Ankara İli Kablosuz Ağ Cihazı Erişim Güvenliği ve Toplumsal Farkındalık Analizi

Uraz Yavanoğlu[a,1], Ahmet Kapkiç[a,2], S. Tuna Yağcı[a,3], Cemal Aktepe[a,4], Gizem Tunçer[a,5]
[a] Gazi Üniversitesi, Bilgisayar Mühendisliği Bölümü, Maltepe 06570, Ankara
[1] uraz@gazi.edu.tr [2] ahmetkapkic@gmail.com [3] yagcituna@gmail.com [4] cemalaktepe06@gmail.com [5] gzm.tuncer@gmail.com

***Özet*—Bu çalışmada, Ankara ilindeki kablosuz internet kullanıcılarının güvenli internet kullanım alışkanlarının incelenmesi ve toplumun sosyoekonomik düzeyi ile bilgi güvenliği farkındalığı arasındaki ilişkinin araştırılması hedeflenmiştir. Bu kapsamda kablosuz ağ cihazlarına yönelik ilçe bazlı güvenlik düzeyi ölçümleri uzaktan izleme ile yapılarak araştırma sonuçları Türkiye İstatistik Kurumu verileriyle karşılaştırılmıştır. Ankara ilinin Çankaya, Yenimahalle ve Keçiören ilçelerinde yapılan alan çalışması kapsamında 16978 kablosuz ağ cihazı incelenmiştir. Elde edilen sonuçlara göre incelenen cihazların %72 oranında güvenli kabul edilen WPA2 şifreleme bulunduğu, %64 oranında SSID kimliğinin değiştirilmiş olduğu, %43 oranında WPS standardı kullandığı, %98 oranında 2GHz bandında yayın yaptığı tespit edilmiştir. Sonuçlar bilgi güvenliği farkındalığı ile Ankara ili halkının sosyoekonomik düzeyleri arasında %95,58 oranında benzerlik ortaya koymaktadır. Bu çalışmanın toplumun bilgi güvenliği farkındalığına dikkat çekmesi ve temel eğitim müfredatlarına konulması yönünde katkılarının olacağı değerlendirilmektedir.**

Anahtar Kelimeler—Kablosuz; Farkındalık; Web Güvenliği

Abstract— This paper analyses the habit of using secure internet between the wireless network users in Ankara, the capital of Turkey and examines the relationship between socioeconomic level of people and information security awareness. In this context, district based security measurements for wireless network devices have done with remote tracking and the results have been compared with TUIK's data. 16978 wireless network devices has been examined within the field study in Ankara city; particularly Çankaya, Yenimahalle and Keçiören districts. Study shows that %72 of the examined devices use WPA2 encryption (which acknowledged as secured), as %64 have changed their SSID, %43 are using WPS security standard and %98 are broadcasting on 2GHz frequency. Results show %95,58 similarity between information security awareness and socioeconomic levels of people of Ankara. It has been considered this study will call attention to information security awareness and contributes to put to syllabuses of basic education.

Keywords— Wireless; Awareness; Web Security

I. GİRİŞ

Teknolojinin hızla geliştiği günümüzde, evlerde ve iş yerlerinde internet ve kablosuz ağ kullanımı artış göstermektedir. Akıllı cihazların ve taşınabilir bilgisayarların kullanımının artması, kablosuz erişim noktalarının çok sayıda kişi tarafından kullanılmasını sağlamıştır. Bu ağ cihazlarını kurup yöneten ve kullanan kişilerin toplumu oluşturan bireyler oldukları düşünülürse bilgi güvenliği farkındalığı ve temel bilişim güvenliği düzeylerinin, halkının ancak %10,76'sının üniversite mezunu olduğu [1] ve temel güvenlik eğitimlerini müfredatlarında bulundurmayan bir ülkede, beklentilerin altında olabileceği öngörülmektedir.

Bilgi güvenliği farkındalığının oluşması için literatürde çok sayıda ve geniş katılımlı çalışmalar yapılmaktadır [2-5]. Kablosuz ağ güvenliği farkındalığı konusunu temel alan çalışmalar da mevcuttur [6].

Bu çalışmalar incelendiğinde mevcut sorunların bilgi güvenliği farkındalığının düşük olması ve kullanıcıların çoğunluğunun kablosuz ağ cihaz güvenliği konusunda cihazın varsayılan ayarlarını kullanmak gibi bilinçsiz yaklaşımlar benimsediği öngörülmektedir.

Holvast tarafından yapılan bir çalışmada güncel gizlilik kavramı teknolojinin gelişmesine bağlı olarak video kayıt, biyometrik, genetik, kimlik hırsızlığı, veri madenciliği, akıllı kartlar, GPS, internet, kablosuz haberleşme ile memetik, dilbilim, ortam zekası gibi gelecek teknolojileri içine alan bir konsept olarak değerlendirilmektedir [7].

Kablosuz ağ cihazlarının yaygın olarak bulunması ve aktif olarak kullanılması güvenlik endişelerini beraberinde getirmektedir. Bu ağlardaki yönetim bilinçsizliğinden kaynaklanan güvenlik açıkları kullanıcı verilerini tehdit etmektedir [8].

Kablosuz ağ cihazlarına erişim ve denetim her geçen gün farklı engelleri beraberinde getirmektedir. Bu alanda Wardriving gibi yöntemler güvenlik tehditlerinin başında gelmektedir [9]. Eğitim faktörü, özellikle ülkemiz gibi güvenlik farkındalığını temel eğitim müfredatlarında bulundurmayan toplumlar için milli tehdit haline gelmektedir.

Bir ülkenin bilgi güvenliği farkındalığının ölçülmesinde bireylere yapılan anketler önemli olmakla birlikte kişilerin kendilerini doğru değerlendirebilecek bilgi birikimi ve deneyimleri olmadığından sonuçların tutarlı çıkması için toplumun genel yapısını çıkartmak zorlaşmaktadır [2].

