ağını oluşturan düğüm noktaları için güvenli bir kurulum ve ayar alışverişi yöntemi tasarlanarak gerçeklenmiştir.

4.1. Kurulum Aşaması

İster sıradan bir telsiz ağ olsun ister telsiz bir örgü ağı olsun güvenli kurulum işleminin ilk aşaması bağlanılacak cihazın doğru tespit edilmesidir. Bugün itibariyle telsiz ağlarda belirli bir standarda bağlı tek cihaz eşleme yöntemi WPS'tir. [3]

WPS'te önerilen yöntemlerden birisi olan düğmeye basma yönteminin bireysel alanlar için kurulum kolaylığı ve gerekli güvenliği sağladığı öngörülmüştür. İlgili yöntem telsiz uç cihazlarını ağa dahil etmek için tasarlanmıştır. Oysa örgü ağı kurulumu için ağa, erişim noktası olarak hizmet verecek düğümlerin eklenmesi gerekmektedir. Bu çalışma kapsamında örgü ağı kurulumunun düğme ile yapılabilmesi için düğüm noktalarının birer uç cihaz gibi çalıştırılıp ağa tek tek eklenmesi öngörülmüştür..

Şekil 4-1'de fabrika ayarlarındaki bir telsiz cihazın düğmeyle kurulum yöntemi kullanılarak ayarlı duruma geçiş algoritması gösterilmiştir.



Şekil 4-1 Düğmeyle kurulum için kullanılan algoritma

WPS tanımlamasına göre eşlenecek cihazlardan birisinin kaydedici (R) diğerinin kaydolan cihaz (E) rolünü uygulaması gerekir. Mevcut kurulu bir örgü ağına yeni bir düğüm ekleme esnasında telsiz ağ ayarları yapılmış düğümün R, fabrika ayarlarındaki düğümlerinse varsayılan olarak her zaman E cihaz rolünde çalışmasıyla bu gereksinim karşılanacaktır. Ancak, fabrika ayarlarındaki iki düğüm noktası kullanılarak örgü ağının ilk kurulumu yapılmaya çalışıldığında her iki düğüm cihazı da E cihaz rolünü uygulayacağından kurulum işlemi gerçekleşmeyecektir. Böyle bir senaryoda kurulumun yapılabilmesi için düğümlerin kendi kendilerine rollerini tayin edebilmesi gerektiği anlaşılmıştır. Cihazların fabrika ayarlarında kendi kendilerine rol tayin edebilmeleri için aşağıda sıralanan adımları takip etmeleri önerilmiştir:

- Örgü ağını oluşturacak düğümlerden birinin DHCP [11] sunucusu cihazına telli bağlantı yapması ön koşulu getirilir

- Telli bağlantı yapılmış düğüm noktasının ağdaki DHCP sunucusundan dinamik IP adresi alması sağlanır

- Dinamik IP adresi alan cihaz kaydedici, fabrika ayarlarındaki diğer cihaz ise E rolü ile çalışmaya başlar

3. bölümde WPS PIN yönteminde açıklandığı üzere cihazlar arası güvenli ayar alışverişi her iki cihazın ortak bir PIN'i kullanmasıyla sağlanabilir. WPS tanımlaması farklı ihtiyaçlara göre farklı PIN değerlerinin tanımlanmasına izin verir. O halde düğüm noktalarının kurulumdan sonraki ayar değişikliklerini birbirlerine güvenli aktarması amacıyla özel bir "Ayar Dağıtım PIN" değeri (AD PIN) tanımlanıp ağa güvenli olarak dahil olan ve güvenilen telsiz cihazlarla paylaşılırsa bu amaca ulaşılabilir.

AD PIN değeri, örgü ağını oluşturan ilk düğüm tarafından rastgele seçilmelidir. Bu PIN değerine sahip olacak cihazların ağ ayarlarını değiştirme yetkisi olacağından PIN değerinin dağıtımının bilinçli yapılması gerekir. Kullanıcının tercih edeceği güvenlik seviyesine göre ya ağa dahil olma esnasında doğrudan her cihaza ya da sonradan bir kullanıcı arayüzü aracılığıyla sadece yetkilendirilen cihazlara AD PIN değerinin dağıtımı sağlanabilir.

WPS tanımlamasının güvenlik analizi bölümüne göre WPS PIN yönteminde kullanılacak PIN değerinin her işlem için farklı değer seçilmesi tavsiye edilir. Özellikle PIN hane sayısı az olursa deneme yanılma yoluyla PIN değerini tespit etmek kolay olacağından güvenlik zaafı doğacağı açıklanmıştır. PIN uzunluğu sıradan kullanıcıların kullanımını kolaylaştırırken güvenliği de belirli bir mertebede tutmak için varsayılan olarak 8 haneli bir sayı belirtilmiş olmasına rağmen daha uzun değerler seçilmesi de mümkündür. Tasarlanan yöntemde AD PIN değerinin sadece ilk kurulumda sabit bir değer olarak belirlenmesi kararlaştırıldığından bahsedilen güvenlik zaafından zarar görmemesi amacıyla 32 haneli bir sayı olmasına karar verilmiştir.

4.2. Otomatik Ayar Güncelleme Aşaması

WPS sayesinde telsiz ağ ayarlarını aktarmak kolaylaşmıştır ancak yine de kullanıcının ya fiziksel bir düğmeye basması ya da bir tuş takımıyla PIN girmesi gerekir. Oysa telsiz örgü ağında düğüm noktalarının çevrelerindeki ayar değişikliğini otomatik algılayıp kurulum aşamasında tanımlanan AD PIN değerini kullanarak ayar alışverişine başlamaları sağlanarak kullanıcının tek bir noktadan ağdaki tüm düğümleri ayarlaması mümkündür. Otomatik algılama işlemi, WPS verisinin yeni özellik eklemeye müsait yapısından faydalanarak,

düğümler üzerinde yeni parametreler tanımlayıp bunların algılanan tüm WPS verilerinde takip edilmesiyle sağlanabilir. Böyle bir uygulama için en azından şu iki parametrenin tanımlanması ve takip edilmesi gerekecektir:

Evrensel Örgü Ağı Tanımlayıcı Kodu (M-UUID): Oluşturulan her örgü ağının ve ilgili ağın ayar kümesinin evrensel olarak tekilliğini ifade edecek koddur. Ağı oluşturan ilk düğüm tarafından rastgele seçilmeli ve WPS verisi içerisinde sürekli yayınlanmalıdır.

