Nevşehir Bilim ve Teknoloji Dergisi

dergi web sayfası: http://dergipark.gov.tr/nevbiltek

Makale Doi: **10.17100/nevbiltek.557886**

Geliş tarihi: 25.04.2019 Kabul tarihi: 04.09.2019

The Attack Methodology to Wireless Domains of Things in Industry 4.0

Ahmet Ali SÜZEN[1*], Mehmet Ali ŞİMŞEK[2], Remzi GÜRFİDAN[3], Kıyas KAYAALP[4]

[1]Isparta University of Applied Sciences, Cyber Security Application and Research Center, Isparta/Turkey
ORCID ID: 0000-0002-5871-1652

[2] Tekirdağ Namık Kemal University, Vocational School of Technical Sciences, Department of Computer Technologies, Tekirdağ/Turkey
ORCID ID: 0000-0002-6127-2195

[3]Isparta University of Applied Sciences, Yalvaç Vocational School of Technical Sciences, Department of Computer Technologies, Isparta/Turkey
ORCID ID: 0000-0002-4899-2219

[4]Isparta University of Applied Sciences, Uluborlu Selahattin Karasoy Vocational School, Department of Computer Technologies, Isparta/Turkey
ORCID ID: 0000-0002-6483-1124

Abstract

In this study, the vulnerability tests were carried out through the techniques of penetration, crack and impersonation the wireless network connections in which the thing in the industry 4.0 was communicating. The MAC addresses of all the devices by the penetration technique has been seen in the network identified. The device is dropped from the network using de-auth attacks with MAC address. As a result of this, the operation of Industrial 4.0 systems is interrupted or stopped. It is possible to predict the standard passwords of the distributors with WPS feature turned on by means of cracking techniques and to penetration the wireless network or to disable the network. In the end, it can be seen that the existing data can be deleted or collected by adding a new device to the system with the fake technique of the wireless network. The results showed that WEP, WPA, and WPA2 security were not sufficiently used in the wireless network. As a result of the penetration methodology, it was determined that the use of wireless networks would not be a solution in the connections where data security was high in Industry 4.0.

Keywords: Cyber Attack, Industry 4.0, Internet of Things, Wireless Network.

Endüstri 4.0’da Nesnelerin Kablosuz Etki Alanlarına Yapılan Saldırı Metodolojisi

Öz

Bu çalışmada Endüstri 4.0 içerisinde yer alan nesnelerin iletişim kurdukları kablosuz ağ bağlantılarının sızma, kırma ve taklit etme teknikleri uygulanarak zafiyet testleri yapılmıştır. Sızma tekniği ile tespit edilen ağdaki tüm cihazların MAC adreslerine erişim sağlanmaktadır. MAC adresi üzerinden de-auth atakları ile cihazlar ağdan düşürülmektedir. Bunun sonucunda Endüstri 4.0 sistemlerinin çalışmasının kesintiye uğradığı veya belirli bir süre durduğu görülmektedir. Kırma teknikleri ile WPS özelliği açık olan dağıtıcıların standart şifreleri tahmin edilerek kablosuz ağa sızmanın veya ağı devre dışı bırakmanın gerçekleştiği görülmektedir. Son olarak kablosuz ağda, oturum taklit etme tekniği ile sisteme yeni bir cihaz ekleyip var olan verilerin silinebileceği veya toplanabileceği görülmektedir. Elde edilen sonuçlar ile kablosuz ağda kullanılan WEP, WPA ve WPA2 güvenliklerinin kendi başlarına yeterli olmadığı görülmüştür. Yapılan sızma metodolojisi ile Endüstri 4.0 sistemlerinde veri güvenliğinin üst düzey olacağı bağlantılarda kablosuz ağ kullanımının çözüm olmayacağı tespit edilmiştir.

Anahtar Kelimeler: Endüstri 4.0, Kablosuz Ağ, Nesnelerin İnterneti, Siber Güvenlik.