Bu sorunun önüne geçmek için farkındalık deneyimleri kişilere anket yapılmadan mesken kablosuz erişim cihazlarının en aktif kullanıldığı zaman dilimlerinde alanında uzman kişilerce uzaktan incelenmesi yani literatürde geçen ifadesiyle Wardriving yöntemleri kullanılmaktadır. Bu çalışmanın sonraki bölümlerinde meskenlerde bulunan cihaz yöneticileri aynı zamanda internet kullanan ve o cihazdan sorumlu ev sahipleri ya da kiracılar cihaz yöneticisi olarak nitelendirilmektedir. Bu çalışma Ankara ili için önerdiğimiz yöntem sayesinde toplumsal bazda orantılı bir örneklem sunmaktadır.

Bu çalışma kapsamında toplumdan örneklem toplanarak kablosuz ağ cihazı yöneticilerinin bilgi güvenliği farkındalığının ölçülmesi ve kişilerin sosyoekonomik durumları arasındaki öngörülen ilişkisinin belirlenerek ileriye yönelik çözüm önerilerinin sunulması amaçlanmıştır.

Bu sayede toplumu oluşturan her kesimden bireyin kendi evindeki kablosuz ağ cihazını nasıl yönettiği ve ne düzeyde farkındalık kültürüne sahip olduğu ortaya konulmaktadır.

Bu çalışmanın ikinci bölümünde kablosuz güvenlik sistemlerine ve yöneticilerin bu güvenlik sistemlerine yönelik davranışlarına ilişkin bilimsel veriler ve araştırmalar, üçüncü bölümünde kullanılan metot ve yöntemler, dördüncü bölümünde deneysel sonuçlar ve son bölümde toplum bilincinin artırılmasına yönelik tartışma ve öneriler sunulmuştur.

II. LİTERATÜR ÇALIŞMALARI

Bu çalışmanın bilimsel yönünün ortaya konulması için mevcut anket çalışmaları, güvenlik raporları, teknik ve sosyal analizler ile toplum farkındalığı önerileri incelenerek tartışılmıştır.

Zhang ve arkadaşları tarafından siber suçlar üzerinde bir araştırma çalışması yapılmıştır. Yazarlara göre bilişim suçları beş farklı sınıfta kategorize edilmelidir. Bu kategoriler; bilgisayar ve ağların bir suç aracı olarak kullanılması(Copyright, Spamming), bilgisayar ve ağların bir suç hedefi olması(DOS Attack, Malware, Hacker), bilgisayar ve ağların bir suç mekanı olması(Phreaking), bilgisayar ve ağlar üzerinden işlenen geleneksel suçlar(Phishing, Online Gambling, Cyberterrorism) ve diğer bilgi suçları(Trade Secret) olarak beş başlık altında incelenmektedir. Sonuç olarak, insanların bu tip saldırılara karşı ayrı ayrı bilinçlendirilmesi ile güvenlik artışı hedeflenmiştir [2].

Rezgui ve Marks tarafından yapılan bir çalışmada gelişmekte olan ülkelerden olan Birleşik Arap Emirlikleri'nde bulunan yükseköğretim kurumlarında çalışan kişilerin bilgi sistemi tehditleri karşısındaki tutumları ile güvenlik farkındalık düzeylerinin belirlenmesine yönelik bir araştırma yapılmıştır. Yazarlar, üniversite çalışanlarının genel olarak davranışlarını etkileyen sosyal değişkenlerin özellikle kültürel önyargılar ve bireysel inançlar ile sorumluluk bilinci olduğunu, güvenlik farkındalık düzeyinin ise bundan kısmi olarak etkilendiğini tartışmaktadır. Bu çalışmada 45 kişilik bir denek grubuna sunulan anket çalışması, gözlemler ve sistem kullanım kütükleri gibi incelemeler sonucunda ortam şartları, politikalar, yönergeler ve standartların bilgi güvenliği farkındalığının sağlanmasında aktif rol oynadığı düşünülmektedir [3].

Parsons ve arkadaşlarının yaptığı bir çalışmada ise bilgisayar sistemlerindeki çoğu tehdidin kullanıcı davranışlarıyla ilişkilendirilebileceği ortaya konulmuştur. Tasarlanan bir anket çalışması ile iş yeri bilgisayarı kullanımındaki prosedür ve politikalar hakkındaki bilgi, tavır ve bunların davranışlar üzerindeki etkileri incelenmiştir. Yazarlar 500 Avusturalyalı bireyin katıldığı anketin sonuçlarına göre politika ve prosedür hakkındaki bilgiler ve bunlara karşı gösterilen direnç davranışı gözlemlemişlerdir [4].

Huang ve arkadaşları tarafından yapılan bir çalışmada bilişim sistemleri güvenliği ve sistemi kullanan kişilerin güvenlik algılarını arasındaki ilişkiyi analiz etmek için 2 farklı yöntem önerilmiştir. İlk yöntem denek grubuna çevrimiçi bankacılık deneyimi diğeri ise bir tartışma sitesine üye olma süreçlerini kapsamaktadır. Sonuç olarak bilginin algı üzerinde en etkili bileşen olduğu, güvenlik algısının insanların bilişim temelli uygulamaları kullanmalarını geliştirdiği görülmüştür. Yazarlar çalışmanın Çin kültürüne bağlı etkilerden dolayı diğer kültürler ve yaş grupları ile kıyaslamalar yapılması gerektiğini tartışmaktadır [5].

Deloitte şirketinin Hindistan'da 2008 yılında yaptığı bir araştırmada, Hindistan'da güvenli sayılmayan (Şifresiz ve WEP) ağların, tüm ağların %86'sını kapsadığını ortaya koymuştur [6].

Fatani ve arkadaşlarının yaptığı bir çalışmada kablosuz ağ güvenlik riskleri; kablosuz sinyallerin bina dışına taşması, izinsiz kablosuz ağ kurulumu, cihaz açıkları, mimari sinyal kayıpları, yasadışı erişim, yasadışı sinyal dinleme, DoS saldırıları ve hatalı yapılandırma olmak üzere 8 kategoride ele alınmıştır [8].