Ayar Sıra Numarası (ASN): Örgü ağının o an etkin olan ayar kümesinin sıra numarasını temsil eder. Örgü ağının ilk kurulumda belirli bir sayıdan başlayıp her ayar değişikliğinde arttırılmalıdır. Aynı esnada birden fazla cihazda ayar değişikliği yapıldığı durumda örgü ağının farklı bölümlerinde aynı sıra numarasına sahip ancak farklı ayarlara sahip cihazların oluşması problemini aşmak amacıyla ASN değerinin düğüm sayısına göre belirli bir aralık içerisinde rastgele oranda arttırılması gerekir. Bu sayede düğümlerin zaman içerisinde yeniden ortak bir ayar kümesinde çalışması sağlanır.

Bu parametreler tanımlandıktan sonra ayar güncelleme işlemi şu şekilde tetiklenir:

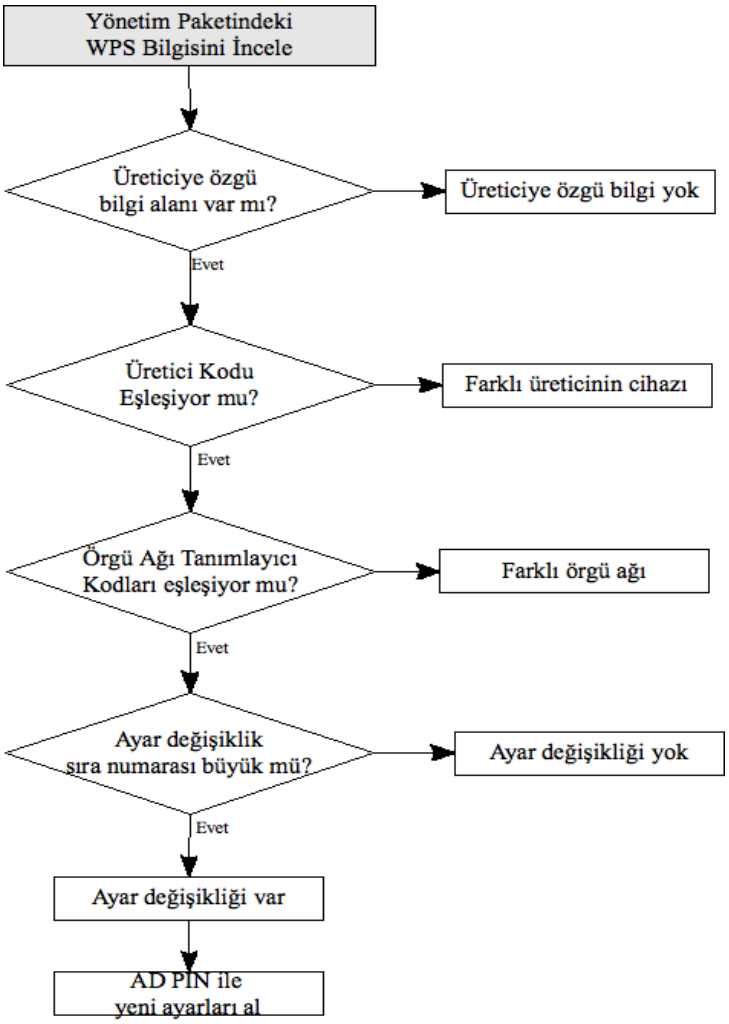
- Düğüm noktaları M-UUID ve ASN değerlerini tüm cihazların algıladığı yönetim paketlerinde etrafa yayar.

- Herhangi bir düğüm noktası etrafındaki kendi örgü ağına dahil bir düğüm noktasında aşağıdaki koşullar sağlandığında AD PIN kullanılarak WPS ayar aktarım işlemi başlatır:

    - M-UUID'leri eşleşiyor
    - Kendi ASN değeri algıladığı düğümdeki ASN değerinden küçük

Bu yöntemde ilgili parametrelerin etraftaki düğüm noktalarına dağıtılması için sadece beacon [1] paketlerinin kullanılması önerilmiştir. Günümüzde kullanılan çoğu telsiz ağ yongası beacon paketlerini sadece çalıştıkları etkin kanalda yaymaktadır. Bu durum bu cihazlar için kanal değişikliği durumunda ayar değişikliğini tetikleyici mekanizmanın ortadan kalkmasına sebep olur. Bu problemi aşmak amacıyla ayar değişikliği durumunda düğüm noktası yeni ayarlarla çalışmaya başlamadan önce tanımlı tüm kanallarda yeni ASN değerini yayacak şekilde kısa süreliğine çalıştırılmalıdır. Pratikte bu işlem telsiz ağların taranmasında kullanılan probe request [1] paketlerinin tüm kanallara gönderilmesiyle sağlanabilir.

Açıklanan yöntemin algoritması Şekil 4-2'de gösterilmiştir.



Şekil 4-2 Tasarlanan otomatik ayar güncelleme algoritması

5. YÖNTEMİN GERÇEKLENMESİ

Bu tez kapsamında tasarlanan yöntemin aynı zamanda 802.11b/g/n protokolüne göre çalışan sıradan telsiz erişim noktaları üzerinde gerçeklenmesi amaçlanmıştır. Yöntem tasarımının tamamlanmasının ardından ilgili çalışmanın gerçeklenmesine örnek olarak AirTies Air6271 ve Air5450 model numaralı telsiz ağ yönlendiricileri ile Air4450 ve Air4240 erişim noktası cihazları seçilmiştir. İlgili cihazların yazılım ve donanım özellikleri Çizelge 5-1'de özetlenmiştir. Tüm bu cihazlarda WPS düğme yöntemi için kullanılacak özel bir düğme ve durum bilgisi bildirimi için bir ışık mevcuttur.