Corresponding Author e-mail: ahmetsuzen@isparta.edu.tr

1. Introduction

At First; Industry 1.0 with the invention of steam engines [1], Industry 2.0 with electrically operated and mass-produced devices [2] and interaction of computers with robots in production has revealed Industry 3.0 [3]. The Industrial Revolution in the last and fourth stage of the so-called Industry 4.0 which artificial intelligence, along with the Internet of Objects (IoT) and big data concepts, is the smart production period that minimizes human impact in production. Basically, Industry 4.0 is based on interoperability, virtualization, independent management, modularity and real-time principles [4].

The IoT, which is emerging from the requirements of the smart society and Industry 4.0, is to manage the devices through the network. Devices connected to the Internet are controlled remotely and perform certain tasks or processes. [5]. The IoT devices are rapidly increasing in an uncontrolled manner with the increase in the needs of the society. The result of this, it has been increasing cyber vulnerabilities [6].

In this study, cyber-attacks on wireless networks of thing within the Industry 4.0 space and its resulting effects are described through a sample model. Developed scenarios in different security levels within the thing space designed. Different attacks have been made for each scenario of the model and their effects have been observed. In the world of rapidly growing things, there is no precaution against cyber-attacks. In a result of this, it has been loss data, time and money. This study aims to show and fix the negative effects of cyber-attacks on wireless networks.

2. Wireless Networks

Wifi, known as wireless networks, is actually a radio communication standard developed by the IEEE as 802.11 in 1997. The 802.11 wireless LAN standard has become inadequate with the emerging technology and 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac standards have been developed [7]. The technical specifications of the standards published by the IEEE are shown in Table 1.

Table 1. Technical specifications of wireless network standards.

IEEE Std.	Frequency	Max Data Rate	Avg Data Rate	Channel Width	Range
802.11a	5 GHz	54 Mbps	27 Mbps	20 Mhz	100 m
802.11b	2.4 GHz	11 Mbps	5 Mbps	22 Mhz	150 m
802.11g	2.4 GHz	54 Mbps	22 Mbps	20 Mhz	150 m
802.11n	2.4 /5 GHz	600 Mbps	300 Mbps	20 /40 Mhz	250 m
802.11ac	5 GHz	1.3 Gbps	450 Mbps	20 /40/ 80/160 Mhz	250m >

Security is provided with the standards developed in wireless network connections. In network devices, different encryption systems have been implemented for the safety of wireless networks from the early years to the present. The encryption standards used for wireless networks are shown with technical specifications in Table 2.

Table 2. Authentication methods used in wireless networks.

Method	Authentication	Encryption Algorithm
WEP	Open/Shared Key	RC4(24 bit)
WPA Personal	Pre-shared Key (PSK)	RC4(48 bit)
WPA2 Personal	Pre-shared Key (PSK)	AES
WPA Enterprise	802.1x	RC4(48 bit)
WPA2 Enterprise	802.1x	AES
WPA3 Personal	Simultaneous Authentication of Equals (SAE)	128-bit
WPA3 Enterprise	Simultaneous Authentication of Equals (SAE)	192-bit

3. Internet of Things (IoT)

The Internet of things is smart and manageable devices connected to each other via networks. It is used in many areas ranging from household appliances to industry in Industry 4.0 and smart society concepts [8]. Communication technologies used to connect their devices and their standards are given in Table 3. These communication technologies are often used in the data binding layer, the network layer, the communication layer, and the application layer [9].

Table 3. Communication Technologies of IoT Devices.

