www.dergipark.gov.tr
ISSN:2148-3736
El-Cezerî Fen ve Mühendislik Dergisi
Cilt: 8, No: 3, 2021 (1286-1308)

El-Cezerî Journal of Science and Engineering
Vol: 8, No: 3, 2021 (1286-1308)
DOI : 10.31202/ecjse.916532

ECJSE

Review Paper / Derleme

A Survey on Security Attacks with Remote Ground Robots

Batuhan ÖZDÖL[a], Elif KÖSELER[b], Ezgi ALÇIÇEK[c], Süha Eren CESUR[d], Perit Jan AYDEMIR[e], Şerif BAHTIYAR[f]

[a,b,c,d,e,f]Department of Computer Engineering, Istanbul Technical University, Maslak, 34469, İstanbul, Turkey
bahtiyars@itu.edu.tr

Received/Geliş: 16.04.2021 **Accepted/Kabul:** 05.07.2021

Abstract: Contemporary healthcare systems contain diverse computing devices that construct very complex systems to manage patients' data more efficiently. Connected computing devices, such as the Internet of Things (IoT) that may have limited processing powers, have contributed more than ever with the advent of wearable body area networks (WBAN). These devices are connected to other medical devices to share sensitive health data with corresponding entities like hospitals, research institutions, and insurance companies. Since health data are very sensitive, they should be always available to authorized entities and unavailable to other entities. Moreover, COVID-19 pandemic has added additional value to health data which case increases cyber-attacks on (Electronic health) E-health systems with different tools dramatically. In this paper, several cyber-attacks on E-health systems are explored. Particularly, we have focused on attacks to IoT based wearable health devices for body area networks. The paper contains the architecture of wearable health devices to show the potential attack surface. One of the main contributions of the paper is to present cyber-attacks on wearable e-health devices with ground robots. A tactical ground robot is portable devices that may be used to carry out several cyber-attacks on E-health systems. Moreover, the paper contains analyses of the attacks with ground robots.

Keywords: Cyber security, E-health, COVID-19, IoT, Body Area Networks, Ground Robot

Yer Robotlarıyla Yapılan Uzaktan Siber Saldırılara İlişkin Bir İnceleme

Öz: Sağlık hizmetleri, hastaların verilerini daha verimli bir şekilde yönetmek için karmaşık sistemler oluşturan çeşitli bilgi işlem cihazları içerirler. Sınırlı işlem gücüne sahip olan, bir iletişim ağına bağlı bilgi işlem cihazları, Nesnelerin İnterneti (IoT) gibi, giyilebilir vücut alanı ağlarının (WBAN) ortaya çıkmasıyla daha yararlı bir hale geldi. Bu cihazlar, hassas sağlık verilerini hastaneler, araştırma kurumları ve sigorta şirketleri gibi ilgili kuruluşlarla paylaşmak için diğer tıbbi cihazlara bağlanır. Sağlık verileri çok hassas olduğundan, bu veriler yetkili kuruluşlar tarafından her zaman erişilebilir olmalı ve diğer kuruluşlar tarafından kullanılamaz olmalıdır. Bununla beraber, COVID-19 salgını sağlık verilerine ek bir değer katmıştır ve bu durum, farklı araçlarla Elektronik sağlık (E-sağlık) sistemlerine yapılan siber saldırıların sayısını önemli ölçüde artırmıştır. Bu yazıda, E-sağlık sistemlerine yönelik siber saldırlar incelenmiştir. Özellikle IoT tabanlı giyilebilir sağlık cihazlarına yönelik saldırılara odaklanılmıştır. Makalede, potansiyel saldırı yüzeyini göstermek için giyilebilir sağlık cihazlarının mimarisi de işlenmiştir. Makalenin ana katkılarından biri, insansız kara robotları ile giyilebilir E-sağlık cihazlarına yönelik potansiyel siber saldırıları göstermektir. Taktiksel bir kara robotu, E-sağlık sistemlerine çeşitli siber saldırılar gerçekleştirmek için kullanılabilen taşınabilir bir cihazdır. Ayrıca makale, bu kara robotları ile yapılan saldırıların analizlerini de içermektedir.