Çizelge 5-1 Tasarlanan yöntemin gerçeklendiği cihazların donanım ve yazılım özellikleri

Cihaz Modeli:	İşletim Sistemi:	Telsiz ağ yongası:	Telsiz ağ özellikleri
AirTies Air6271	Linux 2.6.20	Atheros AR2417	2.4 Ghz, 802.11 b / g
AirTies Air5450	Linux 2.6.20	Broadcom BCM4322	2.4/5 Ghz, 802.11 b / g / n
AirTies Air4240	Linux 2.4.25	Atheros AR2317	2.4 Ghz, 802.11 b/g
AirTies Air4450	Linux 2.6.15	Atheros 9102	2.4 Ghz, 802.11 b / g / n

Yukarıdaki tablodan görüleceği üzere örnek olarak kullanılan 4 cihazda da Linux işletimi kullanılmaktadır. Linux açık kaynak kodlu popüler bir işletim sistemidir. Öncelikle masaüstü sistemler için geliştirilmiş olsa da günümüzde sunucu olarak yaygın olarak kullanılmakta ve gömülü ortam uygulamalarındaki kullanımı da gitgite artmaktadır. [Zhu ve Chen, 2009) Ayrıca WPS uygulamaları öncelikle Linux işletim sistemi için geliştirilmiştir. [12] Bu sebeplerle bu tez kapsamında da cihazlar üzerinde hali hazırda bulunan Linux işletim sistemi üzerinde yazılım geliştirilmeye devam edilmiştir.

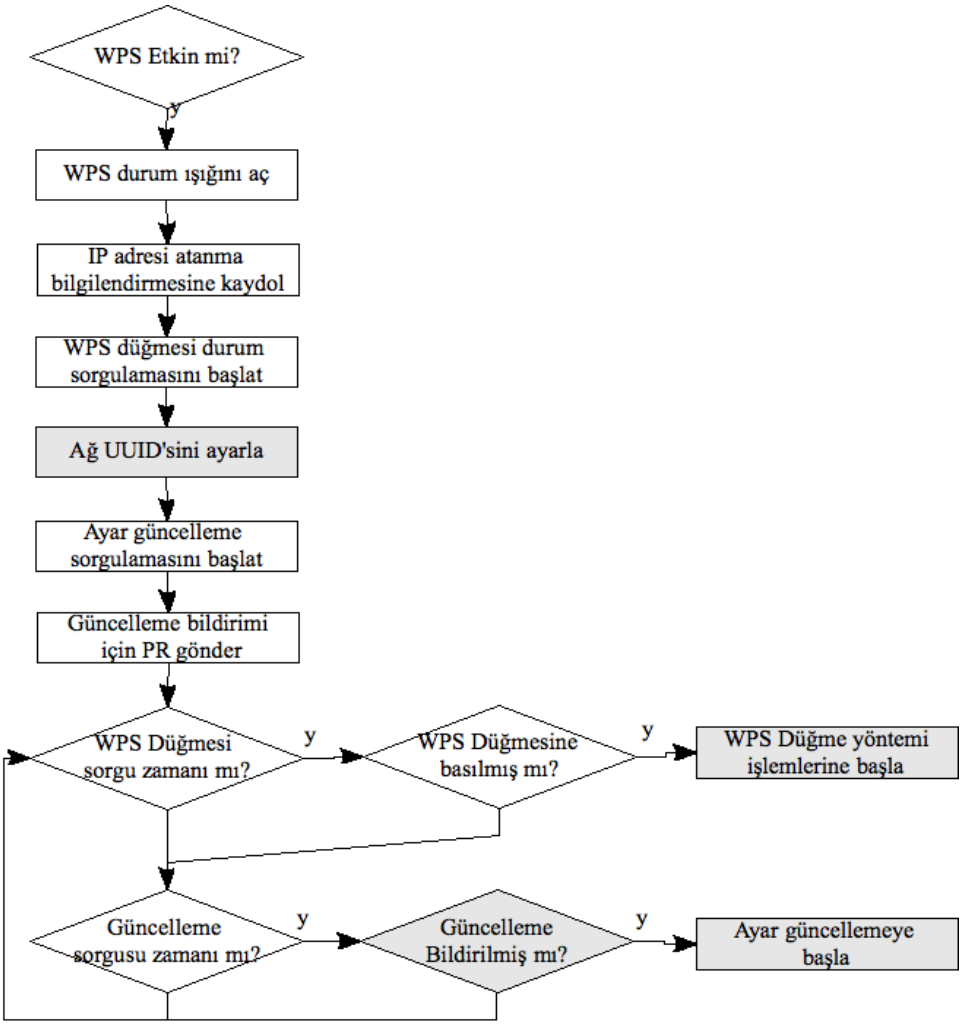
Linux işletim sisteminin 2.6.22 sürümünden itibaren telsiz ağ yongalarını ortak olarak destekleyecek mac80211 adında bir donanım sürücüsü katmanı geliştirme çabası sürdürülmektedir. Bu çalışmanın öncelikli amacı ilgili yongaları kullanan telsiz ağ uç cihazları için sürücü desteği sağlamak olsa da aynı zamanda belirli yongalar için erişim noktası ve örgü ağı düğümü özelliklerini destekleyebilecek seviyeye ulaşılmıştır. 2010 yılı Mart ayı itibariyle bu çalışma kapsamında üzerinde çalışma yürütülen telsiz ağ yongaları ve ilgili yongalarının uç cihazı özelliği yanında hangi telsiz ağ özelliklerini desteklediği EK-1'deki tabloda listelenmiştir. [13]

Linux işletim sistemini kullanan bir bilgisayar sisteminin telsiz ağ erişim noktası olarak hizmet verebilmesi için erişim noktası ayar yönetimi, şifreleme ve kullanıcı doğrulama gibi

amaçlarla kullanıcı seviyesi uygulamalar kullanılmaktadır. Mac80211 sürücü katmanı, erişim noktası yönetim uygulaması olarak *hostapd* [14] uygulamasının kullanımını gerektirir. [15] Bu sayede farklı üreticilerin telsiz ağ yongaları için ortak bir telsiz ağ erişim noktası yönetim uygulaması kullanmak da mümkün hale gelmektedir. Diğer bir deyişle erişim noktası özelliği donanımdan bağımsız hale gelmektedir.

