# KABLOSUZ AĞ CİHAZI ERİŞİM GÜVENLİĞİ VE FARKINDALIK ANALİZİ: ANKARA ÖRNEĞİ

**Uraz Yavanoğlu, Ahmet Kapkiç, S. Tuna Yağcı, Cemal Aktepe ve Gizem Tunçer**
Gazi Üniversitesi, Bilgisayar Mühendisliği Bölümü, Maltepe 06570, Ankara
uraz@gazi.edu.tr , ahmetkapkic@gmail.com, yagcituna@gmail.com, cemalaktepe06@gmail.com, 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 gösterdiği tespit edilmiştir. Bu makale ISDFS 2015 konferansında sunulmuş olup seçilmiş bildiriler içerisine girdiği için bu dergide basılmıştır.

**Anahtar Kelimeler:** Kablosuz Ağ, Cihaz, Erişim Güvenliği, Farkındalık, Analiz, Web Güvenliği, Ankara.

# WIRELESS NETWORK DEVICE ACCESS SECURITY AND AWARENESS ANALYSIS: CASE OF ANKARA

**ABSTRACT**

This paper analyses the habit of using secure internet among the wireless network users and examines the relationship between socioeconomic level of people and information security awareness, especially, in Ankara, the capital city of Turkey. In this context, district based security measurements for wireless network devices have been done with remote tracking devices. The results have been compared with TUIK's data. 16978 wireless network devices have been examined within the field study in Ankara, the capital city of Turkey, particularly, Çankaya, Yenimahalle and Keçiören districts. This study have shown that %72 of the examined devices use WPA2 encryption (which acknowledged as secured), as %64 have changed their SSID, %43 of them are being used WPS security standard and %98 of those are broadcasting on 2GHz. The results have demonstrated that %95.58 similarities between information security awareness and socioeconomic levels of people lived in Ankara.

**Keywords:** Wireless, Networks, Analysis, Device, Access Security, Awareness, Web Security, Ankara.

## 1. GİRİŞ (INTRODUCTION)

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 çalışmalarda mevcuttur [6].

Literatürdeki mevcut çalışmalar incelendiğinde, sorunların bilgi güvenliği farkındalığının düşüklüğü, kullanıcıların çoğunluğunun kablosuz ağ cihaz güvenliği konusunda cihazların varsayılan ayarlarını kullandığı, güvenlik risklerinin farkında olunmadığı veya çözümlerin neler olduğunun bilinmediği gibi hususların bulunduğu belirlenmiştir.

Holvast tarafından sunulan bir çalışmada güncel gizliliği destekleyen, video kayıt, biyometrik, genetik, kimlik hırsızlığı, veri madenciliği, akıllı kartlar, GPS, internet, kablosuz haberleşme ile memetik, dilbilim, ortam zekâsı gibi gelecek teknolojilerin olduğu raporlanmıştır [7].

Kablosuz ağ cihazlarının yaygın olarak bulunması ve aktif olarak kullanılması güvenlik endişelerini beraberinde getirmektedir. Bu ağların yönetimindeki vurdumduymazlık ve bilinçsizlikten kaynaklanan güvenlik açıklarının, kullanıcıları ve sahip oldukları verileri 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 ciddi bir tehdit haline gelmektedir.

Bilgi güvenliği farkındalığının ölçülmesinde yapılan anketler önemli olsa da kişilerin kendilerini doğru değerlendirebilecek bilgi birikimi ve deneyimleri olmadığından sonuçların tutarlı çıkması için toplumun genel yapısını çıkartmak zorlaşmaktadır [2].

Bu sorunun önüne geçmek için bu çalışmada bir çözüm önerilmiş ve anket yapılmadan meskenlerde bulunan kablosuz erişim cihazlarından veri toplanarak analizler yapılmıştır. Bu ağ cihazların aktif kullanıldığı zaman dilimlerinde, alanında uzman kişilerce uzaktan erişim sağlanarak, literatürde geçen ifadesiyle Wardriving yöntemleri kullanılarak incelenmiş ve değerlendirmeler yapılmıştır. Bu çalışma kapsamında, toplumdan örneklem toplanarak kablosuz ağ cihazı yöneticilerinin veya kullanıcılarının bilgi güvenliği farkındalığının ölçülmesi ve kişilerin sosyoekonomik durumları arasındaki öngörülen ilişkisinin belirlenerek ileriye yönelik çözüm önerilerinin sunulması amaçlanmıştır.