Anahtar Kelimeler: Siber Güvenlik, E-sağlık, COVID-19, Nesnelerin Interneti, Vücut Ağları, Kara Robotu

How to cite this article
Özdöl, B., Köseler, E., Alçiçek, E., Cesur, S.E., Aydemir, P.J., Bahtiyar, Ş., "*A Survey on Security Attacks with Remote Ground Robots*" El-Cezerî Journal of Science and Engineering, 2021, 8 (3); 1286-1308.

Bu makaleye atıf yapmak için
Özdöl, B., Köseler, E., Alçiçek, E., Cesur, S.E., Aydemir, P.J., Bahtiyar, Ş., *"Yer Robotlarıyla Yapılan Uzaktan Siber Saldırılara İlişkin Bir İnceleme"* El-Cezerî Fen ve Mühendislik Dergisi 2021, 8 (3); 1286-1308.
ORCID ID: [a]0000-0002-2601-633X; [b]0000-0002-3882-2689; [c]0000-0003-2487-9884; [d]0000-0003-1672-0216; [e]0000-0002-1493-8513; [f]0000-0003-0314-2621

1. Introduction

There have been many developments in the healthcare area with the emerging technologies and recent treatments introduced. Patients' information has started to be transmitted to health professionals remotely by using the new technologies, which reduces the burden of health professionals to share the critical information among corresponding entities. Moreover, these technologies help to create innovative services that increase the quality of treatments and reduce costs considerably. These technologies and services are within the scope of E-health. The definition of E-health is a measurement and an evaluation of health information obtained by using electronic resources. The goal of E-health systems integration is to mitigate the risk of encountering health problems [1, 2].

E-health systems carry out data among patients and healthcare professionals with many devices that are complex in terms of their software and hardware structure. Devices of wearable body area networks, sensors like pulse oximeters, wearable blood pressure monitors, implementable medical devices (IMD) like insulin pumps, and pacemakers coexist under the Internet of Things technology [3, 4, 5], which integrates platforms to virtual and real environments used in E-health systems. Since these devices are highly connected, this makes them vulnerable to many attacks. IoT devices generally depend on wireless communications which consist of three layers, namely application layer, network layer, and perception layer. IoT devices have a firm relationship with sensors, Radio-Frequency Identification (RFID), and Wireless Sensor Networks (WSN) [6, 7], which case inherits vulnerabilities and threats of these devices and networks to E-health systems.

Wearable devices and systems are convenient to manage the sustainable monitoring of patients. These systems give the ability the patient to monitor his/her condition in the most distinct circumstances with almost error-free approach. Health professionals are also informed in case of an emergency situation that may threaten patients' health. Specifically, E-health devices have been used to treat heart disease, diabetes, chronic pain, hearing loss, and etc [8]. Devices that perform transmissions using IoT infrastructure are called wearable IoT (WIoT) devices. Electroencephalography (EEG), electrocardiogram (ECG), blood pressure, heart rate, and motion sensors are examples of WIoT devices. They receive sensor data and allow data monitoring via Bluetooth or WiFi connections. The main objective here is to increase the quality of health care and make the treatment process of patients more efficient.

A tactical ground robot is portable devices that may take 360 degrees immersive video in day and night, may climb stairs, and may contain various attachments. This kind of robots are located in the tactical field, such in the military field, that are controlled remotely. Ground robots are used to collect data about critical infrastructures of targeted institutions and countries with cyber-attacks. Recently, health information has become more significant than ever with the spread of COVID-19 pandemic. Therefore, E-health systems have become one of the main targets of cyber criminals, who may use ground robots to carry out cyber-attacks.

The security of health information has become more significant than ever with the widespread effect of COVID-19 pandemic. The diversity and the increased number of cyber-attacks on E-health systems have shown the challenge regarding security of E-health systems. In this research, we consider potential cyber-attacks with ground robots to wearable E-health devices. We also investigate potential countermeasures against these attacks. Our main contributions are as follows:

• Analysis of security and privacy attacks on healthcare devices by using ground robots in the military field.