Açık kaynak kodlu bir erişim noktası yönetim uygulaması olan *hostapd* 2004 yılından bu yana çoklu donanım desteğine sahip bir uygulama olarak geliştirilmekte ve kendi çalışma alanında 802.11 standardına yapılan eklemeleri de güncel olarak takip etmeye çalışmaktadır. WPS özelliği de bu uygulamanın 0.6.7 sürümünden itibaren eklenmeye başlamıştır. Bu tez kapsamında ihtiyaç duyulan WPS PIN ve düğme yöntemleri bu uygulama sayesinde kullanılmaktadır.

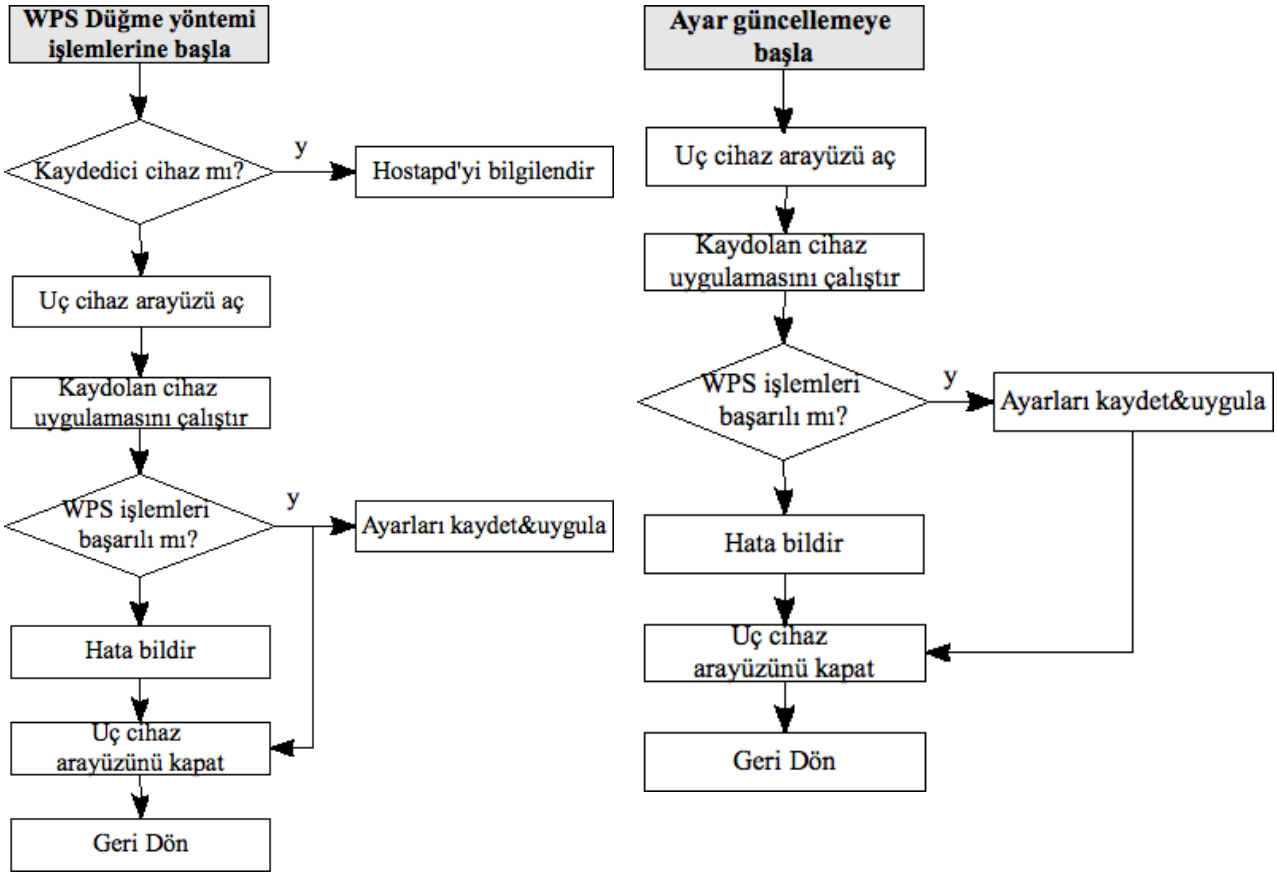
Geliştirilen yöntemin donanımdan bağımsız olması amaçlanmış ve bu sebeple geliştirme özellikle *hostapd* uygulamasının kullanıcı seviyesinde çalışan bölümünde yapılmıştır. Ayrıca düğmeye basma, sonuç bildirim ışığı yakma gibi giriş ve çıkış işlemlerinin örnek donanımlarda çalışabilmesi kullanıcı seviyesinde çalışan bir WPS yönetim uygulaması geliştirilmiştir. Bu uygulama aynı zamanda tasarlanan yöntemin içerdiği algoritmaların uygulanmasından sorumludur. Şekil 5-1'de gerçeklenen kullanıcı seviyesi uygulamasının algoritması genel hatları ile gösterilmiştir.



Şekil 5-1 Geliştirilen kullanıcı seviyesi uygulamanın algoritması

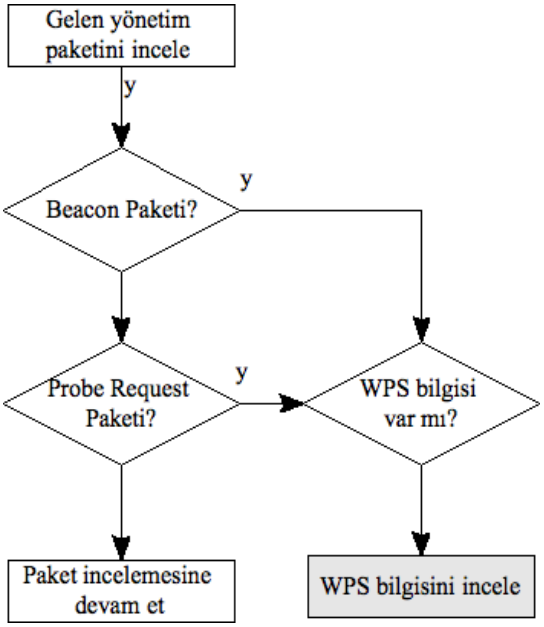
WPS yönetim uygulaması mevcut donanım ve yazılım sistemi ile *hostapd* uygulaması arasında aracılık yapmaktadır.