Communication	Standard
WiFi	IEEE 802.11 a/c/b/ d/g/n
WiMAX	IEEE 802.16
LR-WPAN	IEEE 802.15.4 (ZigBee)
Mobil İletişim	2G-GSM, CDMA 3G-UMTS,CDMA2000 4G-LTE
Bluetooth	IEEE 802.15.1
Lora	LoRaWAN R1.0

4. Background

4.1. Case of Model

A wireless model was created as shown in Figure 1, which performs production and analysis on the data for the realization of the study. In this model, three development cards (Arduino Uno, Raspberry Pi 3, Latte Panda) were used for the Internet of objects. The wireless network configuration of the development cards used has been set. All development cards have been fitted distance, RF and temperature sensors for the creation of the test environment. However, the model that collects data from the external environment and transfers data via the wireless network is established. Data read from the environmental environment is recorded in the Google Firebase database on the cloud server via the wireless gateway. This data is transmitted at intervals of a second.

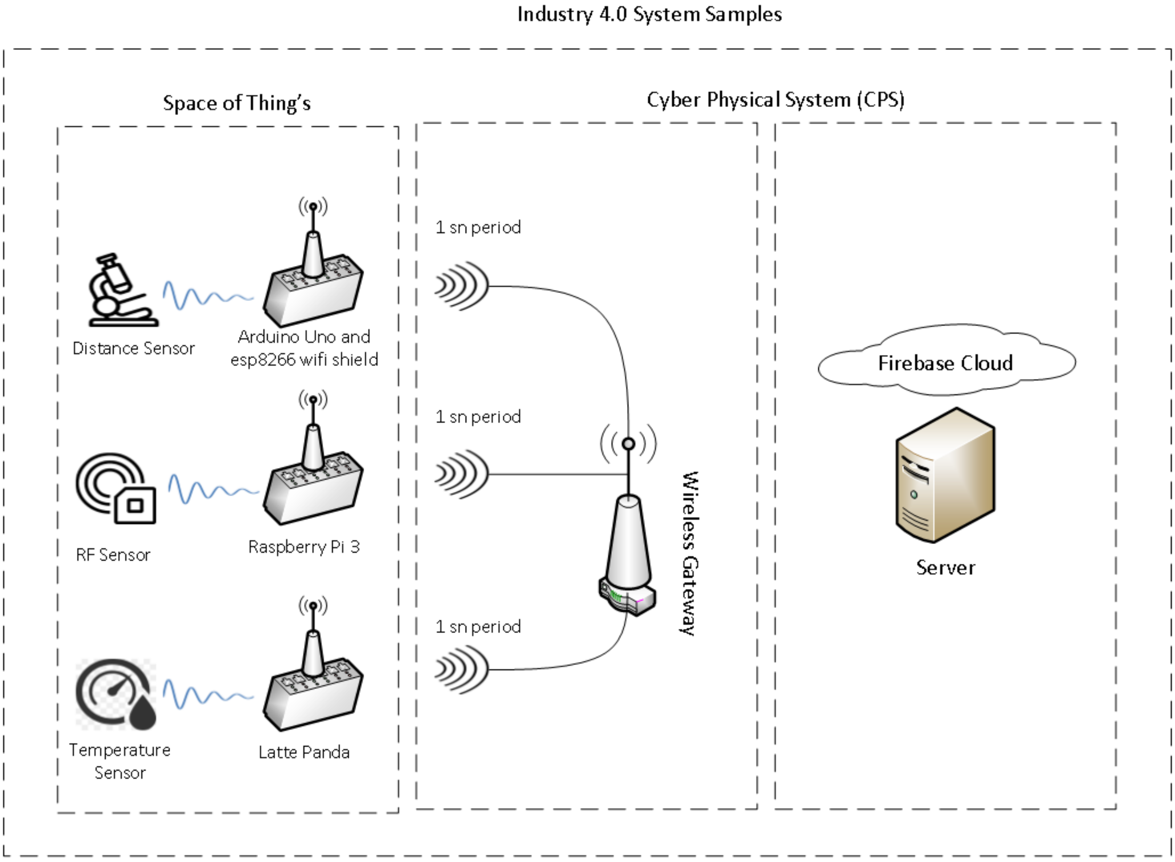

Figure 1. The Internet of things wireless network model.