- Potential countermeasures against attacks with ground robots on E-health systems.
- Exploring security vulnerabilities and attacks on COVID-19 data.

The rest of the paper is organised as follows. Section II is about the architecture of wearable health devices. We show cyber-attacks on medical devices in Section III. Section IV is devoted to COVID-19 and security of E-health systems. We present security attacks with ground robots in Sections V. The analyses of the attacks are given in Section VI. We conclude the paper with Section VII.

2. The Architecture of Wearable Health Devices

Due to the development of wearable devices, the surveillance of individuals is easier than ever [9]. Accordingly, patients' data are more likely to be targeted by cyber attackers. Required security mechanisms for data in wearable health devices depend on the structure of the communication networks. Figure 1 illustrates the structure of an IoT network that is used with wearable health devices. In this structure, medical data are collected quickly, conditions are monitored and treated remotely [10, 11]. Generally, the communication architecture of a wearable IoT system which includes both BAN and IMD networks contains three levels described as follows:

- Intra-wearable device network communication: The interaction of sensors is located around the body of the patient. The communication signals within the region use a Personnel Server (PS) that acts as a gateway to transfer data to the next level.
- Inter-wearable device network communication: This level connects the PS and the user via access points that are considered as an essential part of the network and are positioned to permit emergencies. This communication is also divided into infrastructure-based architecture and ad-hoc based architecture.
- Beyond wearable device network communication: This level is appropriate for large areas and behaves as a gateway. In this level, a medical environment database is a crucial part of the system. It contains medical histories and a private profile of users. Moreover, in emergency cases medical providers or patients may be alerted via the Internet or Short Message Service (SMS). General Packet Radio Service (GPRS)/3G/4G may be used directly to connected E-health network without an access point.

There are two modes for data transfer between the device and the coordinator, namely beacon mode and unsigned mode. In beacon mode, the network coordinator controls the location in the center of the communication, which forms a star topology. To allow device synchronization and network control, the network coordinator initially sends periodic beacons for recognition purposes. The user or the IoT standard may determine the duration of signals. The non-beacon mode uses Collision Avoidance and Carrier Sense Multiple Access to send data to the coordinator using multiple access. Depending on low Signal-to-Noise Ratio (SNR) values, memory space used, computational capabilities of body sensors, and applicable medical devices, security attacks are likely to occur. Therefore, a high level of security and privacy must be accomplished for wearable IoT devices [12].

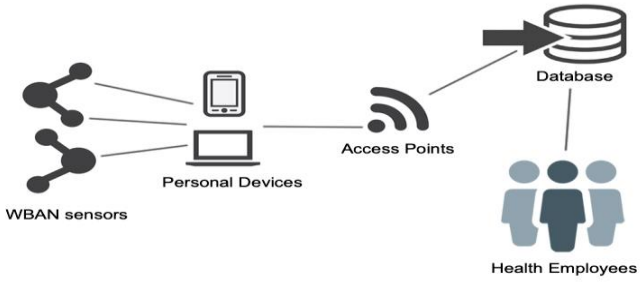

Figure 1. The structure of a wireless health device network.

In intra-wearable device network communication, sensors like ECG, EMG, and EEG may be used to monitor the activities of body units such as heart, muscle, and brain, and to evaluate or anticipate the situation [13]. Each sensor has a structure that may detect and process one or more signals [14]. Inter-wearable device network communication includes personal server application that runs on a cell phone or home personal computer. The personal server is responsible for several tasks that provide wireless medical sensors with a transparent interface, which are an interface for the user and an interface to the medical server. Beyond wearable device network communication contains a medical server that establishes a communication channel on the user's server and collects reports from the user. It also integrates data into the user's medical record accessed over the Internet. The service gives a warning in the form of an alarm if advice or any symptoms appear [15].