Şekil 5-2'de WPS yönetim uygulaması ile *hostapd* uygulamaları arasındaki iletişim genel hatları ile gösterilmiştir.

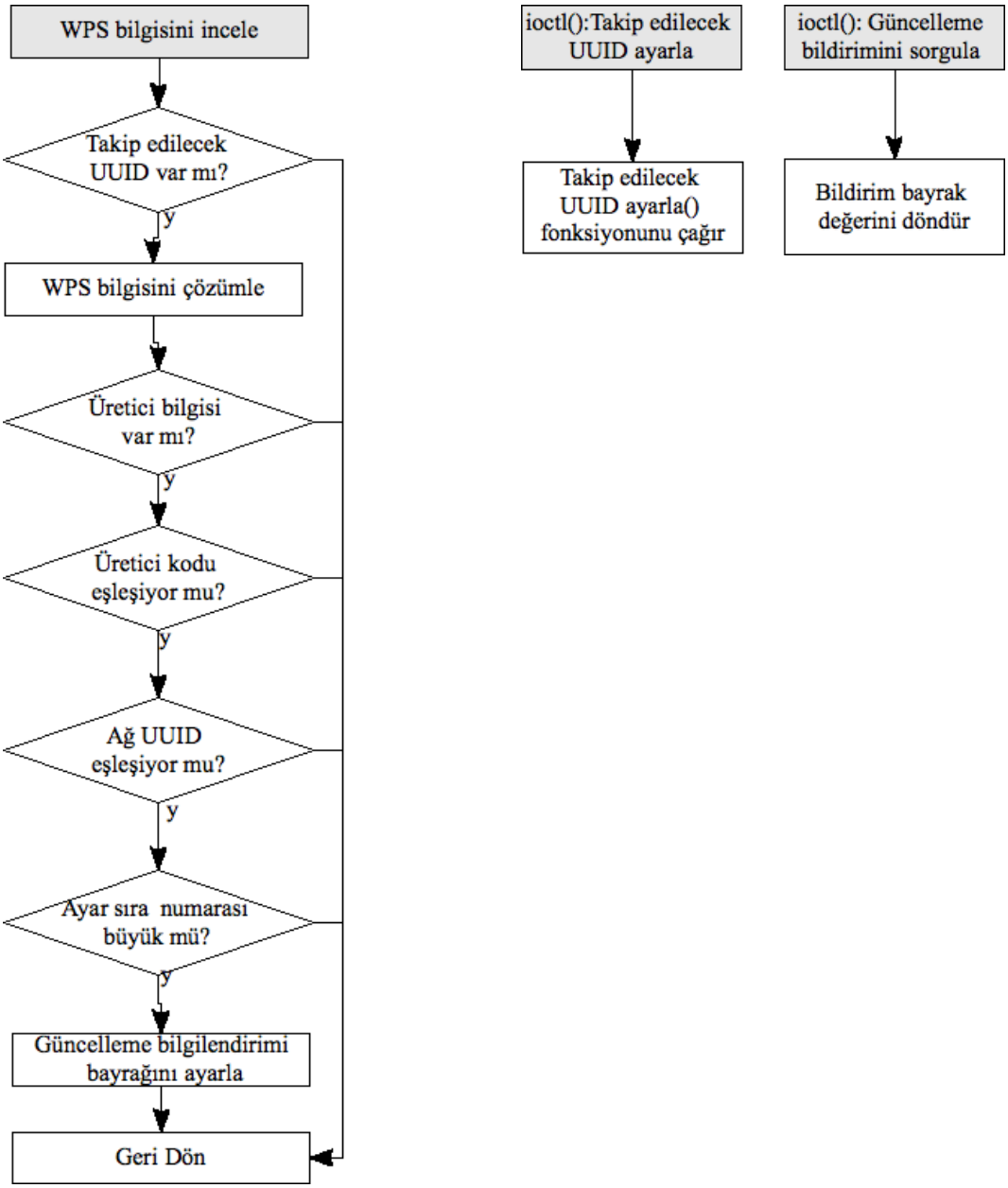


Şekil 5-2 Düğmeye basıldığında veya ayar güncellemesi durumunda ayar aktarımı

WPS işlemlerinin mevcut telsiz ağ donanım sürücüsünde çalışabilmesi için sürücüde paket filtreleme ve inceleme özelliklerine ihtiyaç duyulur. Bu özellikler örnek olarak kullanılan sürücülerde bulunmadığından algılanan yönetim paketlerinin incelendiği fonksiyonda Şekil 5-3'te gösterilen değişikliğe ihtiyaç duyulmuştur. Bu değişiklik sayesinde WPS yönetim uygulaması Şekil 5-4'te gösterilen ek fonksiyonları kullanarak kullanıcı seviyesinden sürücü seviyesindeki gerekli bilgilere erişip tasarlanan yöntemin çalışmasını sağlar.