Shukla ve arkadaşlarının yaptığı bir çalışmada 33 yükseköğrenim enstitüsünün kullandıkları kablosuz ağ standartları ve güvenlik özellikleri araştırılmıştır. Çalışmada, WPA-PSK'nın statik bir şifreleme türü kullandığı, WPA'nın (Wi-Fi Protected Access) ise TKIP kullanıp şifresinin otomatik olarak değiştiği, bu yüzden de WPA'nın daha güvenli bir şifreleme olduğu tartışılmıştır. WEP (Wired Equivalent Privacy) protokolü ise paylaşımlı statik şifreler kullandığından güvenliğinin diğerlerinden daha düşük ve istenilirse izinsiz erişime karşı açık bir protokol olduğu gösterilmiştir [10].

Cone ve arkadaşları tarafından yapılan bir çalışmada ise siber güvenlik eğitimi ve farkındalığı için bir video oyunu önerilmiştir. Tasarlanan oyun eğitim politikalarına ve kurum gereksinimlerine uygun olarak geliştirilmiştir. Yazarlar, bu oyun motoru sayesinde fiziksel güvenlik, sistem yapılandırma güvenliği, para korunumu ve siber saldırılara karşı tepki gibi konulara katılımcının dikkatini çekmeye çalışmışlardır. Sosyal Mühendislik, erişim denetimi, şifre yönetimi, veri korunması

ve fiziksel güvenlik mekanizmaları gibi konuları içeren temel farkındalık senaryoları önerilmiştir. Geliştirilen senaryolar halen 130 kuruluş çalışanı üzerinde test edilmekle birlikte sonuçlar henüz açıklanmamıştır [11].

Veri güvenliği farkındalığını artırmak için ülkemizde de geliştirilmiş uygulamalar mevcuttur. Bu uygulamalardan birisi olan Ajan4141, bilgi güvenlik bilincini artırmak için geliştirilmiş bir eğitim benzetimidir [12].

Kruger ve arkadaşları 2006 yılında yaptıkları bir çalışmada uluslararası bir madencilik şirketinde bilgi güvenlik farkındalığını ölçmek için prototip bir model geliştirmişlerdir. Sonuç olarak ölçüm aracının bilgi güvenlik farkındalığı programının yönetim kuruluna bilgi sağlayabilecek yardımcı bir kaynak olarak öngörülmüştür. Bu şekildeki bir model basit bir yöntem ile veri toplanmasına ve derecelendirme sisteminin yapılmasına olanak tanımaktadır. Ayrıca çok kriterli sorunun çözümünü ve güvenlik bilinci seviyelerinin nicel bir şekilde ölçümünü sağlamıştır [13].

Gonzalez tarafından yapılan bir araştırmada Wi-Fi standartlarının geçmişi ve yeni Wi-Fi teknolojilerinin uyumluluk sorunları ele alınmıştır. 1999 yılında WEP şifrelemesinin çıktığı, 2001 yılında ise WEP'in ciddi güvenlik açıklarının bulunduğundan bahsedilmiştir. Bunun üzerine 2003'te gelen TKIP WPA ağını 2004'te duyurulan, WPA'ya göre daha güvenli ve AES şifrelemeli WPA2'nin izlediğinden söz edilmiştir. WPA2'nin daha güvenli olmasına karşın AES şifrelemesinin güçlü donanımlar istemesi ve geriye dönük olmaması, bunun günümüzde dahi bu teknolojiye geçemeyen insanların bulunmasına yol açtığını göstermiştir [14].

Bu konuyla ilgili daha önceden yapılan araştırmalar, bilgi güvenliğinin sağlanmasında teknoloji kadar eğitim ve bireysel farkındalık sorunlarının da olduğunu ortaya koymaktadır. Bu çalışmanın sonraki bölümünde bireylerin bilgi güvenliği farkındalıklarının ölçülmesi ile ilgili yeni bir yöntem sunulmaktadır.

III. METODOLOJİ

Bu bölümde mesken ağ yöneticilerinin bir diğer ifadeyle ev ve işyeri gibi alanlarda internet kullanan ve kullandıran ev sahibi ya da kiracıların kablosuz kullanım alışkanlıklarının incelenebilmesi için Ankara'da yapılan kablosuz ağ cihazı taraması ve bu taramanın nasıl yapılması gerektiğine ilişkin bilgiler ve taramanın yapılış şekline ilişkin gerekçeler verilmiştir.

Çeşitli bölgelerdeki kablosuz ağ cihazlarının incelenmesi kapsamında en uygun zamanı bulmak için çeşitli araştırmalar yapılmıştır. Bu araştırmalar sonucunda internet kullanımının en yoğun olduğu saatlerin 19:00-23:00 arasındaki süre olduğu tespit edilmiştir [15]. Ancak yerleşimi iş yeri ağırlıklı olan bölgeler bu saatlerde mevcut mesai saatlerinden dolayı aktif olmadıklarından iş yeri ağırlıklı bölgeler mesai saatleri dahilinde taranmıştır. Kablosuz ağ cihazlarını listelemek ve bunları bölgelere göre sıralamak için çeşitli uygulamalarla testler ve sonuçlarının performans karşılaştırmaları yapılmıştır. Analizler sonucunda en uygun programın özellikle akıllı cihazlar ile işlemin yapılmasına olanak tanıyan Nirsoft firması tarafından geliştirilen Wi-Fi Collector uygulaması olduğu tespit edilmiştir [16].

Bu araştırmanın alan çalışması için gerekli bölge seçimi, verilerin toplanması ve bu verilerin işlenmesi Grafik 1'de sunulmuştur.

Alan çalışmasında ilk adım, araştırma yapılacak bölgenin seçilmesidir. Bu bölge seçimi; bölgenin eğitim seviyesi ve o bölgenin ağırlıklı olarak mesken veya iş yeri olarak kullanımı göz önüne alınarak yapılmaktadır.

Sonraki adımda, gezici ekipler seçilen bölgeyi GPS ve haritalar ile gezerek kablosuz ağ cihazlarının meta verilerine ulaşmaktadır. Veriler Wi-Fi Collector uygulaması ile toplanarak ön işlemlerden geçirilmekte ve tasarlanan veri, veri işleme modülüne aktarılmaktadır.

Veri işleme modülü, toplanan verilerin önce sınıflara ayrılması ve anlamlı parçaların ayıklanması süreçlerini yönetmektedir.