3. Cyber Attacks Against Medical Devices

Cyber attacks on medical systems have been increased dramatically. As a result of attacks on WBAN or IMD devices and sensors, patients' data may be changed or captured. One of the methods that will change data of the system is a spoofing attack. If the system accepts an external signal that it detects as part of the sensor, the attack has occurred, and the system undergoes data changes. An acoustic attack is detected by sending ultrasonic frequencies at resonance frequencies to wearable IoT devices [16]. Denial of service attack, spoofing, and acoustic attack may help attacker to access confidential medical information of patients that may be detected with power consumption [17]. Fitbit which is a wireless wearable medical device that measures data such as pedometers, heart rate, sleep quality, climbed steps, and other personal fitness metrics are attacked by injecting fake steps into the system using a low-cost speaker [18].

There have also been attacks using machine learning algorithms. Xue, Q., and Chuah, M.C. have proposed a weight adjustment attack approach for a Recurrent Neural Network (RNN) based model. The attack provides tainted information during training phase. A possible strategy of RNN-based model incorporates end-to-end training model to prevent such attacks [19].

Tactical robots may be used for communications during IoT cyber-attacks due to their size, ability to move in all kinds of terrain, and remote control. Figure 2 illustrates a type of ground tactical robot. These robots pose a serious threat to medical devices and data held in these devices, as any wireless-communicating component in the system may sneak into the shooting zone undetected. Therefore, it makes difficult to find the person performing the attack.

A study analyzed cyber-attacks using an unmanned aerial vehicle (UAV). The most common forms of UAV cyber-attacks have been theoretically explained and analyzed in [20]. Kristiyanto, Y. and Ernanstuti tested WiFi connectivity against authentication attacks on IoT devices. A penetration test method to analyze activities and changes is used. A network analyzer, packet sniffer, IoT-based simulation device that uses the ESP8266 module, a gateway that contains a transceiver, antenna, a computer, and a target device that is an IP camera connected to the gateway tools are used for realizing attack scenarios. A scenario is created and simulated for a deauthentication attack on a device with WiFi connectivity. The goal of the attack is to record all activities when the attack occurs using tools [21].

In another study, it has been shown that UAVs may be used in attacks on healthcare services, including medical devices. Possible UAV-based attacks have been demonstrated and a cyber-attack experiment was carried out on medical sensors using a drone [22]. There is also a theoretical analysis of how to attack a wireless network system using aircraft and how this attack may be carried out over the network architecture [23]. A cyber-attack in a war is investigated with tools that

are controlled by remote devices or with sensors. In this paper, we investigate how wireless networks and devices that communicate may be interfered with robots for military purposes.

Another study reported major security requirements and attacks on different layers of wearable BAN. The attacks have many effects on the performance of the physical, data link, network, and transport layers of wearable BAN. Three nodes of wearable medical devices architecture were mentioned; implant node, body surface node, and the external node that these devices consist of a 3-tier architecture. Wearable medical device sensors and actuators are defined in Tier-1. Personal services and access points as Internet are defined in Tier-2. Medical database system and health system employees are defined in Tier-3. The study gives examples of basic security requirements and it explains principles such as confidentiality, authentication or proof of identity, secure communication, integrity, data freshness, network availability, secure management, reliability, accountability, and flexibility. Additionally, the security levels are increased with medical applications to make it more widely available [24].

In this study, we analyze cyber threats and attacks on wearable body area networks. Moreover, we have explained potential attacks in E-health system using ground robots. In addition, we present countermeasures against these attacks.

Figure 2. A tactical ground robot.

4. COVID-19 and Security of E-Health Systems

With the recent outbreak of the coronavirus epidemic, there has been a huge increase in the number of users working online interacting with each other. It was seen that cyber attackers turned the pandemic period into an opportunity. Cyber security attacks are increased nearly by five times throughout the COVID-19 pandemic [25]. People have become victims of phishing attacks through content related to COVID-19. Attacks that occurred during the pandemic period and the possible cybersecurity threats are described in [26].

Due to the global COVID-19 outbreak, there is an urgent need to harness existing technologies to their full potential. IoT is considered one of the trendiest technologies with great potential in combating the coronavirus outbreak. IoT consists of a network where devices detect the environment and send data over the Internet. During the emergence of the global COVID-19 pandemic, confidence in technologies such as IoT, Artificial Intelligence (AI), Blockchain, Big Data Analytics, and Cloud computing has increased. IoT-based healthcare units respond promptly through medical staff to deal with COVID-19 patients. In addition to the large number and small size of IoT devices, they have security requirements. There are algorithms with less computational costs that may be used to secure wearable E-health devices [27].