The wireless network security conditions of the modem used in the model that was created as an example for the attack were varied with three different scenarios. These scenarios and precautions have been listed in Table 4. the wireless network is scripted as poor, medium and good depending on the preferred security options.

Table 4. Created scenarios for attack tests.

Scenario 1	Scenario 2	Scenario 3
There is NO password in the modem interface.	There is password in the modem interface..	There is password in the modem interface.
NO MAC address filtering.	MAC address filtering.	MAC address filtering.
WEP (Wired Equivalent Privacy) Password	WPA (Wi-Fi Protected Access) Password	WPA2 (Wi-Fi Protected Access) Password
WPS (Wi-Fi Protected Setup) PASSIVE.	WPS (Wi-Fi Protected Setup) PASSIVE.	WPS (Wi-Fi Protected Setup) ACTIVE.

It was used in Windows and Kali operating systems during the attacks on scenarios. Kali operating system has been preferred for the use of the tool (*Aircrack*, *Bully, coWPAtty, Fluxion, Fern, Wifite, MDK3*) for attacks on wireless domains [10]. In order to see the effects on the end-user size, some attacks were made in the Windows 10 operating system. External USB wifi adapter is used to scan and explore wireless networks on computers.

At first, the IP address of the target wireless network has been identified for the implementation of different attack types. Hence, The *Aircrack* tool in Kali operating system used the external wifi adapter in spectator mode Information such as the name of all wireless access points, MAC address, encryption type in the adapter's capture area was collected. IP addresses are monitored by making DHCP discovery on wireless access points (Table 5). All the information obtained will be used for the attack and listening methods to the wireless network. In three scenarios, the wifi scan has been repeated because the encryption methods of the wireless network are selected differently.

Table 5. Coarse code and output of DHCP and wifi discovery.

DHCP Discover	Wifi Discover

# dhd 	
Sniffing on any
Injecting on eth1 (4f:03:3b:f5:31:35)
 #0:
      SERVER-MAC: 4f:03:3b:f5:31:35
            IP: 192.168.0.1
      CLIENT-MAC: 00:0b:16:a1:b2:c3
            IP: 192.168.0.195
            MASK: 255.255.255.0
      GW: 192.168.0.1
      DNS: 192.168.0.1
>> "0 "0 "0 "0
	airodump-ng mon0
	
	# BSSID ENC ESSID
	
	01:00:A0:F5:4C:EE WPA TurkTelekom_T2S
	12:03:E0:F5:31:D8 WPA2 TTNET_4DC_A
	64:3B:00:DC:31:92 WPA TTNET_01
	4F:03:3B:F5:31:35 WPA2 Samples_Model

4.2. Cyber-attacks on Scenario 1

In Scenario 1 the conditions of the attack were investigated with data obtained at preliminary stages of attacks. First of all, access to the modem interface through the IP address of the wireless router has been attempted. Since the login password has not been changed to the modem interface, the user name and password of the modem brand and model has been taken from the database. As a result, standard input information has been entered into the modem. The following procedures can be done to create a network danger from the modem interface.

- Turn off the wireless network
- Find/ replace a network password
- Port on / off
- Redirect
- Internet off

BSSID, ESSID, MAC address and broadcast channel number are required to access the WEP passphrase assigned to the wireless network in the model. This data was collected at the preliminary stage. The packets of the destination network are taken to listen with a fake session after the destination network's data is entered as a parameter. After listening ARP packets have been counted enough to be interpreted, the Initialization Vector has been started and the WEP passphrase has been accessed.

In the last step, DDoS attacks were implemented on the network model of objects arranged in Scenario 1, and the system was unable to provide service for a specified period of time. The sample model transfers the data received from the sensors to the server every second. However, the denial of service caused the system to fail for 10 minutes. As a result of such attacks within the Industrial 4.0 network, production, analysis and evaluation steps are expected to be severely damaged.

