©2020 Published in 8th International Symposium on Innovative Technologies in Engineering and Science 23-25 October 2020 (ISITES2020 Bursa - Turkey)
https://doi.org/10.33793/acperpro.03.01.118

Nesnelerin interneti teknolojileri kullanılarak Wi-Fi MAC Adresi tabanlı insan toplulukları izleme ve analiz sistemi

Crowd monitoring and analysis system based on Wi-Fi MAC Address and Internet of Things technologies

*[1]Turgay Tugay Bilgin ve [2]Recep Tayyib Aksakal
*[1] Bursa Teknik Üniversitesi, Mühendislik ve Doğa Bil. Fakültesi, Bilgisayar Mühendisliği Bölümü, Bursa, Türkiye
[2]Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği Bölümü, Elazığ, Türkiye

Özet

Bu çalışmada, belirli bir konumdan geçen insan topluluklarının hareketlilik analizini yapmayı sağlayacak bir system geliştirilmiştir. Bu çalışmada, amaç belirli bir lokasyondaki insan trafiğini ve yoğunluğunu tespit edebilmektir. Bu amacı, KVKK sınırlamalarını aşmadan Wi-Fi paketlerini yakalayarak ve analiz ederek gerçekleştirdik. ESP8266 mikrokontrol kartı kullanılarak kapsama alanındaki Wi-Fi (Wireless Fidelity) trafiği dinlenmiştir. Yakalanan IEEE 802.11 paketlerinin MAC (Media Access Control) header kısmı alınarak, ortamdaki AP (Access Point) cihazlar ve STA (Station) cihazlar belirlenmiştir. Belirlenen STA cihazların MAC adresleri bir Wi-Fi ağına bağlanılarak Bulut Tabanlı API'ye (Application Programming Interface) gönderilmiş ve donanım üreticisi (vendor) tespiti yapılarak veritabanına kaydedilmiştir. Geliştirilen yönetim paneli sayesinde belirli bir konumdan geçen kalabalıklar Günlük, Haftalık, Aylık veya girilen zaman dilimine bağlı olarak analiz edilebilmektedir. Ayrıca Cihaz Sayısı/Vendor ve Cihaz Sayısı/Zaman grafikleri de çizdirilmiştir.

Anahtar Kelimeler: Nesnelerin Interneti, Topluluk İzleme, Wi-Fi ile veri toplama.

Abstract

In this study, a system has been developed to analyze mobility of human populations that walks through a certain location. In this study, the aim is to detect the human traffic and density in a specific location. We achieved this goal by capturing and analyzing Wi-Fi packets without exceeding the GDPR limitations. Using the ESP8266 microcontroller card, the Wi-Fi (Wireless Fidelity) traffic in the coverage area was monitored. By collecting the MAC (Media Access Control) header part of the captured IEEE 802.11 packets, AP (Access Point) devices and STA (Station) devices in the environment were determined. The MAC addresses of the determined STA devices were stored and sent to the Cloud-Based API (Application Programming Interface) over a Wi-Fi network. The vendor of the hardware was also identified and stored in the database. Thanks to the developed management panel, crowds walking over a certain location can be analyzed based on Daily, Weekly, Monthly or between the specific interval. Also, Device Number / Vendor and Device Number / Time graphs were plotted.

Key words: Internet of Things, Crowd Monitoring, Wi-Fi Sniffing

1. Giriş

Belirli konumlarda, örneğin dükkan önü, toplanma alanları, avm içi gibi insan trafiğinin ve yoğunluğunun doğru tespiti önemli bir problemdir. Bunu için literatürde birçok yöntem mevcuttur. Bunlardan ilk akla geleni bir kamera aracılığıyla, çeşitli görüntü işleme metotları kullanılarak

*Corresponding author: Address: Bursa Technical University, Department of Computer Engineering, Yıldırım, BURSA, TURKEY. E-mail address: turgay.bilgin@btu.edu.tr

kişilerin tespit edilmesidir [1]. Bu yöntem hukuksal olarak incelendiğinde KVKK'ya aykırı olabildiği göze çarpmaktadır [2]. Bu makalede önerdiğimiz yöntemde ortamdaki cep telefonlarının yayınladığı Wi-Fi paketlerinin yakalanarak, paketlerde yer alan "MAC header" bölümünden cihazların MAC (Media Access Control) adreslerinin ayıklanarak veri olarak işlenmesi önerilmektedir. Bu veriyi cihaz zaten kendisi yayınladığı için kişisel verilen gizliliğine dair herhangi bir engel söz konusu olmamaktadır. Bu bilgi ile kişi/cihaz sayısı tespiti de gerçekleştirilebilmektedir.