Following the pandemic outbreak, cyber-attacks related to COVID-19 have become increasingly common, specifically three or four cyber-attacks have been reported on some days. Many cyber-attacks during this period start with a phishing campaign that directs victims to download a file or

access Uniform Resource Locator (URL). The file or the URL acts as a carrier of malware, when uploaded, acts as a tool for financial fraud. Analyses show that the phishing campaign take advantage of the media and government announcements to increase the likelihood of success [28]. Apple Inc. and Google Inc. provided a security analysis of the COVID-19 Contact Tracing Specifications, DP-3T, and Temporary Contact Numbers (TCN) protocols. The system is intended to help fight the COVID-19 pandemic while keeping user privacy and security at the center of its design. COVID-19 diagnostic tests or existing specifications have been shown to pose significant risks to the community, such as privacy breaches and loss of trust in E-health systems. Storage drain attacks, relay and replay attacks, trolling attacks, linking attacks, and tracking and de-anonymity attacks are analyzed for their consequences and new mitigation strategies. The proposed mitigation strategies are easy to use as they do not require architectural changes [29].

A comprehensive study examined interventions through emerging technologies such as IoT, drones, AI, blockchain, and 5G [30]. Any attack on the health system will cause further damage to the health system, which is already burdened by the pandemic. The security of many devices that diagnose COVID-19 should be ensured as much as possible. Nine COVID-19 applications that use deep learning algorithms allow rapid diagnosis of the pathogen. Six methods of deep learning based COVID-19 diagnosis are widely used by researchers. However, researchers have discovered different types of attacks against these nine types of deep learning applications. Moreover, the six applications were tested from open source libraries. Their models were examined to design competing samples for each type and identify vulnerabilities of models. The findings show that deep learning applications are vulnerable to adversarial example attacks. Additionally, these applications require further investigation, enforcement, and appropriate defense mechanisms before they are used in real-life healthcare systems [31].

The COVID-19 pandemic results in cyber security concerns about Working From Home (WFH). For instance, it is observed that the possibility of government-sponsored attacks, phishing attacks, and ransomware increase considerably. On the other hand, some practical approaches are provided to reduce the risks of cyber-attacks for WFH, including mitigating healthcare-related security risks in [32]. The impact of COVID-19 on cyber security rests largely on emerging technologies. Actually, the increase in anxiety and fears associated with the pandemic increase the success rate of cyber-attacks. Our analyses show that healthcare institutions are one of the main victims of cyber-attacks during the epidemic. Additionally, attacking systems with a remotely controlled robots will provide attackers more effective tools.

5. Security Attacks with Ground Robots

5.1. Distributed Denial of Service Attack

Denial of Service attacks (DoS) are among the most common types of attacks on connected devices. Recently, the number of DoS attacks keep increasing partially because DoS attacks may be carried out with a low amount of technical knowledge [33]. DoS attacks are realized by either sending malformed packets to disturb a protocol [34] or sending a massive amount of data to the system in order to limit the bandwidth. Simply, the goal of DoS attacks is to consume system resources thus denying service for legitimate users [35]. System shortages are often used as a way to plant malware and steal possibly personal data. Over 90 percent of organizations are hit by DoS attacks [36].

There are different types of DoS attacks. The most widely used DoS attacks are Distributed Denial of Service (DDoS) attacks. DDoS attacks have appeared in common since 1998. Moreover, the popularity of DDoS attacks has become widely known with attacks on some high-profile targets in

2000 [37]. Now, E-health systems are among the targets of DDoS attacks that are done by using multiple machines which are usually referred as agents to send packets to the target. Each agent takes commands from another machine called master or handler. Handler machines are controlled by the attacker. Sometimes handlers do not exist and different methods are used for communications between agents and the attacker. A simple DDoS attack is shown in Figure 3.