Son olarak verilerin kıyaslama grafiklerine aktarılmasıyla ve şehir haritası üzerinde görselleştirilmesi ile işlem tamamlanmaktadır.

Araştırma kapsamında incelenen ve genel eğitim seviyesi bilinen [17] bölgelerde yaşayan kablosuz ağlar cihazları tarafından kullanılan WEP, WPA ve WPA2 şifreleme standartları Tablo I üzerinde gösterilmiştir.

TABLO I. KABLOSUZ AĞ CİHAZLARINDAKİ ŞİFRELEME TÜRLERİNİN KARŞILAŞTIRILMASI

Özellik/ Şifreleme Yöntemi	**WEP**	**WPA**	**WPA2**
Yılı	1999	2003	2004
Şifre Uzunluğu	40bit-5/104bit-13 karakter	8-63 ASCII/ 64 Hexadecimal karakter	
Şifreleme Kuvveti	40bit/104bit	128 bit	
Şifreleme Protokolü	Kullanıcı tarafından girilen 40/104bitlik bir şifreleme anahtarı	TKIP	TKIP/AES

Tablo I WEP şifreleme sisteminin WPA ve WPA2'ye göre çok daha güçsüz olduğunu ortaya koymaktadır. Günümüzde WEP şifreleri kolayca kırılabilir hale gelmiştir [18].

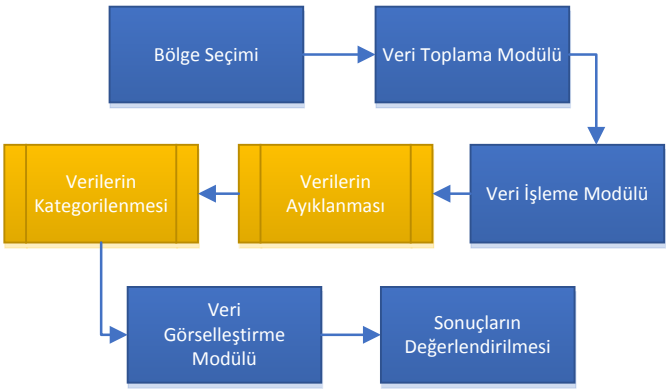
A. Bölge Seçimi

Bölge seçimi kapsamında Ankara ilinin sosyoekonomik düzeyi ve bölgelerin mesken-iş nüfus farklılıkları göz önünde bulundurularak bölgeler seçilmiştir.

Bölgeler seçilirken seçilecek bölgenin yerleşiminin mesken veya iş ağırlıklı olması, seçilen bölgeler arasındaki sosyoekonomik düzey farklılığının belirgin olması ve seçilecek bölgelerdeki nüfusun yoğunluğu olarak üç kriter baz alınmıştır.

Çankaya, yerleşimi iş ağırlıklı alanlardan olup ve sosyoekonomik seviyesi yüksek olduğundan [19];

Yenimahalle ve Keçiören ise yerleşimleri mesken ağırlıklı olduklarından bu çalışma kapsamında seçilmiştir. Bu üç bölgenin ortak özelliği ise nüfus yoğunluklarının örneklem oluşturabilecek kadar fazla olmasıdır.



Grafik 1: Alan çalışmasında izlenilen yöntem

B. *Veri Toplama Modülü*

Veri toplama modülü, verilerin Warwalking ve Wardriving metotlarıyla toplanmasını kapsamaktadır.

Wardriving ve Warwalking metotları, bir araçla veya yaya olarak bölgenin taranıp; bölgede bulunan kablosuz ağ cihazlarının bir sisteme kaydedilmesidir [9]. Toplanan bu veriler kablosuz cihazın ismi, MAC adresi, modem markası, sinyal seviyesi, yayın yaptığı frekans ve kanal, güvenlik ve şifreleme sistemi, BSS tipi, WPS desteği, verinin elde edilme zamanı ve GPS koordinatlarını içermektedir. Bu çalışmada Warwalking ve Wardriving sistemlerini uygularken GPS yardımıyla belirli rotalardaki kablosuz ağ cihazları bölgesel olarak tespit edilmiştir.

Alınan bu veriler ile bir harita taslağı oluşturulup, seçilen bölgelerdeki eksik kısımlar ve rotalar gözlemlenmiş; çeşitli rotalardaki ve bölgelerdeki kablosuz yoğunluk değişimleri incelenerek bu inceleme sonuçları bölgelerin sosyoekonomik düzeyleri ile karşılaştırılmıştır.

C. *Veri İşleme Modülü*

Veri işleme modülünde toplanan veriler ayıklanma işleminden sonra kategorize edilmektedir.

Veriler, bulundukları bölgedeki çakışmaları önlemek ve bu bölgelerdeki eksik bilgi veren kablosuz ağ cihazlarının ayıklanması, dolayısıyla tarama verilerinin daha kaliteli analiz edilmesine olanak tanımaktadır.

Veriler ayıklandıktan sonra bölgelerine, şifreleme türlerine, WPS özelliklerine, ağların bağlı olduğu cihazın markasına, SSID'sine ve yayın yaptıkları frekanslara göre kategorileri ayrılmaktadır.

Örnek olarak Çankaya verileri için:

- Yapılan diğer tarama verileriyle aynı olan ögeler ayıklanır.
- Eksik bilgi veren kablosuz ağ cihazları ayıklanır.
- Ayıklanan veriler daha sonra belirlenen kategorilere göre sıralanır.

D. *Veri Görselleştirme Modülü*

Ayıklanan ve kategorize edilen veriler görselleştirme modülü ile grafikler üzerinde anlaşılır hale getirilir. Buna ek olarak Veri Toplama Modülünde oluşturulan harita taslağı işlenen veriler ve bu verilerin sahip oldukları GPS koordinatlarıyla beraber kullanılarak tamamlanır.

Resim 1: Tamamlanmış bir harita taslağı.

E. *Sonuç Modülü*

Ayıklanan ve görsel haline getirilen veriler, diğer bölgelerle ve araştırmalarla karşılaştırılır.