Şekil 5-3 Sürücü koduna yapılan değişikliğin algoritması



Şekil 5-4 Sürücü koduna eklenen algoritma

Geliştirilen yönteme göre çalışan iki tane Air6271 ve bir tane Air4240'ın kullanıldığı örnek örgü ağı Şekil 5-5'te gösterilmiştir. Bu sistem üzerinde aşağıdaki adımlar izlenerek geliştirilen yöntem test edilmiştir:

- Tüm cihazlar fabrika ayarlarına alınır
- WPS durum ışığının hazır durumunu gösterdiği kontrol edilir
- Cihazlardan sadece biri DHCP sunucusuna erişimi olan ağa kablo ile bağlanır, bu cihaz WPS tanımlamasına göre R rolünde çalışacaktır
- Herhangi bir ağa bağlantısı olmayan cihazlardan birinde kurulum için ayarlanmış düğmeye basılır, bu cihaz WPS tanımlamasına göre E rolünde çalışacaktır
- Aynı anda ortamda ikinci bir kaydolan cihazın düğmesine basılmadıysa R cihazı E cihazına telsiz ağ ayarlarını gönderir

- WPS işlemleri başarıyla tamamlanırsa her iki cihaz R cihazında tanımlı ayarlara göre ve birbirleri arasında telsiz dağıtım sistemi bağlantısı tanımlı halde çalışmaya başlar. Telsiz dağıtım sistemi sayesinde iki erişim noktası arasında veri alışverişi yapılabilir.
- WPS işlemlerinde hata olması durumunda kullanıcı durum bildirim ışığıyla bilgilendirilir.
- Örgü ağına erişim noktası ekleme işlemine örgü ağının üyesi olan herhangi bir erişim noktasında düğmeye basarak ilgili cihazı R, fabrika ayarlarındaki bir erişim noktasında düğmeye basarak da ilgili cihazı E rolünde çalıştırmak suretiyle devam edilebilir
- Örgü ağına üye cihazlardan herhangi birisinin telsiz ağ ayarlarında değişiklik yapıldığında geri kalan erişim noktalarının WPS PIN yöntemi tetiklenerek ayar değişikliğini kendilerine aktarması beklenir

Şekil 5-5 Geliştirilen yöntemi kullanan örnek cihazlar

Geliştirilen yöntem telsiz ağa erişim noktası ekleyerek telsiz örgü ağı kurulmasına imkan tanımasının yanı sıra telsiz bir uç cihazın telsiz ağa dahil edilmesi ve ayarlarının otomatik güncellenmesi için de kullanılabilir. Örneğin telsiz bir IPTV alıcısı, üzerindeki kurulum düğmesine basılarak telsiz ağa kolayca dahil edilebilir. Ayrıca bu telsiz ağdaki ayar değişikliklerinden otomatik olarak haberdar olup ayarlarını güncelleyebilir.

6. SONUÇ

Telsiz örgü ağları, dağıtık erişim noktalarından meydana geldikleri için telsiz ağ ayarları ve şifrelerinin dağıtımı ve güncellenmesi için bir yönetim sistemine ihtiyaç duyulur. Bu tez çalışması kapsamında telsiz örgü ağının tüm üyelerinde telsiz ağ ayarlarının ve şifrelerinin güncellenmesini sağlayacak bir yöntem tasarlanarak gerçeklenmiştir. Ayrıca, bu yöntem veri alış verişinde bireysel kullanım alanlarında güvenli kurulum için tanımlanmış olan WPS tanımlamasını temel aldığı için güncelleme işlemlerinin güvenliğini sağlar. Mevcut bir tanımlamayı kullanmak üreticiler arası uyumluluk açısından da fayda sağladığından bu yöntemin bu tanımlamayı destekleyen farklı donanıma sahip erişim noktalarına uygulanması kolaylaşmaktadır. Bu tez çalışması kapsamında geliştirilen yöntem bu sayede farklı üreticilerin farklı özellikleri destekleyen telsiz ağ yongalarını kullanan erişim noktalarında gerçeklenebilmiştir.

Geliştirilen yöntem, sıradan bir bilgisayar kullanıcısın bile fabrika ayarlarındaki erişim noktaları üzerinde kurulum düğmelerine basmak suretiyle güvenli bir örgü ağı kurarak telsiz ağ kapsama alanını genişletmesine olanak sağlar. Ayrıca telsiz ağ ayarları ile ilgili bir değişikliğe ihtiyaç duyulduğunda kullanıcının örgü ağını oluşturan cihazlardan herhangi birinin yönetim arayüzünden bu değişikliği yapması yeterlidir. Yapılan değişiklik örgü ağının diğer üyelerine telsiz ağ üzerinden güvenli ve otomatik olarak aktarılıp örgü ağı yeni ayarlarıyla çalışmaya başlar. Geliştirilen yöntem telsiz örgü ağını oluşturan erişim noktalarının ayar aktarımı esnasında telsiz uç cihaz olarak çalışması ilkesine dayanır. Bu yüzden ilgili yöntem aslında tüm telsiz ağ uç cihazlarının telsiz ağa dahil edilmesi ve ayarlarının dağıtık olarak yönetimi için de kullanılabilir.

Her ne kadar geliştirilen yöntem telsiz örgü ağına erişim noktası eklemeyi kolaylaştırsa da pratikte telsiz örgü ağına eklenebilecek erişim noktalarının sayısı önceden planlanmalıdır. Sadece tek kanalda çalışma özelliğine sahip erişim noktalarının kullanıldığı telsiz örgü ağlarında iletişim ortamı tüm erişim noktaları ve bunların oluşturduğu kapsama alanındaki uç cihazlar tarafından paylaşılır. Bu sebeple uygulama alanı ve ihtiyaç duyalan veri akış hızına göre örgü ağına ancak belirli sayıda erişim noktası eklenebilir. Örnek olarak, yöntemin gerçeklendiği örnek cihazların kullanıldığı yüksek çözünürlüklü vidyo aktarımı uygulamasında en çok üç, metin içerikli internet sayfalarının aktarımı uygulamasında ise en çok on erişim noktasından oluşan telsiz örgü ağının verimli olduğu görülmüştür.

Gerçekleştirilen tez çalışmasında örgü ağını oluşturan düğümler arasında yönlendirme bilgisi sabit olarak tanımlanmaktadır. Ek çalışma olarak dinamik bir yönlendirme algoritması

tasarlanarak bu yöntemden faydalanan ve kendi kendisini onarabilen bir örgü ağı oluşturulabilir. Diğer yandan otomatik ayar güncellemede kullanılan AD PIN değeri sabit bir değer olarak tasarlandığından bu değerin güvenilmeyen kişilerce tespit edilmesi durumunda ağın güvenliği ortadan kalkabilmektedir. AD PIN değerinin dağıtımı ve güncellenmesi için güvenli bir yönetim sistemi geliştirmek güvenlik seviyesini arttıracaktır.