Bu çalışma kavramsal tasarımın ispatı (proof of concept) olup, 2.4 GHz bandındaki Wi-Fi paketlerini dinleme üzerine kuruludur. Daha yüksek bandlardaki paketlerin dinlenmesiyle daha çeşitli cihaz bilgileri de elde edilebilir. Örneğin, 4G cihazlar için 2-8 GHz band aralığındaki paketler incelenebilir.

2. Materyal ve Metod

802.11 paket yapısı incelendiğinde bir çok farklı bölümden oluştuğu görülmektedir [3]. Cihaz sayısının tespit edilebilmesi için tekil (unique) bilgi olan MAC adresinin kullanılması hedeflenmiştir. Yakalanan 802.11 paketinden MAC adresinin elde edilebilmesi için birkaç ayrıştırma işlemi gerekmektedir. Öncelikle yakalanan 802.11 paketinden MAC header bölümü ayrıştırılmıştır. Sonrasında ise MAC header bölümünden de Transmitter MAC Adress bilgisi ayrıştırılmıştır.

Ortamdaki cihazların tespit edilebilmesi için cihazın 2.4 GHz bandında 802.11 paketlerini o anda kullanıyor olması gerekmektedir [4]. Cihaz tespiti iki farklı şekilde yapılabilmektedir. Bunlardan ilki cihazın bir Wi-Fi ağına bağlı olması dolayısıyla 802.11 paketlerini kullanıyor olmasıdır. İkinci yol ise cihazda herhangi bir ağa bağlı olmasa bile Wi-Fi özelliğinin açık olması durumunda cihazın yaptığı Probe Request'ler dolayısıyla 802.11 paketlerini kullanması sonucudur [4].

Cihazlarda Wi-Fi özelliğinin kapalı olması durumunda veya Wi-Fi özelliği açık olmasına rağmen cihazda kayıtlı ağ yoksa yani Probe Request yapmıyorsa yada herhangi bir Wi-Fi ağına bağlı değilse cihaz tespit edilememektedir.

2.1 Gömülü Sistem Tasarımı

Ortamdaki Wi-Fi trafiğinin dinlenebilmesi için NodeMCU LoLin ESP8266 CP2102 geliştirme kartı kullanılmıştır [5]. Yakalanan paketler için zaman damgası (timestamp) üretilebilmesi için DS1302 RTC modülü kullanılmıştır [6]. Ayrıca yakalanan paketlerden ayrıştırılan MAC bilgisi ile zaman damgası bilgisinin düz metin dosyaya depolanması ve sonrasında Bulut tabanlı API'ye yollanabilmesi için SD Card modülü kullanılmıştır. Devre şeması Şekil 1'de görülmektedir.