Since medical data are very critical in terms of security and privacy, DoS attacks are very dangerous threat for E-health systems. Wireless body area networks need to communicate with a master device to send patients' data to the doctors. By attacking the availability of the master device, DDoS attacks may prevent availability of data to communications parties. For example, patients' health data may be unavailable to medical staff or attackers may use the vulnerability to steal personal health data with DDoS attacks.

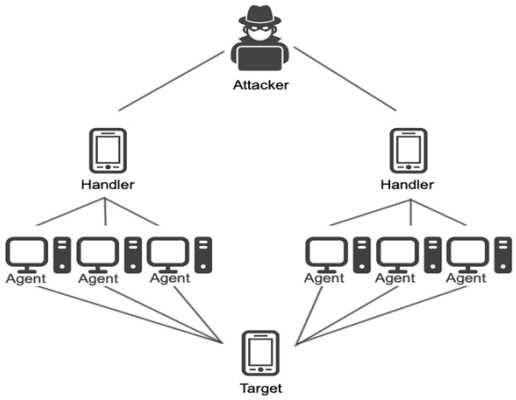

Figure 3. A representation of DDoS attack.

5.2. Jamming Attack

Jamming is a discharge of radio signals to disrupt communication systems. The first occasions of jamming attacks have been recorded back in the beginning of the 20th century against military radiotelegraphs. Germany and Soviet Union were the first to engage in jamming [38].

Jamming attack is considered one of the most severe security threats to Wireless Sensor Networks. It is achieved by directing an electromagnetic signal towards a network system to interrupt and overload the system's signal transmission. Jammer does not follow MAC layer protocol. If the source of the jam is strong, the possibility of a successful attack increases. Jamming attacks may be considered as a different kind of DoS attack. According to Chamola's Research, "The level of interference that a spread spectrum system may handle and still be able to perform with a specified level of performance is measured with the help of the jamming margin." [39].

In a jamming attack, a jammer source sends a stronger signal to the Wireless Sensor Networks. The system's original signal is overloaded by the jammer source. The signal that is sent from the jammer is a strong white noise signal. Therefore, the jammer signal reduces the effect of original signal. Figure 4 shows the general jamming attack.

There are different types of jamming attacks. Spot Jamming is the widely used attack type among jamming attacks. In this attack, a jammer directs all the transmission power to a single frequency to override the original signal. In Sweep Jamming, the frequency changes its frequency promptly. It causes to intervene in different transmissions in the close range with a single attack. In the third one, Barrage Jam, the jammer sends a range of frequencies, which has wide jamming band and

large noise power, which is widely used in processing backup jamming to radar, missile, and communication [40]. The last and the most sophisticated one is Deceptive Jamming that does not leave any trace. The jammer sends a fake signal like the system's original signals.

The essential damage is mostly caused by the design architecture of the Wireless Sensor Networks. Because of their nature, Wireless Sensor Networks have limited memory, low battery resources, and slow processing capabilities. Wireless Sensor Networks are very vulnerable to jamming attacks. Therefore, countermeasures are vital to prevent these attacks. A general prevention for jamming attack is dynamically changing the transmission frequency. This is achieved by perceiving the electromagnetic environment. Then, analyzing the characteristic of jamming signals and dynamically choosing the best frequency hole as the operating frequency transmission [41].

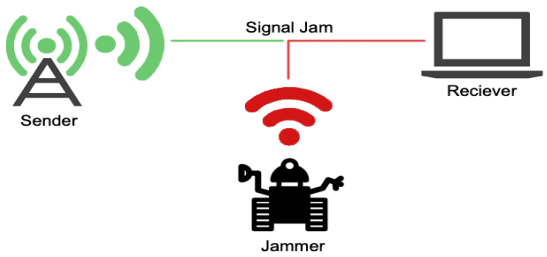

Figure 4. A jamming attack.

5.3. De-authentication Attack

De-authentication attack is performed on wireless networks. The attack reduces network connections by sending frames to devices that are connected to an access point. If a client or access point send a disconnect request, one of them sends de-authentication frames to the other party. Goals of this attack are:

- Disconnecting or blocking networked clients connected to the network.
- To get the WiFi Protected Access (WPA) Handshake value.
- Falling from the network during the attack and reconnecting to the network with the WPA Handshake value obtained from the running client, a brute-force attack may be performed on this handshake value to find the WPA password information belonging to the network.