KAYNAKLAR

Camp, J. D., ve Knightly, E. W. (2008), "The IEEE 802.11s Extended Service Set Mesh Networking Standard", IEEE Communications Magazine, 46(8):120-126

Chandra, P., (2005), "Bulletproof Wireless Security", Elsevier Inc., Newnes, Oxford

Glass, S., Portmann, M. ve Muthukkumarasamy, V., (2008), "Securing Wireless Mesh Networks", IEEE Internet Computing, 12(4):30-36

Gürkaş, G. Z., (2005), "Kablosuz Güvenlik Protokollerinin Karşılaştırmalı Analizi", İstanbul Üniversitesi Fen Bilimleri Enstitüsü (Yayınlanmamış)

Hiertz, G. R., Max, S., Weiß,E., Berleman, L., Denteener, D. ve Mangold, S., (2006), "Mesh Technology enabling Ubiquitous Wireless Networks", The 2nd Annual Int'l Wireless Internet Conference(WICON,'06), 2-5.Ağustos.2006, Boston, MA, ABD

Hiertz, G. R., Denteener, D., Max, S., Taori, R., Cardona, J., Berleman, L., ve Walke, B., (2010), "IEEE 802.11s: The Wlan Mesh Standard", IEEE Wireless Communications, 17(1):104-111

Hottell, M., Carter, D. ve Deniszczuk, M., (2006), "Predictors of home-based wireless security", 5th Workshop on Economics of Information Security, 26-28.Haziran.2006, Cambridge, İngiltere

Köksal, A. S., (2007), "802.11 Kablosuz Yerel Alan Ağlarında Güvenlik Sorunu", Sakarya Üniversitesi Fen Bilimleri Enstitüsü (Yayınlanmamış)

Kuo, C., Walker, J. ve Perrig, A., (2007), "Low-cost Manufacturing, Usability, and Security: An Analysis of Bluetooth Simple Pairing and Wi-Fi Protected Setup", Usable Security (USEC), 15-16.Şubat.2007, Scarborough, Trinidad-Tobago

Lehembre, G., (2005), "Wi-Fi security – WEP, WPA and WPA2", Hakin9, 2005(6):2-15

Ritz, J.A., (2003), "Introduction to the 802.11 Wireless Network Standard", CyberScience Laboratory, Rome

Wi-Fi Alliance, (2006), "Wi-Fi Protected Setup Specification", Wi-Fi Alliance

Zhu, F. ve Chen, H., (2009), "μCLinux-based WEBSERVER Realization on ARM platform", 2009 ISECS International Colloquium on Computing, Communication, Control, and Management, 08-09.Ağustos.2009, Sanya, Çin

İNTERNET KAYNAKLARI

[1] ANSI/IEEE Std 802.11, 1999 Edition,

standards.ieee.org/reading/ieee/std_public/new_desc/lanman/restricted/802.11-1999.html

[2] en.wikipedia.org/wiki/IEEE_802.11

[3] www.wi-fi.org

[4] en.wikipedia.org/wiki/Wi-Fi_Protected_Access

[5] en.wikipedia.org/wiki/IEEE_802.11i-2004

[6] www.broadcom.com/products/secureeasysetup.php

[7] Braskich, T., "A vendor specific plan for centralized security", mentor.ieee.org/802.11/file/09/11-09-0114-01-000s-a-vendor-specific-plan-for-centralized-security.ppt

[8] Fleishman, G., "Under the Hood with Broadcom SecureEasySetup", wifinetnews.com/archives/2005/01/under_the_hood_with_broadcom_secureeasysetup.html

[9] https://www.wi-fi.org/files/kc/20090123_Wi-Fi__Protected_Setup.pdf

[10] www.upnp.org

[11] tools.ietf.org/html/rfc2131

[12] software.intel.com/en-us/articles/wsc-linux-reference-implementation

[13] linuxwireless.org

[14] hostap.epitest.fi/hostapd

[15] linuxwireless.org/en/users/Documentation/modes#AP

EKLER

EK 1 WPS Kayıt Protokolü Paket İçerikleri

Enrollee → Registrar: M_1 = Version || N1 || Description || PK_E

Enrollee ← Registrar: M_2 = Version || N1 || N2 || Description || PK_R [|| ConfigData] || $HMAC_{AuthKey}(M_1 || M_2^*)$

Enrollee → Registrar: M_3 = Version || N2 || E-Hash1 || E-Hash2 || $HMAC_{AuthKey}(M_2 || M_3^*)$

Enrollee ← Registrar: M_4 = Version || N1 || R-Hash1 || R-Hash2 || $ENC_{KeyWrapKey}$(R-S1) || $HMAC_{AuthKey}$ ($M_3 || M_4^*$)

Enrollee → Registrar: M_5 = Version || N2 || $ENC_{KeyWrapKey}$(E-S1) || $HMAC_{AuthKey}$ ($M_4 || M_5^*$)

Enrollee ← Registrar: M_6 = Version || N1 || $ENC_{KeyWrapKey}$(R-S2) || $HMAC_{AuthKey}$ ($M_5 || M_6^*$)

Enrollee → Registrar: M_7 = Version || N2|| $ENC_{KeyWrapKey}$(E-S2 [||ConfigData]) || $HMAC_{AuthKey}$ ($M_6 || M_7^*$)

Enrollee ← Registrar: M_8 = Version || N1 || [$ENC_{KeyWrapKey}$(ConfigData)] || $HMAC_{AuthKey}$ ($M_7 || M_8^*$)

|| : paketi oluşturan parametrelerin ardarda eklendiğini ifade eder.

Altsimge : kriptogragrafik bir fonksiyon adıyla yer aldığında o fonksiyonda kullanılan parametreyi ifade ederler. Ör: HMAC fonksiyonunun anahtarı için HMACKey.

Mn* : Mn'in HMAC-SHA-256 kısmı hariç değeri

Version : Kayıt protokolü mesajının sürüm numarası

N1 : Kaydolan cihaz(E) tarafından tanımlanmış 128-bit'lik rastgele bir sayı

N2 : Kaydedici cihaz(R) tarafından tanımlanmış 128-bit'lik rastgele bir sayı

Description : Cihaz bilgisi(UUID, üretici adı, model numarası, MAC adresi, vb.) ve cihazın telsiz ağ özellikleri.