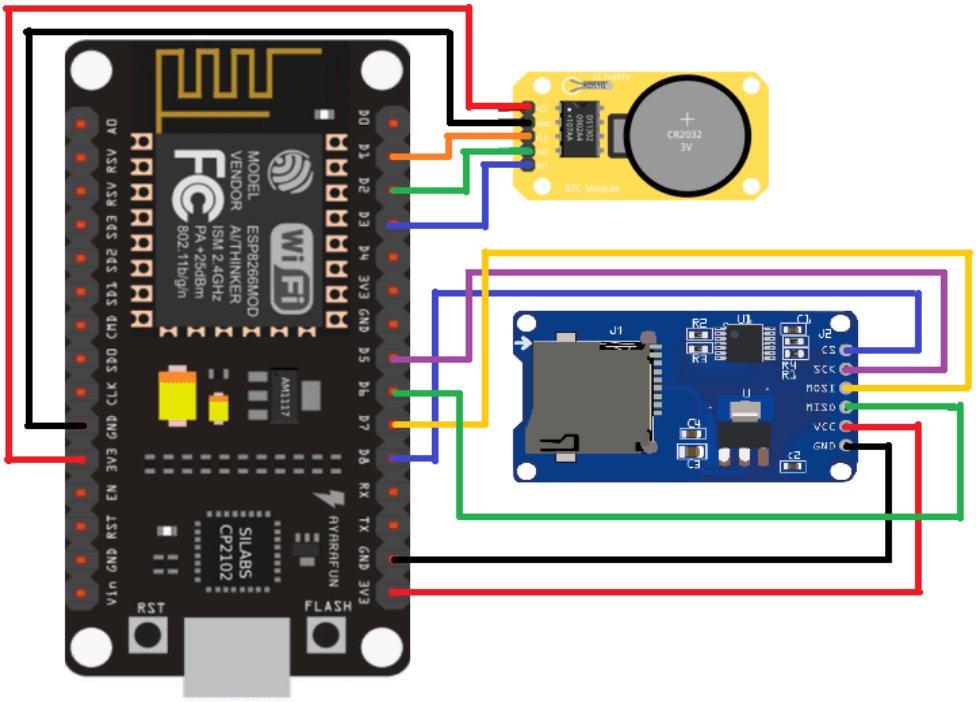
2.1.1 ESP8266

Espressif System firması tarafından geliştirilen, TCP/IP yığınına sahip, çeşitli Wi-Fi IoT modüllerinin üzerinde yer alan SoC(System-On-Chip) olan çiptir. İlk defa 2014 yılında 3.parti olarak AI-Thinker tarafından ESP8266-01'den ESP8266-14'e kadar çeşitli modeller üretilmiştir.

Bu çip için geliştirilmiş bir çok modül ve açık kaynak yazılım mevcuttur [7]. Bu modüller oldukça ekonomik olmakla birlikte, boyutları, ebatları da oldukça küçüktür ve düşük güç tüketimine sahiptir[8]. Temel özellikleriyle ekstra bir mikroişlemciye gerek dahi duymadan birçok şey yapabilmektedir.

ESP8266 çok geniş bir kullanım alanına sahiptir. Akıllı ev uygulamaları, endüstriyel kablosuz kontrol üniteleri, ip kameralar, giyilebilir teknolojiler gibi daha birçok alanda karşımıza çıkmaktadır.

ESP8266 STA, AP veya STA+AP modlarına sahiptir. Bu modülü kullanırken bu modlar ile kullanıcıya çok geniş bir alan sunmaktadır. STA modu ile bir ağa bağlanarak internete erişilebilir, web sunuculardan çeşitli isteklerde bulunulabilir veya sensörlerden okunan değerler bulut tabanlı depolama ortamlarına aktarılabilir. AP modu ile bir erişim noktası oluşturabilir ve başka modüller ile veya cihazlar ile bağlanarak çeşitli komutlar gönderebilir bununla birlikte bir dizi olayı tetikleyebilirsiniz.[9]