4.3. Cyber-attacks on Scenario 2

The login passwords have been changed in the modem interface of the wireless network by the brand and model. For this reason, brute force attack and dictionary attack have been applied to access the modem interface. A previously created and collected 3.215.998 registered list was preferred for the implementation of the dictionary attack. the following cases have been identified result of brute force attack and dictionary attack.

- The password assigned to the modem interface is solved in 2 minutes with a brute-force attack as it is composed of letters and numbers consecutively (admin123).
- The password assigned to the modem interface is mixed with letters, numbers, and characters as it could not be resolved at the end of 134 minutes with a brute-force attack (xtr-%2a1.).
- The password assigned to the modem interface is easy to guess word or numbers as it is solved with the dictionary attack in 10 minutes (admin123).
- The password assigned to the modem interface is composed of difficult words or numbers, as it has been cannot be resolved with the dictionary attack (xtr-%2a1.).

In Scenario 2, an active network packet must be captured to log in the wireless network or to drop a device on the network. For this purpose, the scanning of devices connected to the wireless network was performed as shown in Table 6. In the network of things, the credentials of the three development cards have been obtained which created as models. The script was developed using the *scapy* library in Python for these operations.

Table 6. List of IoT devices in the network domain.

BSSID	Station	PWR	Rate	Lost	Frames
4F:03:3B:F5:31:35	0E:54:15:98:52	-53	0-1e	3	4
4F:03:3B:F5:31:35	00:FF:CC:D4:8F:1E	-53	0-1e	365	105
4F:03:3B:F5:31:35	0C:54:15:98:60:53	-64	0-24	0	1

The device can be disconnected from the network by sending deauthentication (de-auth) packets to devices within the wireless network without being connected to the wireless network. This can stop or damage the functioning of the system. In Scenario 2, 100 de-auth packets were sent to Raspberry Pi with 00:FF:CC:D4:8F:1E MAC addresses. Result of this, the device was disconnected from the network and failed to send data.

One of the securities implemented in the network of things is MAC filtering. In the filtering process, the MAC address of each device is previously introduced to the system. This type of protection can be bypassed with detecting devices on the network. The following process was followed to bypass MAC filtering in Scenario 2.

- Determination of devices authorized to connect to the network (3 Devices)
- Cloning MAC addresses that have the authority to connect to the network. (Target Arduino Uno device)
- Connect to the network with the MAC address which accesses permission. (As a target, Arduino Uno was selected which 0E:54:15:98:52 MAC addresses)

If you want to connect to the target network, “Access Point: Not-Associated” is notified. To bypass the target network, the MAC address of the target device has been assigned to the attack device's MAC address with the *Macchanger* tool in Kali. After the MAC replacement, the wireless network was reconnected and the result was successful. The connection issue has occurred because two different IP addresses are occurring with the same MAC address during this process The target device was dropped from the network with de-auth packets. Thus, the issue of IP assignment has been eliminated.

In the 802.11 standard, WPA and WPA2 security are applied to Data frames. However, it is not applied to Control Frame and Management frames. It uses a 4-way handshake to authenticate devices to the network in WPA and WPA2. Therefore, the wireless network was attacked via Management frames in Scenario 2 and Scenario 3. MAC addresses of network devices were detected in preliminary preparation. Here, 0C: 54:15:98:60:53 MAC Address Latte Panda device has been dropped from the network. A certain amount of time (5 min.) packets were saved as *test.cap* when the device tried to reconnect to the network. The saved packages were applied with an *aircrack-ng* brute force attack and it was succeeded.

4.4. Cyber-attacks on Scenario 3

It is seen that the model applying Scenario 3 is the same as the results of scenario 2 of cyber-attacks applied to log in the modem interface from the IP address. The MAC address of the device connected to the network is changed because the network has a MAC filtering. Finally, the WPA and WPA2 encrypted networks are logged on as described in Scenario 2.