Bu karşılaştırmaların sonuçlarına göre bölgenin kablosuz ağ farkındalığı yüzde olarak (WPS aktif olmayan ağ yüzdesi(WPS^-) + WPA2 şifreleme türüne sahip ağ yüzdesi + SSID'si değiştirilmiş ağ yüzdesi($SSID_D$))/3 formülü ile hesaplanır.

KFP(Kablosuz Farkındalık Puanı)= ($\%WPS^-$ + $\%SSID_D$ + %WPA2)/3

Sonraki bölümde bu çalışma kapsamında elde edilen sonuçlar ve önerilen Kablosuz Farkındalık Puanı değerleri sunulmuştur.

IV. DENEYSEL SONUÇLAR

Metodoloji bölümünde önerilen yöntem ile yapılan tarama ve sonuçları bu bölümde sunulmaktadır.

Alan çalışması kapsamında Ankara'da önerilen yöntem ve uygulama ile mesken çeşitliği dikkate alınarak çeşitli güzergahlardaki kablosuz ağ cihazlarına ait bilgiler toplanmıştır.

Yaptığımız alan çalışmaları neticesinde 16.978 adet kablosuz ağ cihazına ait veri elde edilmiştir. Bu verilerin işlenmesi ve incelenmesi sonucunda: 16.978 kablosuz ağ cihazının 12.303 tanesi WPA2, 3.119 tanesi WPA, 426 tanesi WEP güvenliğine sahipken 1130 tane güvenliği olmayan ve

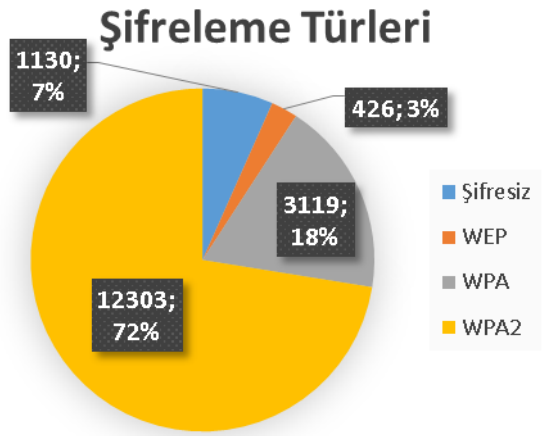
herkes tarafından erişebilir konumda ağ cihazı olarak bulunmaktadır.

Bu ağların 10.136 tanesinin varsayılan (default) haldeki SSID'leri değiştirilmişken 6.112 cihazın SSID'leri varsayılan olarak bırakılmıştır. Bu verilere ek olarak 730 tane de SSID'si gizlenmiş ağ tespit edilmiştir. Bu ağların 7.320'sında WPS bulunurken 9.658 ağda WPS'ye rastlanılmamıştır. 16.978 ağın 16.570'i 2GHz frekansında, 408 tanesi de 5GHz frekansında yayın yapmaktadır. Araştırma kapsamında bulunan bütün kablosuz cihazların yasal aralık dahilinde [20] yayın yaptıkları tespit edilmiştir.

TABLO II. İLÇELERE GÖRE KABLOSUZ AĞ ÖZELLİKLERİ

Özellik	Kategori	Çankaya	Keçiören	Yenimahalle
SSID	Varsayılan	1318	2076	2718
	Değiştirilmiş	4349	3288	2499
	Gizli	338	201	191
Şifreleme Türü	Şifresiz	563	316	251
	WEP	202	151	73
	WPA	887	1196	1036
	WPA2	4354	3903	4046
WPS	WPS+	2347	3480	3831
	WPS-	3659	2086	1575

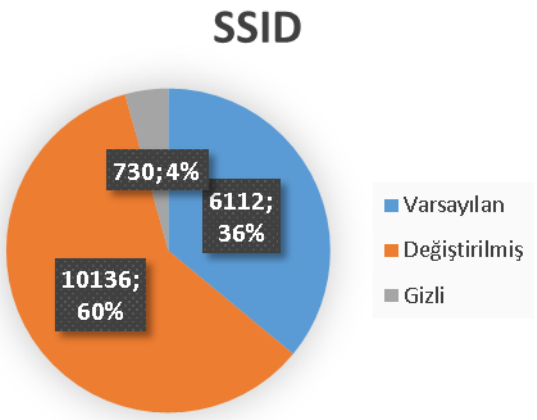
Bu araştırma ile elde edilen verilere ait kıyaslama görselleri Şekil 1-6 nolu grafiklerde sunulmaktadır.



Şekil 1: Kablosuz ağlardaki şifreleme türleri

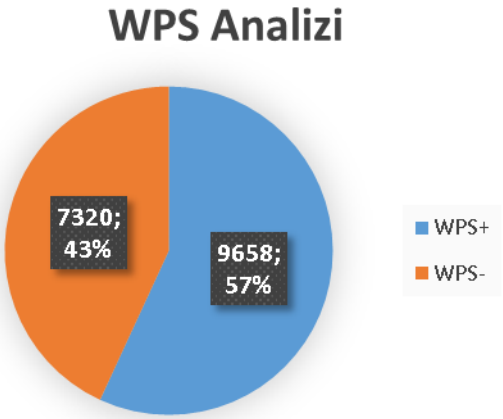
Şekil 1'de araştırmaya katılan ağ cihazlarının şifreleme yöntemlerine ait karşılaştırmalar sunulmaktadır.

Güvenli sayılan WPA2'nin bütün kablosuz ağ cihazlarının %72'ini kapsaması araştırmanın yapılmış olduğu bölgelerdeki kablosuz ağ güvenliğinin ve güvenlik farkındalığının yüksek olduğunu gösterir.