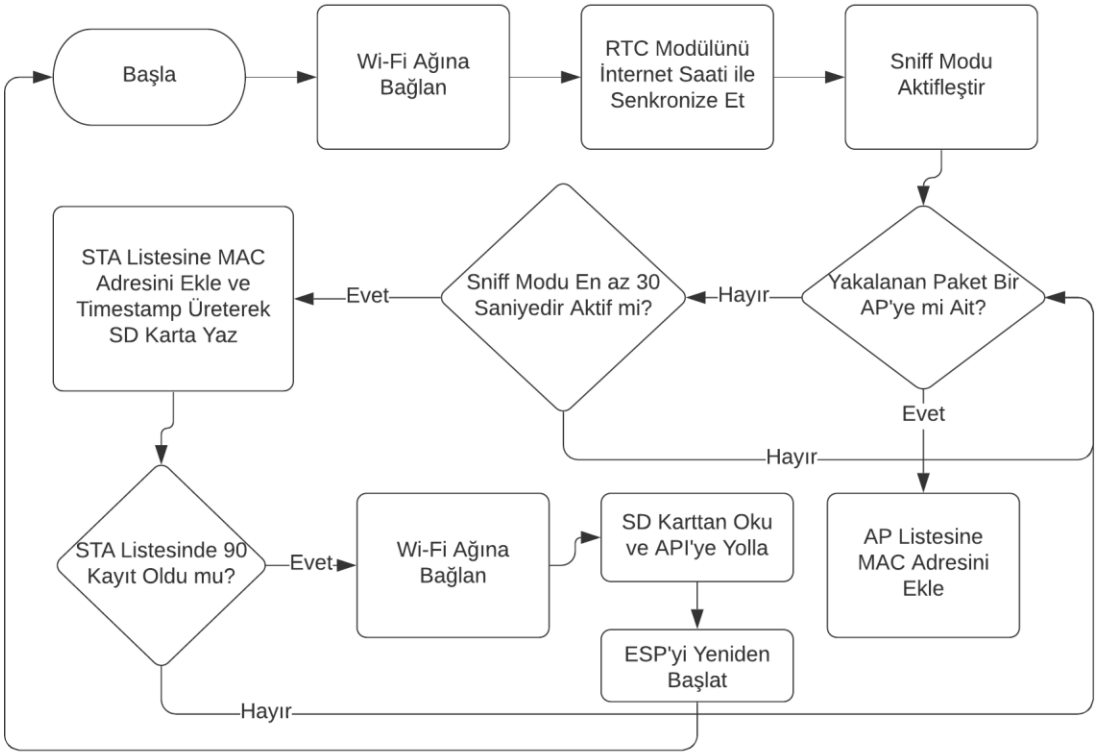


Şekil 1. Devre Şeması

2.2 Gömülü Sistem Yazılımı

Geniş bir literatür taraması yapılarak ESP8266 tabanlı çeşitli Wi-Fi sniffer örnekleri incelenmiş ve test edilmiştir. Bu örneklerden, GitHub üzerinde "esp8266-simple-sniffer" adlı reponun hız, stabilite ve performans açısından uygun olduğu görülmüştür [10]. Bu repo temel alınarak kendi

kodlarımız geliştirilmiş ve üzerinde çeşitli geliştirmeler yapılmıştır. Bu proje kapsamında geliştirilen Gömülü yazılım kodlarına GitHub üzerinden erişilebilir. [11]



Şekil 2. Gömülü Sistem Akış Diyagramı

Şekil 2'de bu proje kapsamında geliştirdiğimiz gömülü yazılımın akış diyagramı verilmiştir.

2.3 Web Platformu

MAC ve zaman damgası verilerinin gömülü yazılım üzerinden Bulut ortamına gönderilebilmesi için Python tabanlı bir Web Servisi kütüphanesi olan Flask kullanılmıştır. Gömülü yazılım ile bulut ortamının haberleşmesi için Flask kullanılarak bir API yazılmıştır. Ayrıca API ile alınan verilerden oluşturulan grafiklerin gösterilebilmesi için yine Flask ile bir görselleştirme paneli (dashboard) yazılmıştır.

2.3.1 Flask Web Servisi Sunucusu

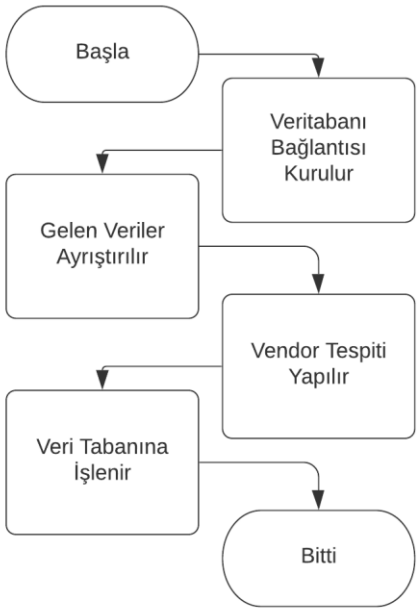
Flask, Werkzueg ve Jinja 2 tabanlı olup geliştiricilere sadece temel öğeleri veren ve ihtiyaç doğrultusunda paketler eklenebilen, ihtiyaç kadar geliştirebilen bir Python Web Uygulama çatısıdır (Python Web Framework). Flask ile mikro servisler yazabilir, web projeleri

gerçekleştirebilir ve bu sayede farklı platformlar arası ve bulut ortamı arası haberleşme çok hızlı bir şekilde gerçekleştirilebilir.

2.3.2 Uygulama Programlama Arayüzü (API)

Uygulama Programlama Arayüzü (Application Programming Interface), bir uygulamanın işlevlerine dışarıdan veya uzaktan erişilip bu işlevlerin kullanılmasına olanak sağlayan arayüzdür. API, bir sunucunun üzerindeki uygulamaya farklı platformlardan ulaşılmasını ve sunucuda işlenen verinin cevap olarak çağıran uygulamaya döndürülmesine olanak sağlar.