WPS allows devices to be quickly connected to the network with the help of a pin when establishing a network. The manufacturer accounts for these pin numbers on their devices, by to the last six numbers of MAC addresses or fixed figures. Pin numbers consist of 8 digits [11]. But the final digit is used for accuracy detection. The WPS protocol controls the pin numbers in the first four and three digits. There are possibilities 10,000 for the first four digits and 1000 for the three digits.

The devices must have WPS locked feature turned off as a result of the scan for WPS attacks. Otherwise, WPS is closed to attack. In Scenario 3, the device's WPS locked feature is “No”. A brute-force attack, which applies 11,000 possibilities to connect to the network with WPS, has been attempted by entering known PIN numbers. In Scenario 3, the WPS PIN number on the MAC address of the modem is calculated with Python script code. The generated PIN number has been tested with the *Reaver* tool. As shown in Table 7, the attacker device log in the network with the command line *“reaver -i mon0 -b 4F:03:3B:F5:31:35 -p 12345678 -e Samples_Model -c 8 –vvv”*.

Table 7. WPS attack outcomes.

```
Reaver v1.4 WiFi Protected Setup Attack Tool
[+] Switching mon0 to channel 11
[+] Waiting for a beacon from 4F:03:3B:F5:31:35
[+] Associated with 4F:03:3B:F5:31:35 (ESSID: Samples_Model)
[+] Trying pin 85654747
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 4 seconds
[+] WPS PIN: ‘12345678’
[+] WPA PSK: ‘Samples_Model!!’
[+] AP SSID: ‘Samples_Model’
[+] Nothing done, nothing to save.
```

5. Conclusion

In this study, cyber-attacks were applied to the model in order to test the security of wireless networks on the internet of things rapidly growing. Three different scenarios have been created for these attacks. Each scenario has been attacked and its effects are collected. In Scenario 1, only the wireless network has been attacked. In Scenario 2 and Scenario 3, the wireless network and devices on this network were attacked. Although various security precautions are taken in wireless network configurations, they are vulnerable to cyber-attacks. It has been shown the attacks and their effects on the scenarios in Table 8.

Table 8. Attacks on scenarios and their effects.

Scenario 1		Scenario 2		Scenario 3	
Attack	**Effect**	**Attack**	**Effect**	**Attack**	**Effect**
DDOS	Service Blocking	DDOS	Service Blocking	DDOS	Service Blocking
Modem Interface	Session Opened	Modem Interface	Session Opened (Password-Dependent)	Modem Interface	Session Opened (Password-Dependent)
		MAC Fake Address	Authentication Succeeded	MAC Fake Address	Authentication Succeeded
		WPA	Authentication Succeeded	WPA2	Authentication Succeeded
				WPS	Authentication Succeeded

As a result, it is expected that the devices participating in the internet space of the existing things will not be able to shut down their weaknesses even if security is taken. In order to solve the problem, standards need to be developed in the network of things with including confidentiality, security policies, authorization, integrity, and encryption systems.

References

[1] Lasi, H., Fettke, P., Kemper, H. G., Feld, T., & Hoffmann, M. (2014). **Industry 4.0. Business & Information Systems Engineering**, 6(4), 239-242.

[2] Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. **Manufacturing Letters**, 3, 18-23.

[3] Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. **Journal of Industrial Information Integration**, 6, 1-10.

[4] Gorecky, D., Schmitt, M., Loskyll, M., & Zühlke, D. (2014, July). Human-machine-interaction in the industry 4.0 era. In Industrial Informatics (INDIN), **12th IEEE International** Conference on(pp. 289-294). IEEE.

[5] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions**. Future generation computer systems**, 29(7), 1645-1660.

[6] Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. **Future Generation Computer Systems**, 78, 964-975.

[7] Yüksel, M. E., & Zaim, A. H. (2009). RFID'nin Kablosuz İletişim Teknolojileri ile etkileşimi. **Akademik Bilişim**, 11-13.