Bunu gerçekleştirmek için toplumu oluşturan her kesimden kablosuz ağ cihazları hakkında bilgiler toplanmış ve bu cihazların nasıl yönetildiği ve ne düzeyde farkındalık kültürüne sahip olduğu belirlenmeye çalışılmıştır. Ankara ili için önerdiğimiz yöntem sayesinde toplumsal bazda orantılı bir örneklem sunulmaya çalışılmıştır.

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 olarak elde edilen bulgular verilmiş, bazı huşular üzerine değerlendirmeler yapılmış ve bazı öneriler sunulmuştur.

## II. LİTERATÜR ÇALIŞMALARI
**(LITERATURE SURVEY)**

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

Siber suçlar üzerine Zhang ve arkadaşları tarafından yapılan bir çalışma da, bilişim suçları beş farklı sınıfta kategorize edilmiştir. 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 mekânı olması (Phreaking), bilgisayar ve ağlar üzerinden işlenen geleneksel suçlar (Phishing, Online Gambling, Cyberterrorism) ve diğer bilgi suçları (Trade Secret) olarak beş başlık altında incelenmiş ve insanların bu tip saldırılara karşı ayrı ayrı bilinçlendirilmesi ile güvenlik artışı hedeflenmiştir [2].

Rezgui ve Marks tarafından, gelişmekte olan ülkelerden olan Birleşik Arap Emirlikleri 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 belirtilmiştir [3].

Parsons ve arkadaşlarının yaptığı başka bir çalışmada, bilgisayar sistemlerindeki çoğu tehdidin kullanıcı davranışlarıyla ilişkilendirilebileceği ortaya konulmuştur. Tasarlanan bir anket çalışması ile işyeri bilgisayarı kullanımındaki, prosedür ve politikalar hakkındaki bilgi, tavır ve davranışlar üzerindeki etkileri incelenmiştir. Yazarlar, 500 Avusturalyalı bireyin katıldığı anketin sonuçlarına göre politika ve

prosedür hakkındaki bilgiler ve bunlara karşı gösterilen direnç davranışını raporlamışlardır [4].

Huang ve arkadaşları tarafından yapılan diğer 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. 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 belirtmişlerdir [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 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 (METHODOLOGY)

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 işyeri ağırlıklı olan bölgeler bu saatlerde mevcut mesai saatlerinden dolayı aktif olmadıklarından işyeri ağırlıklı bölgeler mesai saatleri dâhilinde 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 Şekil 1'de sunulmuştur.

Alan çalışmasında ilk adım, araştırma yapılacak bölgenin seçilmesidir. Bu bölge seçimi; bölgenin eğitim seviyesi ve o bölgenin ağırlıklı olarak mesken veya işyeri 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 [17] ve genel eğitim seviyesi bilinen bölgelerde yaşayan kablosuz ağlar cihazları tarafından kullanılan WEP, WPA ve WPA2 şifreleme standartları Tablo I'de gösterilmiştir.

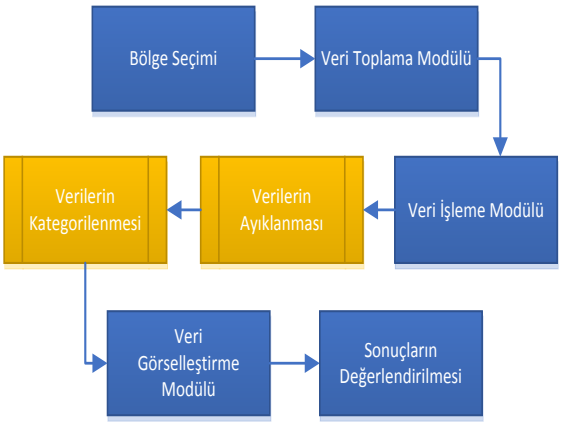
Tablo I'den görülebileceği gibi WEP şifreleme sisteminin WPA ve WPA2'ye göre çok daha güçsüz olduğunu ortaya koymaktadır. Günümüzde, WEP şifreleri kolayca kırılabilir hale gelmiştir [18]. Bu çalışma kapsamında takip edilen metodoloji alt başlıklarda verilmiştir.