ESP8266 tarafından toplanan her MAC adresi anında sunucuya gönderilmez. Anında gönderme internet bağlantısını fazladan kullanmaya ve gömülü sistemin enerji tüketimine olumsuz etki yapmaktadır. Bu sebeple gömülü sistem 90 adet MAC adresi toplandığında veriler API'ye gönderilmektedir. API'ye gelen veriler ayrıştırılır ve donanım üreticisi (vendor) tespiti de yapılarak daha sonrasında görselleştirme ve loglama amacıyla veritabanına kaydedilir. API üzerinde gerçekleşen işlemlerin akış diyagramı Şekil 3'de verilmiştir.

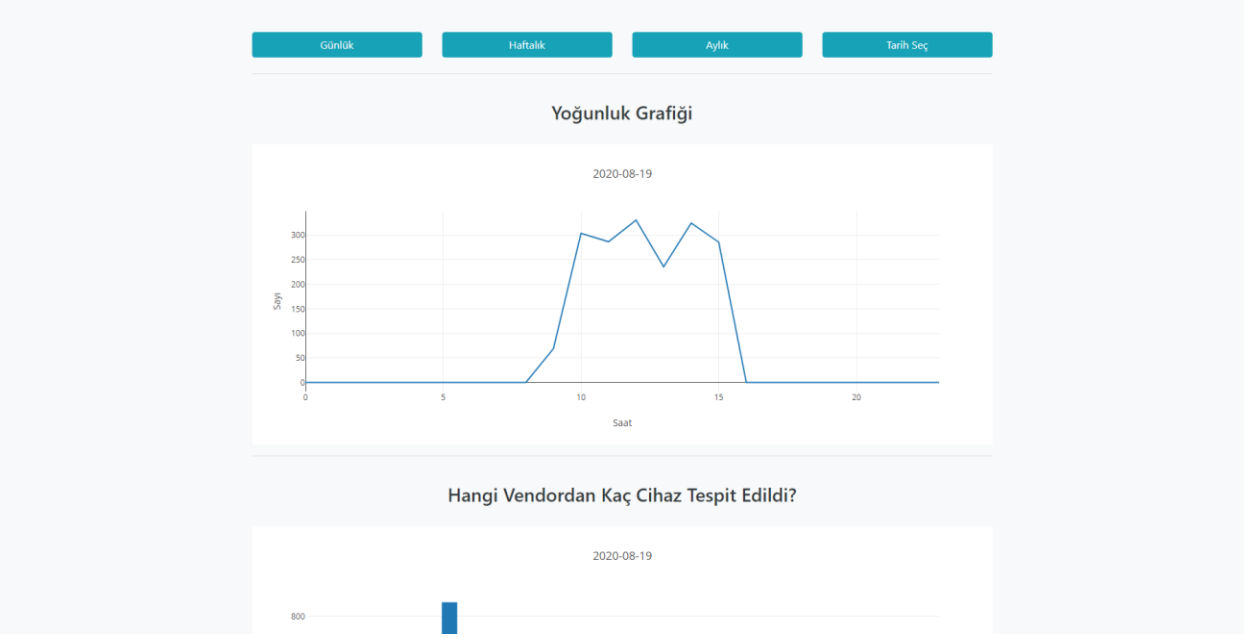


Şekil 3. API işlemleri akış diyagramı

2.3.3. Web Tabanlı Kontrol Paneli

Bu adımdan önceki adımlarda, ESP8266 ile tespit edilen MAC adresleri zaman damgası bilgileri ile birlikte API'ye aktarılmış ve donanım üreticisi tespiti de yapılarak veri tabanına kaydedilmişti.

Elde yer alan bu 3 bilgi ile 2 farklı grafik üretecek bir web tabanlı grafik çizdirme yazılımı geliştirilmiştir. Bu grafikler ve zaman filtrelemesi bir panel aracılığıyla kullanıcıya sunulmaktadır.