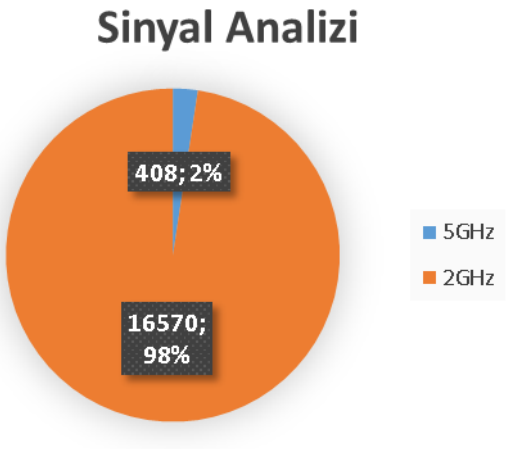
Şekil 2: Kablosuz ağların SSID türü

SSID, her modemin kendini kullanıcıya tanıtmak için kullandığı maksimum 32 alfanümerik karakterden oluşabilen isimdir. SSID, kullanıcının isteğine göre değiştirilebilir veya gizli hale getirilebilir. SSID'nin varsayılan olarak bırakılması, modemi çeşitli saldırılara açık hale getirebilmektedir [21]. Şekil 2'de araştırmaya katılan ağ cihazlarının SSID isimlerine ait karşılaştırmalar sunulmaktadır.



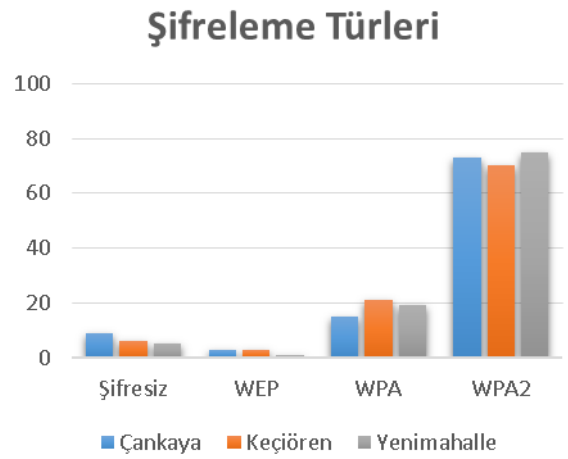
Şekil 3: Kablosuz ağ cihazlarının WPS analizi

WPS(Wi-Fi Protected Setup), kullanıcıların bir tuş aracılığıyla uzun şifreler girmesine gerek kalmadan kablosuz bir ağa bağlanmasını sağlayan bir internet güvenlik standardıdır. Ancak WPS'nin açık tutulması kablosuz ağ cihazını saldırılara açık hale getirebilir [22]. Şekil 3'te araştırmaya katılan ağ cihazlarının SSID isimlerine ait karşılaştırmalar sunulmaktadır.



Şekil 4: Kablosuz ağ cihazlarının yayın frekansı

Normal şartlar altında kablosuz yayınların frekansı 2GHz'dir. Ancak bazı modemler 5GHz frekansta yayın yapmaya da olanak sağlamaktadır. 5GHz frekans daha az kullanıldığından ötürü diğer frekanslarla karışma ihtimali 2GHz'ye göre daha düşüktür. Ancak frekansı yüksek olduğundan dolayı kapsama alanı 2GHz'ye göre daha düşüktür. Bazı ülkelerde ise askeri ve hava-radar iletişimleriyle çakışmayı engellemek için [23] 5GHz yayın frekansının kullanılması yasa dışı sayılmaktadır [20]. Şekil 4'te araştırmaya katılan ağ cihazlarının frekans bant karşılaştırmaları sunulmaktadır.



Şekil 5: İlçelere göre kablosuz ağ şifreleme türleri

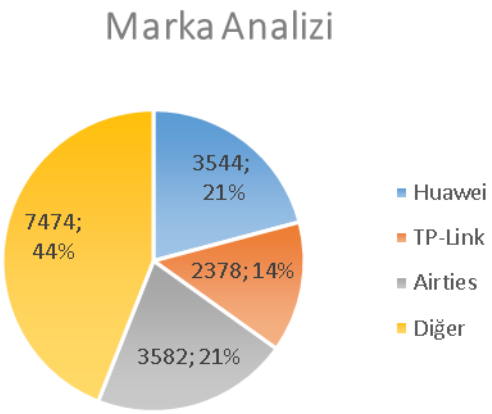
Şekil 5'teki verilere bakıldığı zaman yerleşimi hem iş yeri hem mesken ağırlıklı olan Çankaya semtindeki şifrelemesi olmayan kablosuz oranı mesken ağırlıklı yerleşim yerleri olan Keçiören ve Yenimahalle'ye göre daha fazla olduğu tespit edilmiştir. Bunun en büyük sebebi çoğu kurumsal ağların müşteri ihtiyaçları doğrultusunda şifresiz sunulması olduğu düşünülmektedir.

TABLO III. EN UZUN VE EN KISA 10 SSID

En Uzun 10 SSID	**Uzunluk**
Anca internetini ac dersin zaten	32
Turkcell BlackBerry Hotspot 4451	32
www.icgiyimkolik.com>0312*****63	32
ANKARAGUCU_DUSTU_MELIH_DE_DUSCEK	32
YeniBinyilSurucuKursuMotorsiklet	32
HP-Print-7F-Officejet Pro X476dw	32
GOLGE ILK YARDIM EGITIM MERKEZI	31
Uyan_ey_gozlerim_gafletten_uyan	31
Basgan internet mi lazim la? :)	31
DIRECT-2H-Dilan KasacÄ± (Galaxy	31

En Kısa 10 SSID	a	B	n	X	x	9	13	AB	AC	ae
Uzunluk	1	1	1	1	1	1	2	2	2	2

En uzun SSID'ler incelendiği zaman 10 SSID'nin sadece 1'inin varsayılan SSID olduğu gözlenmektedir.



Şekil 6: Kablosuz ağ cihazlarının marka analizleri

Marka analizi verilerinde %10 ve altı diğer kategorisinde belirtilmiştir. Burada belirtilmiş 3 markanın diğer markalardan daha fazla olmasının başlıca sebebinin internet dağıtım şirketlerinin bu 3 marka ile ortak yürüttüğü kampanyalar olduğu düşünülmektedir.

Bütün bu verilerin KFP'si hesaplandığında özellikle mesken ve işyerlerinde bulunan kablosuz ağ yöneticilerinin %64 oranında bilgi güvenliği farkındalığına sahip oldukları anlaşılmaktadır.

Elde edilen bulgular ve mevcut istatistikler sonraki bölüm içerisinde tartışılmıştır.