TABLO I. KABLOSUZ AĞ CİHAZLARINDAKİ ŞİFRELEME TÜRLERİNİN KARŞILAŞTIRILMASI

| **Özellik/ Şifreleme Yöntemi** | **WEP** | **WPA** | **WPA2** |
|---|---|---|---|
| **Yıl** | 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 40/104 bitlik bir şifreleme anahtarı | TKIP | TKIP/AES |

**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.




Şekil 1. Alan çalışmasında izlenilen yöntem

**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 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.

**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.

TABLO II. İLÇELERE GÖRE KABLOSUZ AĞ ÖZELLİKLERİ

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

### Veri Görselleştirme Modülü

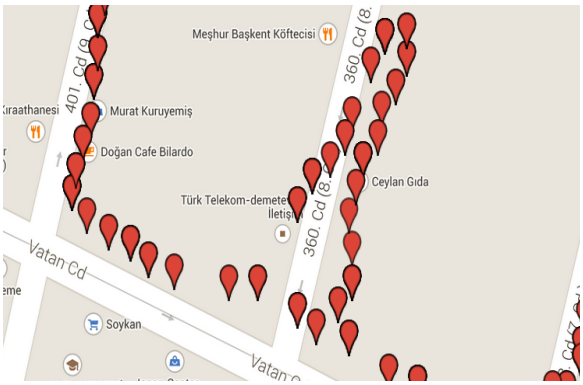
Ayıklanan ve kategorize edilen veriler görselleştirme modülü ile grafikler üzerinde anlaşılır hale getirilir. Buna ek olarak, Veri Toplama Modülünde oluşturulan harita taslağı işlenen veriler ve bu verilerin sahip oldukları GPS koordinatlarıyla beraber kullanılarak Resim 1'de verildiği gibi tamamlanır. Test edilen yerler Google Maps üzerinde otomatik olarak işaretlenmiştir.

### 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 aşağıda verildiği Kablosuz Farkındalık Puanı (KFP) şekilde hesaplanır.

$$KFP = (\%WPS + \%SSID_D + \%WPA2) / 3 \quad (1)$$

Sonraki bölümde, bu çalışma kapsamında elde edilen Kablosuz Farkındalık Puanı değerleri ile sonuçlar sunulmuştur.




Resim 1: Tamamlanmış bir harita taslağı.

## IV. DENEYSEL SONUÇLAR (EXPERIMENTAL RESULTS)

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

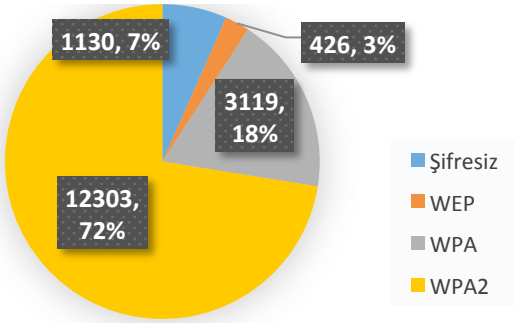
Alan çalışması kapsamında Ankara'da uygulanan yöntem ve yaklaşım ile mesken çeşitliği dikkate alınarak çeşitli güzergâhlardaki kablosuz ağ cihazlarına ait bilgiler toplanmıştır.

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 adedi WPA2, 3.119 adedi WPA, 426 adedi WEP güvenliğine sahipken 1130 adedi güvenliği olmayan ve herkes tarafından erişebilir konumda ağ cihazı olarak bulunmaktadır.