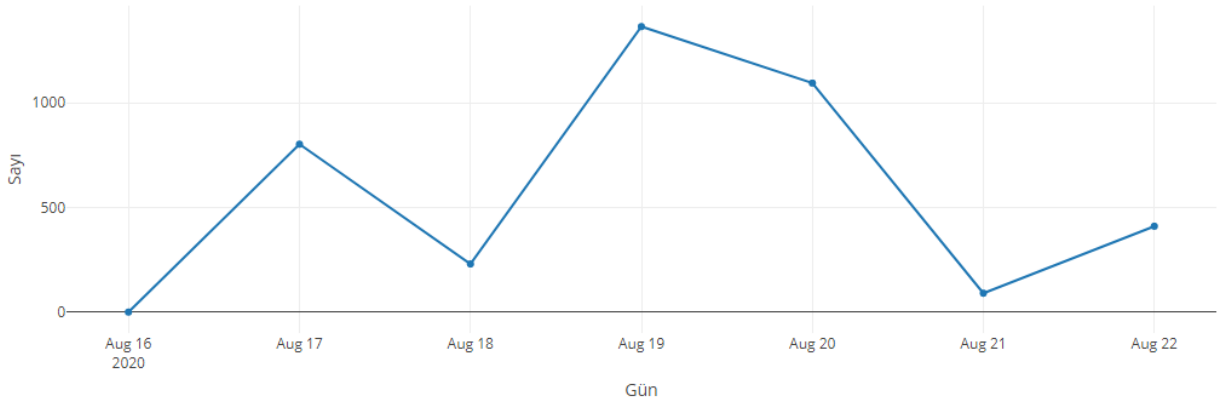


Şekil 4. Web tabanlı kontrol paneli ekran görüntüsü

Üretilen grafikler:

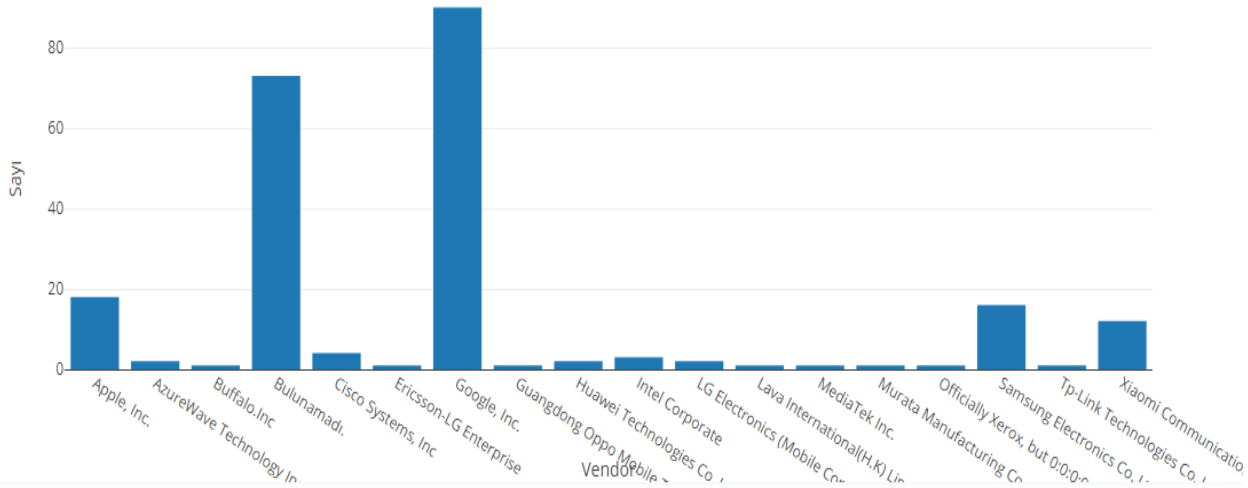
- Yoğunluk Grafiği,
- Cihaz Sayısı Vendor Dağılımı Grafiği

olarak iki çeşittir.



Şekil 5. Yoğunluk (seçilen zaman aralığında tespit edilen tekil MAC sayısı) Grafiği

Kontrol panelinde yer alan butonlar aracılığıyla "Günlük" butonu seçildiğinde; geçerli günün yoğunluk grafiği (seçilen zaman aralığında tespit edilen tekil MAC sayısı) (Şekil 5) ve cihaz sayısı vendor dağılımı grafiği (Şekil 6), "Haftalık" veya "Aylık" seçildiğinde; son 1 haftanın veya son 1 ayın yoğunluk grafiği ve cihaz sayısı vendor dağılımı grafiği ekrana çizdirilmektedir. Ayrıca kullanıcı özel tarih aralığı girebilmekte veya özel bir günü seçip bu tarih aralığına veya güne ait grafikleri de görebilmektedir.