[8] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities**. Future Generation Computer Systems** ,Volume 78, Part 2, pp 544-546.

[9] Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. **Journal of Computer and Communications**, 3(05), 164.

[10] Čisar, P., & Čisar, S. M. (2018). Ethical Hacking Of Wireless Networks In Kali Linux Environment. **Annals of the Faculty of Engineering Hunedoara**, 16(3), 181-186.

[11] Goncharov, D. E., Zareshin, S. V., Bulychev, R. V., & Silnov, D. S. (2018, January). Vulnerability analysis of the Wifi spots using WPS by modified scanner vistumbler. **IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)** (pp. 48-51). IEEE.

Genişletilmiş Özet

Giriş

Akıllı toplum ve Endütri 4.0 gereksinimlerinden ortaya çıkan IoT, cihazların ağ aracılığla yönetilmesidir. İnternete bağlı cihazlar uzaktan kontrol edilerek belirli iş veya süreçleri gerçekleştirmektedir (Gubbi et. al., 2013). Toplumun ihtiyaçlarının artması ile beraber IoT cihazları kontrolsüz şekilde hızla artmaktadır. Bunun sonucunda da siber zafiyetleri beraberinde getirmektedir (Stergiou et. al., 2018).

Bu çalışmada Endüstri 4.0 uzayı içerisinde yer alan nesnelerin kablosuz ağları karşı yapılan siber saldırılar ve etkileri örnek bir model üzerinden anlatılmıştır. Oluşturulan nesne uzayı içerisinde farklı güvenlik seviyelerinde senaryolar geliştirilmiştir. Modelin her senaryosuna yönelik farklı saldırılar yapılmış ve etkileri izlenmiştir. Hızla büyüyen nesnelerin dünyasında siber saldırılara karşı alınan önlem alınamaz duruma gelmiştir. Bunun sonucunda veri, zaman ve para kayıpları oluşmaktadır. Bu çalışma ile kablosuz ağlara yapılan siber saldırı sonucundaki olumsuz etkilerin görülmesi ve düzeltilmesine hedeflenmektedir.

Yöntem

Kablosuz ağlar olarak bilinen Wifi, gerçekte 1997 yılında IEEE tarafından 802.11 olarak geliştirilmiş bir radyo iletişim standardıdır (Yüksel and Zaim, 2009). Gelişen teknoloji ile beraber 802.11 kablosuz yerel ağ standardı yetersiz hale geldi ve 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac standartları geliştirildi. Kablosuz ağ bağlantılarında güvenlik geliştirilen standartlar ile sağlanmaktadır. Ağ cihazlarında kablosuz ağların güvenliği için ilk yıllarında günümüze kadar farklı şifreleme sistemleri uygulanmıştır. Bunlar sırasıyla WEB, WPA,WPA2 ve WPA3' tür.

Çalışmanın gerçekleştirilmesi için veriler üzerinde üretim ve analiz gerçekleştiren kablosuz bir model oluşturulmuştur. Bu model içerisinde nesnelerin interneti kavramı sağlayan üç adet geliştirme kartı (Arduino Uno, Raspberry Pi 3 ve Latte Panda) kullanılmıştır. Kullanılan geliştirme kartlarının wifi kablosuz ağ yapılandırılması yapılmıştır. Test ortamın oluşturulması için her geliştirme kartına mesafe, RF ve sıcaklık sensörleri yerleştirilmiştir. Bununla beraber dış ortamdan veri toplayan ve verileri kablosuz ağ üzerinden aktaran IoT modeli tasarlanmıştır. Çevresel ortamdan okunan veriler, kablosuz ağ geçidi üzerinden bulut sunucuda bulunan Google Firebase veri tabanında saklanmaktadır. IoT cihazları 1 saniye periyodla verileri veri tabanına kaydetmektedir.