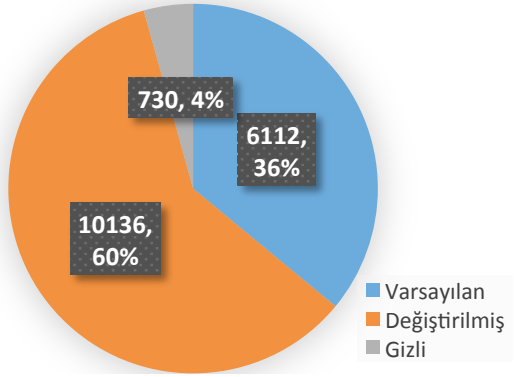
Bu ağların 10.136 adedinin varsayılan (default) haldeki SSID'leri değiştirilmişken, 6.112 cihazın SSID'leri varsayılan olarak bırakılmıştır. Bu verilere ek olarak 730 adedi de SSID'si gizlenmiş ağ tespit edilmiştir. Bu ağların 7.320'sinde WPS bulunurken 9.658 ağda WPS'ye rastlanılmamıştır. 16.978 ağın 16.570'i 2GHz frekansında, 408 adedi de 5GHz frekansında yayın yapmaktadır. Araştırma kapsamında bulunan bütün kablosuz cihazların yasal aralık dahilinde [20] yayın yaptıkları tespit edilmiştir. Bu araştırma ile elde edilen verilere ait kıyaslama görselleri Şekil 2-7'de sunulmuştur.

Şekil 2'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 ağlardaki şifreleme türleri




Şekil 3. Kablosuz ağların SSID türü

SSID, her modemin kendini kullanıcıya tanıtmak için kullandığı maksimum 32 alfanümerik karakterden oluşabilen isimdir.

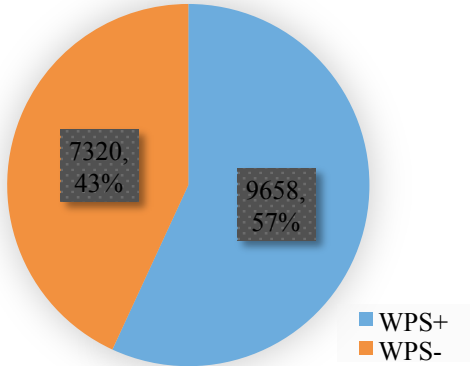
SSID, kullanıcının isteğine göre değiştirilebilir veya gizli hale getirilebilir. SSID'nin varsayılan olarak bırakılması, modemi çeşitli saldırılara açık hale getirebilmektedir [21]. Şekil 3'de araştırmaya katılan ağ cihazlarının SSID isimlerine ait karşılaştırmalar sunulmaktadır.

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].

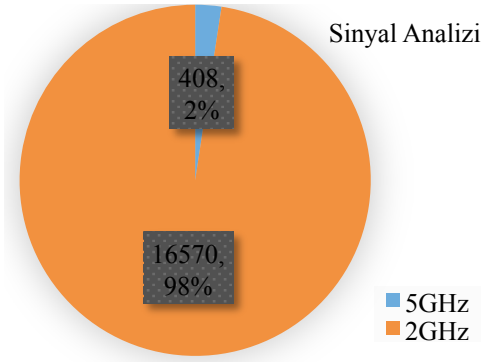
Şekil 4'te araştırmaya katılan ağ cihazlarının SSID isimlerine ait karşılaştırmalar sunulmaktadır.

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 5'te araştırmaya katılan ağ cihazlarının frekans bant karşılaştırmaları sunulmaktadır.

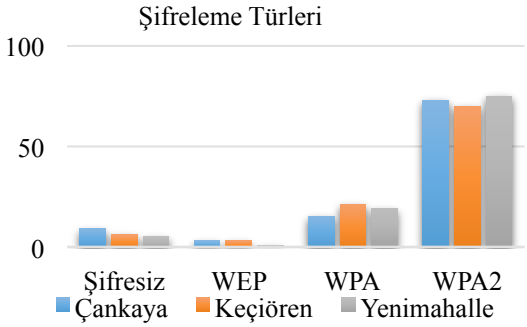
Şekil 6'daki verilere bakıldığı zaman yerleşimi hem işyeri hem mesken ağırlıklı olan Çankaya semtindeki şifrelemesi olmayan kablosuz oranı mesken ağırlıklı yerleşim yerleri olan Keçiören ve Yenimahalle'ye göre daha fazla olduğu tespit edilmiştir. Bunun en büyük sebebi çoğu kurumsal ağların müşteri ihtiyaçları doğrultusunda şifresiz sunulması olduğu düşünülmektedir.