Şekil 6. Donanım üreticilerine göre cihaz sayısı grafiği

3. Sonuçlar ve Tartışma

Günümüzde açık alanda hareket etmekte olan hemen hemen tüm insanlarda internet erişimine sahip telefonlar bulunmaktadır. Herhangi bir konumdaki insan yoğunluğu, bu telefonlardan ortama yayılan paketler yakalanarak tespit edilebilmektedir. Bu çalışmada, amaç belirli bir lokasyondaki insan trafiğini ve yoğunluğunu tespit edebilmektir. Bu amacı, KVKK sınırlamalarını aşmadan Wi-Fi paketlerini yakalayarak ve analiz ederek gerçekleştirdik. Benzer şekilde, daha yüksek frekans bandlarında dinleme yapılarak GSM operatörlerinin telefonlara sağladığı internet erişimi dinlenebilir, paketler yakalanabilir ve çeşitli tespitler yapılabilir.

Bu çalışma ticari ürün haline getirilerek farklı amaçlar için kullanılabilir. Örnek verecek olursak, şirket içi ERP/CRM sistemlerine entegre edilerek, şirketin kapsam haritasını çıkartıp tüm şirketi kapsayacak şekilde belirli noktalara konumlandırabilir ve şirket içerisinde kablosuz iletişim kuran yabancı cihazların tespiti gerçekleştirilebilir. Başka bir örnek verecek olursak şirket/fabrika içerisinde kapsam haritasına göre belirli noktalara yerleştirilerek hangi cihazdan hangi saatlerde ne kadar paket giriş-çıkışı oldu gibi analizler yapılarak, çalışanların performansı ölçülebilir.

Başka bir örnek ise okullarda veya mobil cihazların yasak olduğu alanlarda cihaz tespiti amacıyla kullanılabilir. Benzer şekilde yine okullarda veya şirketlerde öğrencilerin/çalışanların giriş çıkış

saatleri gibi bilgi çıkarımları yapılarak yoklama sistemlerinde kullanılabilir. Sonuç olarak, bu çalışma geliştirilmeye açık ve birçok alanda kullanılabilecek ürünlerin, fikirlerin doğmasını tetikleyebilecek nitelikte bir çalışmadır.

Referanslar

[1] Morerio, P., Marcenaro, L., & Regazzoni, C. S. (2012, September). People count estimation in small crowds. In *2012 IEEE Ninth International Conference on Advanced Video and Signal-Based Surveillance* (pp. 476-480). IEEE.

[2] Momen, N., Hatamian, M., & Fritsch, L. (2019). Did App privacy improve after the GDPR?. *IEEE Security & Privacy*, *17*(6), 10-20.

[3] Friess, K. (2018, July). Multichannel-Sniffing-System for Real-World Analysing of Wi-Fi-Packets. In *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)* (pp. 358-364). IEEE.

[4] Natarajan, R., Zand, P., & Nabi, M. (2016, October). Analysis of coexistence between IEEE 802.15. 4, BLE and IEEE 802.11 in the 2.4 GHz ISM band. In *IECON 2016-42nd Annual Conference of the IEEE Industrial Electronics Society* (pp. 6025-6032). IEEE.

[5] Al Dahoud, A., & Fezari, M. (2018). NodeMCU V3 For Fast IoT Application Development.

[6] DS1302 Trickle-Charge Timekeeping Chip https://datasheets. maximintegrated.com/en/ds/DS1302.pdf

[7] Brian Benchoff (Ağustos 26, 2014). "New Chip Alert: The ESP8266 WiFi Module (It's $5)". Hackaday.

[8] Brian Benchoff (Eylül 6, 2014). "The Current State of ESP8266 Development". Hackaday.

[9] Soft Access Point, https://arduino-esp8266.readthedocs.io/en/latest/esp8266wifi/soft-access-point-examples.html

[10] esp8266-simple-sniffer https://github.com/n0w/esp8266-simple-sniffer

[11] ESP-MAC https://github.com/orange-beard/ESP-MAC