V. TARTIŞMA

Bu bölümde elde edilen sonuçlar TÜİK verileri kullanılarak [17] toplumun sosyoekonomik örneklemleri ile kıyaslanması ve incelemenin yapıldığı bölgelerde yaşayan kablosuz ağ cihazlar yöneticilerinin bilgi güvenliği farkındalık düzeyleri tartışılmıştır.

TABLO IV. ARAŞTIRMA VERİLERİ İLE TÜİK EĞİTİM SEVİYESİ VERİLERİNİN [17] YÜZDELİK ORANDA KARŞILAŞTIRMASI

Özellik	Kategori	Çankaya	Keçiören	Yenimahalle
SSID	Varsayılan	22	37	50
	Gizli	6	4	4
	Değiştirilmiş	72	59	46
Şifreleme Türü	Şifresiz	9	6	5
	WEP	3	3	1
	WPA	15	21	19
	WPA2	73	70	75
WPS	WPS^+	39	63	71
	WPS^-	61	37	29
KFP	**(WPS^- + $SSID_D$ + WPA2)/3**	**68**	**55**	**50**
Eğitim Durumu	İlkokul	12	24	20
	İlköğretim	10	19	14
	Ortaokul	5	8	7
	Lise	34	32	33
	Üniversite	39	17	26
Ortaöğretim Üzeri Eğitim Durumu	**Lise + Üniversite**	**73**	**49**	**59**

KFP (Kablosuz Farkındalık Puanı); belirli bir bölgedeki kablosuz ağların bilinçli kullanım oranını hesaplamak için düşünülen; bilinçli kullanılan kablosuz ağ cihaz özellikleri (WPS kullanılmaması, WPA2 şifreleme kullanılması ve SSID'nin değiştirilmiş olması) yüzdelerinin toplanıp 3'e bölünerek, 0 ile 100 arasında elde edilen bir puandır.

KFP verilerinin TÜİK eğitim durumu verileri ile ilişkisini incelemek için KFP'ler ve Ortaöğretim Üzeri Eğitim Durumu yüzdeleri kendi aralarında toplanıp aralarındaki ilişki yüzde olarak hesaplanmıştır.

TÜİK verilerine göre [17] Yenimahalle bölgesindeki ortaöğretim üzeri eğitim (Lise + Üniversite) %59 oranındadır. Yenimahalle verilerine KFP uygulandığında ise kablosuz ağ bilinçlilik oranının %50 olduğu görülmektedir. Aynı şekilde Çankaya ilçesindeki bu oranlar sırasıyla %68 ve %73'tür. Keçiören ilçesinde ortaöğretim üzeri eğitim %49 iken kablosuz ağ bilinçlilik oranının %55 olduğu görülmektedir.

Bu veriler ışığında eğitim seviyesi ile kablosuz ağ bilinci arasında doğru orantılı bir ilişki olduğu öngörülmekle birlikte çalışmanın farklı coğrafi bölgelerde ve ülkelerde yapılarak sonuçların desteklenmesi gerekmektedir.

VI. SONUÇ VE ÖNERİLER

Bu çalışmada kablosuz ağ cihazı kullanıcılarının, kablosuz ağ cihaz kullanım alışkanlıklarının incelenmesi ve toplumun eğitim düzeyinin kablosuz ağ kullanım farkındalığıyla ilişkisinin incelenmesi amaçlanmıştır. Bu çalışmanın yapılması için önceki bölümlerde anlatılan Wardriving ve Warwalking yöntemleri kullanılmıştır. Bu yöntemler seçilirken yöntemin efektifliği ve daha sonra yapılacak çalışmalar ile uyumluluğu göz önüne alınmış, seçilen yöntemlerin uygulanması kapsamında 5 adımlı bir alan çalışması yöntemi önerilmiştir. Bu çalışma kapsamında çalışır halde 16978 kablosuz ağ cihaz verisi incelenmiş, incelenen bu verilerin yüzdeleri Tablo IV üzerinde gösterilmiştir. Bütün bölgelerde WEP şifreleme türüne sahip kablosuz ağ cihazlarının diğer türlere göre en küçük payı almasına karşılık güncel olan WPA2 şifreleme türünün ise bütün bölgeler için en yüksek paya sahip olduğu anlaşılmaktadır. Yenimahalle ilçesindeki kablosuz ağ cihazlarında diğer bölgelerden farklı olarak, varsayılan (default) SSID oranı, SSID türleri arasında çoğunluğa sahip olduğu görülmektedir. Buna karşılık olarak WEP şifreleme türünün diğer bölgelere göre daha az cihazda bulunmuştur. Çankaya bölgesinde ise WPS özelliği kullanılmayan cihaz yoğunluğunun diğer iki bölgeye göre daha fazla olduğu görülmektedir. Ayrıca Çankaya bölgesinde ortaöğretim üzeri eğitim seviyesi ve önerdiğimiz Kablosuz Farkındalık Puanı diğer iki bölgeye göre daha fazla olduğu görülmektedir. TÜİK'in 2013 ilçelere göre eğitim seviyesi verileri ile bu ilçelerin KFP'leri arasında %95,58'lik bir yakınsama olduğu görülmektedir. Bu çalışma, Türkiye'deki sosyoekonomik durumun bilgi güvenliği üzerindeki etkisini ortaya koymaktadır.

Kablosuz ağların kullanımı için devlet ve kullanıcıların yapması gerekenler maddeler halinde belirtilmiştir.

- Kablosuz ağ güvenliğindeki farkındalığı artırmak için ilköğretim düzeyinden itibaren müfredatlara bilgi güvenliği farkındalık eğitimleri eklenmelidir.
- Kullanıcılar SSID ve şifreleme türleri hakkında kurulum sihirbazları, kamu spotları, cihaz üreticileri ve servis sağlayıcılar tarafından bilgilendirilmelidir.
- Okuma yazma oranı düşük olan ülkemizde bilgi güvenliği farkındalığı için halk eğitimlerine önem verilmelidir.
- Kablosuz ağ cihazlarının güvenlik özellikleri BTK tarafından standart haline getirilerek, bu cihazlar için bir SSID ataması veya ilk kurulumda SSID'nin değiştirilmesinin, şifre değişikliğini WPA2 türünde yapılması ve WPS özelliğinin kapalı olmasının sağlanması niteliklerini kapsayan bir süreç olmalıdır.