Şekil 4. Kablosuz ağ cihazlarının WPS analizi




Şekil 5. Kablosuz ağ cihazlarının yayın frekansı




Şekil 6. İlçelere göre kablosuz ağ şifreleme türleri

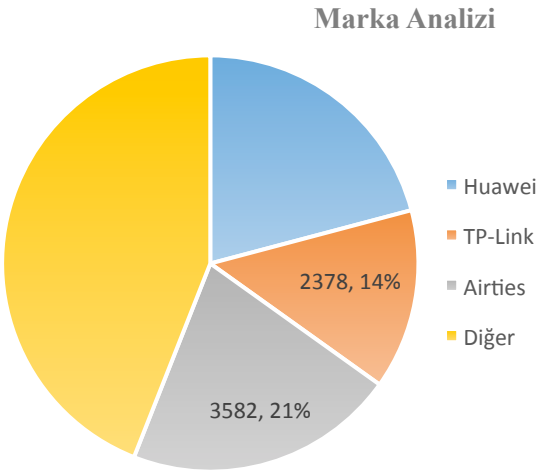
TABLO III. EN UZUN VE EN KISA 10 SSID

| **En Uzun 10 SSID** | **Uzunluk** |
|---|---|
| Anca internetini ac dersin zaten | 32 |
| Turkcell BlackBerry Hotspot 4451 | 32 |
| www.icgiyimkolik.com>0312*****63 | 32 |
| ANKARAGUCU_DUSTU_SEKER_ 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 |

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** | **Şifresiz** | 9 | 6 | 5 |
| **Türü** | **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 |
| **Orta öğretim Üzeri Eğitim Durumu** | **Lise + Üniversite** | **73** | **49** | **59** |

| **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 |




Şekil 7. Kablosuz ağ cihazlarının marka analizleri

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

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 (DISCUSSION)

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.

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 16.978 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.
- Kablosuz ağ cihaz güvenliğinin sağlanmasında sosyoekonomik kriterlerin önemli olduğu ve halkın bilgi güvenliği farkındalığı kazanmasında gelir ve eğitim düzeyi arasında ilişki olduğu gösterilmiştir.
- Genel olarak değerlendirildiğinde, ülkemizde bilgi güvenliği farkındalığının pek çok kaynakta da ifade edildiği gibi düşük olduğunu belirtmekte fayda vardır.
- Bilgi güvenliği farkındalığını artırmanın yolunun aslında sosyoekonomik durumları iyileştirmeden geçtiği de unutulmamalıdır.

## VII. KAYNAKLAR

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

**[2].** Y. Zhang, Y. Xiao, K. Ghaboosi, J. Zhang and H. I. Deng , A survey of cyber crimes, 2011.

**[3].** Y. Rezgui, A. Marks, Information security awareness in higher education: An exploratory study, 2008.

**[4].** K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, C. Jerram, Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q), 2014.

**[5].** D. L. Huangan, P. L. P. Raua, G. Salvendy, F. Gaoa, J. 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].** J. Holvast, History of Privacy, 2009.

**[8].** H. A. Fatani, I. F. Zamzami, M. Aydin and M. Aliyu, Awareness Toward Wireless Security Policy:Case Study of International Islamic University, 2013.

**[9].** H. Said, M. Guimaraes, N. Al Mutawa, I. Al Awadhi, Forensics and War-Driving on Unsecured Wireless Network, 2011.

**[10].** R. Shukla, S. S. Kolahi, R. Freeth and A. Kumar, Educational Institutes: Wireless Network Standards Security and Future, 2010.

**[11].** B. D. Cone, C. E. Irvine, M. F. Thompson, T. D. Nguyen, A video game for cyber security training and awareness, 2006.

**[12].** *Ajan 4141. [Online]*. HRİKa Çözümler, 2009.

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

**[14].** D. G. Tarragó, Home Wireless Security and Privacy: A Practical Protocol Mixing, 2010.

**[15].** T. 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

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

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

**[18].** N. Borisov, I. Goldberg, D. Wagner. (2015-4-2) [Online]. Available: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

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

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

**[21].** S. Young, D. Aitel, The Hacker's Handbook: The Strategy Behind Breaking into and Defending Networks, 2003, pp. 588-589.

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

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