PKE ve PKR : E ve R cihazın Diffie-Hellman paylaşılan anahtarları

AuthKey : Diffie-Hellman şifresi gAB mod p, N1, N2 ve E'nin MAC adresinden türetilmiş kimlik doğrulama anahtarı

E-Hash1, E-Hash2 : E'nin kendi cihaz şifresinin her iki yarısını bildiğini ispatlamak için kullanacağı değerler

R-Hash1, R-Hash2 : R'nin kendi cihaz şifresinin her iki yarısını bildiğini ispatlamak için kullanacağı değerler

ENCKeyWrapKey(...) : Parantez içindeki değerlerin KeyWrapKey değeri kullanılarak simetrik kodlanması. Kullanılan kodlama algoritması: AES-CBC(FIPS 197), PKCS#5 v2.0.

R-S1, R-S2 : E'nin, R'nin cihaz şifresinin her iki yarısını doğru bildiğini onaylamak için R-Hash1 ve R-Hash2 ile beraber kullandığı 128-bit'lik rastegele değerlerden oluşan şifreler

E-S1, E-S2 : R'nin, E'nin cihaz şifresinin her iki yarısını doğru bildiğini onaylamak için E-Hash1 ve E-Hash2 ile beraber kullandığı 128-bit'lik rastegele değerlerden oluşan şifreler

HMACAuthKey(...) : Parantez içindeki değer üzerinde AuthKey anahtarı ile uygulanmış HMAC fonksiyonunun değeri ile elde edilen bir kimlik belirleyici özelliği ifade eder. Hash fonksiyonunun tipi: HMAC-SHA-256 per FIPS 180-2 ve RFC-2104.

ConfigData : E'nin kullanımı için paylaşılan telsiz ağ ayarları ve şifreleri paketi. Bu paket ihtiyaca göre ek ayarların aktarılması için de kullanılabilir. Veri şifreler için şifreli gönderilir ancak diğer ayarlar için şifresiz de gönderilmesi mümkündür

[Wi-Fi Alliance, 2006]

EK 2 Telsiz Ağ Yongalarının Linux Sürücü Desteği Listesi

Çizelge 6-1 Telsiz Ağ Yongalarının Linux Sürücü Desteği Listesi [13]

Sürücü Adı	Üretici Adı	Ortak Sürücü	Erişim Noktası	Örgü Ağı	Protokol
acx1xx	Texas Instruments	+	?	-	B
adm8211	ADMtek/Infineon	+	-	-	B
agnx	Airgo/Qualcom	+	?	?	A/B/G
airo	Aironet/Cisco	-	?	?	B
ar9170usb	ZyDAS/Atheros	+	-	-	A/B/G/N
ar9271	Atheros	-	?	?	B/G/N
at76c50x-usb	Atmel	+	-	-	B
ath5k	Atheros	+	+	+	A/B/G
ath9k	Atheros	+	+	+	A/B/G/N
ath9k_htc	Atheros	+	-	-	B/G/N
atmel	Atmel	-	?	?	B
b43	Broadcom	+	+	+	A/B/G
b43legacy	Broadcom	+	+	+	A/B/G
hostap	Intersil/Conexant	-	?	?	B
ipw2100	Intel	-	-	-	B
ipw2200	Intel	-	-	-	A/B/G
iwl3945	Intel	+	-	-	A/B/G
iwlagn	Intel	+	-	-	A/B/G/N
iwmc3200wifi	Intel	+	-	-	A/G
mwl8k	Marvell	+	?	?	A/B/G/N
libertas	Marvell	-	-	+	B/G
libertas_tf	Marvell	+	+	+	B/G
orinoco	Agere/Intersil/Symbol	+	-	-	B
p54pci	Intersil/Conexant	+	+	+	A/B/G
p54spi	Conexant/ST-NXP	+	+	+	A/B/G
p54usb	Intersil/Conexant	+	+	+	A/B/G
poldhu	NWN	-	?	?	B
prism2_usb	Intersil/Conexant	-	?	?	B
rndis_wlan	Broadcom	+	-	-	B/G
rt61pci	Ralink	+	+	-	A/B/G
rt73usb	Ralink	+	-	-	A/B/G
rt2400pci	Ralink	+	+	-	B
rt2500pci	Ralink	+	+	-	A/B/G
rt2500usb	Ralink	+	+	-	A/B/G
rt2800pci	Ralink	+	?	?	A/B/G/N

rt2800usb	Ralink	+	?	?	A/B/G/N
rtl8180	Realtek	+	-	-	B/G
rtl8187	Realtek	+	-	-	B/G
rtl8187se	Realtek	+	-	-	B/G
r8192_pci	Realtek	-	?	?	B/G/N
r8192s_usb	Realtek	-	?	?	B/G/N
r8192u_usb	Realtek	-	?	?	B/G/N
vt6655	VIA	-	?	?	A/B/G
vt6656	VIA	-	?	?	A/B/G
winbond	Winbond	+	?	?	B
wl1251	Texas Instruments	+	?	?	B/G
wl1271	Texas Instruments	+	?	?	B/G/N
wlags49_h2	Lucent/Agere	-	?	?	B/G
zd1201	ZyDAS/Atheros	-	?	?	B
zd1211rw	ZyDAS/Atheros	+	-	+	A/B/G

ÖZGEÇMİŞ

Doğum tarihi	12.09.1983	
Doğum yeri	Şumnu/Bulgaristan	
Lise	1998-2001	Edirne Fen Lisesi, A. Rıfat Canayakın Lisesi(YDA)
Lisans	2001-2005	İstanbul Teknik Üniversitesi Elektrik-Elektronik Mühendisliği Fakültesi Kontrol Mühendisliği Bölümü
Yüksek Lisans	2006-2010	Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı

Çalıştığı kurum(lar)

2005-2009	AirTies Kablosuz İletişim A.Ş., İstanbul/Türkiye
2010-Devam ediyor	AirTies, Inc., Kaliforniya, ABD