Saldırı yapılması için örnek olarak oluşturulan modelde kullanılan modemin kablosuz ağ güvenlik durumlarını üç farklı senaryolar ile çeşitlendirilmiştir. Bu senaryolar ve alınan tedbirler Tablo 1'de listelenmiştir. Tercih edilen güvenlik seçeneklerine bağlı olarak kablosuz ağ; zayıf, orta ve iyi olarak senaryolandırılmıştır.

Tablo 1. Oluşturulan senaryolar.

Senaryo 1	Senaryo 2	Senaryo 3
Modem arayüzünde parola YOK.	Modem arayüzünde parola VAR.	Modem arayüzüne parola VAR.
MAC adresi filtrelemesi YOK.	MAC adresi filtrelemesi VAR.	MAC adresi filtrelemesi VAR.
WEP (Wired Equivalent Privacy) türünde parola VAR.	WPA (Wi-Fi Protected Access) türünde parola VAR.	WPA2 (Wi-Fi Protected Access) türünde parola VAR.
WPS (Wi-Fi Protected Setup) YOK.	WPS (Wi-Fi Protected Setup) YOK.	WPS (Wi-Fi Protected Setup) VAR.

Farklı saldırı türlerin uygulanması için öncelikle hedef kablosuz ağın IP adresini tespit edilmiştir. Bunun için Kali işletim sistemindeki *aircrack* aracı ile harici wifi adaptörünü izleyici modunda kullanılmıştır. Adaptörün çekim alanı içerisinde bulunan tüm kablosuz erişim noktalarının adı, MAC adresi, şifreleme türü gibi bilgiler toplanmıştır. Kablosuz erişim noktalarında DHCP keşfi yapılarak IP adresleri listelenmiştir. Elde edilen tüm bilgiler daha sonra kablosuz ağa yapılacak saldırı ve dinleme yöntemlerinde kullanılacaktır. Üç senaryoda kablosuz ağın şifreleme yöntemleri farklı seçildiği için wifi taranası tekrar edilmiştir.

Sonuç

Bu çalışmada hızla büyüyen nesnelerin interneti kavramının kablosuz ağlarda güvenliklerini test etmek için örnek model üzerinden siber saldırılar uygulanmıştır. Bu saldırılara için 3 farklı senaryo oluşturulmuştur. Her senaryoya özgü saldırılar yapılmış ve etkileri belirtilmiştir. Senaryo 1 ‘de sadece kablosuz ağa yönelik saldırılarda bulunulmuştur. Senaryo 2 ve Senaryo 3’de hem kablosuz ağa hem de ağ içerisindeki cihaza saldırı yapılmıştır. Her ne kadar kablosuz ağ yapılandırmalarında çeşitli güvenlik önlemleri alınsa da siber saldırılara karşı zayıf durumdadır. Tablo 2’de senaryolara karşı yapılan saldırılar ve etkileri gösterilmiştir. Sonuç olarak mevcut nesnelerin interneti uzayına katılan cihazların, güvenlik önlemleri alınsa da zafiyetlerinin kapatılamayacağı öngörülmektedir. Sorunun çözümü için nesnelerin ağında gizlilik, yetkilendirme, bütünlük ve şifreleme sistemi konularını içeren güvenlik politikalarına sahip standartların geliştirilmesi gerekmektedir.

Tablo 2. Saldırılar ve bu saldırıların etkileri.

Senaryo 1		**Senaryo 2**		**Senaryo 3**	
Saldırı	**Etki**	**Saldırı**	**Etki**	**Saldırı**	**Etki**
DDOS	Hizmet Engelleme	DDOS	Hizmet Engelleme	DDOS	Hizmet Engelleme
Modem Arayüz	Oturum Açıldı	Modem Arayüz	Oturum Açıldı	Modem Arayüz	Oturum Açıldı
		MAC Taklit etme	Oturum Başarılı	MAC Taklit etme	Oturum Başarılı
		WPA	Oturum Başarılı	WPA2	Oturum Başarılı
				WPS	Oturum Başarılı