Kablosuz ağların güvenliğini artırmak için; aktif olarak kullanılmıyorsa WPS'nin devre dışı bırakılması, kablosuz ağ cihazınızın SSID'sinin değiştirilmesi ve WPA2 şifreleme türünün kullanılması önerilmektedir.

Bu çalışmanın sonuçları tartışıldığı zaman kablosuz ağ cihaz güvenliğinin sağlanmasında sosyoekonomik kriterlerin önemli olduğu ve halkın bilgi güvenliği farkındalığı kazanmasında gelir ve eğitim düzeyi arasında ilişki olduğu gösterilmiştir.

KAYNAKÇA

[1] TÜİK, Ulusal Eğitim İstatistikleri Veri Tabanı, 2013.

[2] Yanping Zhang, Yang Xiao, Kaveh Ghaboosi, Jingyuan Zhang and Hongmei Deng , A survey of cyber crimes, 2011.

[3] Yacine Rezgui, Adam Marks, Information security awareness in higher education: An exploratory study, 2008.

[4] Kathryn Parsons, Agata McCormac, Marcus Butavicius, Malcolm Pattinson, Cate Jerram, Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q) 2014.

[5] Ding-Long Huangan, Pei-Luen Patrick Raua, Gavriel Salvendy, FeiGaoa, Jia Zhou, Factors affecting perception of information security and the irimpacts on IT adoption and security practices, 2011.

[6] Deloitte, Wireless Network Security Landscape of India, 2008.

[7] Jan Holvast, History of Privacy, 2009.

[8] Hanan A. Fatani, Ikhlas F. Zamzami, Muhammed Aydin and Mansur Aliyu, Awareness Toward Wireless Security Policy:Case Study of International Islamic University, 2013.

[9] Huwida Said, Mario Guimaraes, Noora Al Mutawa, Ibtesam Al Awadhi, Forensics and War-Driving on Unsecured Wireless Network, 2011.

[10] Ranjana Shukla, Samad S. Kolahi, Robert Freeth and Avikash Kumar, Educational Institutes: Wireless Network Standards,

[11] Security and Future, 2010.

[12] Benjamin D. Cone, Cynthia E. Irvine, Michael F. Thompson, Thuy D. Nguyen, A video game for cyber security training and awareness, 2006.

[13] Ajan 4141. [Online]. HRİKa Çözümler, 2009.

[14] Kruger, H. Kearney, W.,"A prototype for assessing information security awareness", 2006.

[15] David González-Tarragó, Home Wireless Security and Privacy: A Practical Protocol Mixing, 2010.

[16] Tom Lawrence. (2011, November 16). "Evening internet 'rush-hour' affects Broadband users" [Online]. Available: http://www.independent.co.uk/life-style/gadgets-and-tech/news/evening-internet-rushhour-affects-broadband-users-6262838.html

[17] Nirsoft, Wifi-Collector. [Online]. Nir Sofer, 2014.

[18] Türkiye İstatistik Kurumu, Seçilmiş Göstergelerle Ankara 2013, 2014.

[19] Nikita Borisov, Ian Goldberg, David Wagner. (2015-4-2) [Online]. Available: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[20] Ankara'nın Kentsel Yoksulluk Haritası, 144 p., Ankara, Turgut Özal Üniversitesi, 2012.

[21] Kısa Mesafe Erişimli Telsiz Cihazları (KET) yönetmeliği Resmi Gazete 10.03.2010 Madde 8 - Genişband veri iletim sistemleri.

[22] Susan Young, Dave Aitel, The Hacker's Handbook: The Strategy Behind Breaking into and Defending Networks, 2003, pp. 588-589.

[23] Viehböck, Stefan. (2011-12-26) "Brute forcing Wi-Fi Protected Setup" [PDF]. Available: https://sviehb.files.wordpress.com/2011/12/**viehboeck_wps**.pdf

[24] Federal Communications Commission 15.407 (2014,October 1).

Uraz YAVANOĞLU Ankara doğumludur. Gazi Üniversitesi Bilgisayar Mühendisliği Bölümü'nde araştırma görevlisi olarak çalışmaktadır. Yüksek lisansını Gazi Üniversitesi Bilgisayar Mühendisliği'nden ve doktorasını Gazi Üniversitesi Elektrik Eğitimi'nden almıştır. Araştırma alanları Yapay Zeka, Veri Madenciliği, Bilgi Güvenliği, Adli Bilişim Analizi ve Bilgisayar Grafikleridir. GUTIC (Gazi University Technology and Innovation Center) araştırmacısı olup doktora sonrası çalışmalarını Arizona Eyalet Üniversitesi Bilgisayar Bilimleri Mühendisliği'nde sürdürmektedir.

Ahmet KAPKİÇ Ankara doğumludur. Şu anda Gazi Üniversitesi Bilgisayar Mühendisliği bölümünde lisans eğitimini sürdürmektedir. Araştırma ilgi alanları Yapay Zeka, Obje Yönelimli Programlama, Kriptoloji ve Bilgi Güvenliğidir.

Sadık Tuna YAĞCI Karabük, Türkiye'de doğmuştur. Şu anda Gazi Üniversitesi Bilgisayar Mühendisliği bölümünde lisans eğitimini sürdürmektedir. Araştırma ilgi alanları Yapay Zeka, Obje Yönelimli Programlama ve Bilgi Güvenliğidir.

Cemal AKTEPE Ankara, Türkiye'de doğmuştur. Şu anda Gazi Üniversitesi Bilgisayar Mühendisliği bölümünde lisans eğitimini sürdürmektedir. Araştırma ilgi alanları Yapay Zeka, Obje Yönelimli Programlama ve Bilgi Güvenliğidir.

Gizem TUNÇER Ankara, Türkiye'de doğmuştur. Şu anda Gazi Üniversitesi Bilgisayar Mühendisliği ve Anadolu Üniversitesi İşletme bölümünde lisans eğitimini sürdürmektedir. Araştırma ilgi alanları Bilgi Güvenliği, Obje Yönelimli Programlama ve Yapay Zekadır.