A de-authentication attack may be used to detect hidden Service Set Identifier (SSID) information. The attacker sends a series of deauthentication packets to the Access Point (AP) and these frames are for re-authenticating connected clients. This handshake is re-authenticated between clients and access point, initiated to disconnect all connected clients [42]. There are two types of De-authentication attack:

1) Client-based De-authentication Attacks: The attack is done by targeting a specific client. The purpose is to disconnect the target client from the network. The attack has a higher success percentage.
2) Broadcast De-authentication Attacks: The goal of this attack is to disconnect all clients connected to the access point by making the attack directly against the access point. The success rate of the attack will decrease because we may slow down the network when attacking the access point directly. Additionally, clients may drop the deauthentication packets sent to them when a broadcast attack occurs.

5.4. Evil Twin Attack

Evil Twin attack is a kind of fake access point attack. It is one of the most dangerous WiFi attacks which is threading access points, nearly two decades old. This attack involves fake broadcasting of the same name as the existing wireless network environment, making network traffic of victims or devices for our system traceable or configurable. It takes the name or Service Set Identifier (SSID) of a computer or phone of a wireless network and it works like its twin. In an E-health system, data are sending from access points to the medical database server of a hospital system. Considering that device, as well as wearable devices, it is realized by the patient making a fake broadcast with the same name as the network broadcast at the location. Users create a send a connection request to the fake access point.

Evil Twin attack involves the Man in the middle attack (MitM). The WiFi router may be replaced by our ground robot's data receiver which is replaced by an attack into the device to control the transmission medium between two devices. This intercept and redirects the communication. In this case, Address Resolution Protocol (ARP) poisoning, Domain Name System (DNS) poisoning, or side-jacking attacks for session stealing are possible.

A system is proposed to detect Botnet on 6LoWPAN attacks, which is a type of MitM attack. Analyzing the packets that pass through the border router between the physical and the network domain for the unexpected changes in the traffic of 6LoWPAN sensor nodes. Their system computes the average for the sum of Transmission Control Protocol (TCP) control field, packet length, and the number of connections of each sensor. Then, the system monitors network traffic and issues a warning when measurements for any node violate the calculated averages [43].

Intrusion Detection Systems (IDS)s may be applied to IoT environments that use Constrained Application Protocol (CoAP). Bit flips, byte exchanges, and modifications of entire data fields that can be related to MitM attacks are implemented. Results show that both anomaly and signature based IDSs failed in detecting some kinds of attacks [44]. Another proposed detection system, a scan-based self-anomaly detection (SSAD) which enables wireless devices to verify the authenticity of wireless access points without the support of the access points to detect and mitigate channel-based Man-in-the-Middle attacks. It is observed that a 99 percent detection rate is achieved in the condition of the attacker being in the same room with the AP [45].

In Evil Twin attack, many users should be connected to the target network. The number of users dropped from the network depends on sent deauthentication packets. Thus, there is a high probability that an unconscious user is found and connected to the network. A simple solution is proposed to detect Evil Twin access point to prevent the attack. Round-Trip Time (RTT) and number hops are used between the client and server-based technique and deauthentication detection between client and legitimate access point-based technique [46]. Figure 5 illustrates the scheme of Evil Twin attack by using tactical ground robots. With this attack the attacker can give Internet Protocol (IP) from a specific IP pool, change the default gateway, listen to network traffic, interfere with secure socket layer (SSL) traffic, and change the DNS settings.

The best way to avoid this type of attack is avoiding connecting unencrypted channels. Therefore, various informative reminder texts may be published for patients and hackers. Patients should not connect WiFi hotspots that are insecure and should not auto-save hotspots. To provide struggling the attacker, two-factor authentication should be provided in the E-health system. Another protection method is to limit the number of available Media Access Control (MAC) and IP addresses for wearable health devices that are connected through the modem interface. Other

devices will not be able to connect even if they provide the correct password. For the patients who use wearable devices, an evil twin AP is nearly impossible to detect because the SSID appears legitimate, and the attacker provides the Internet service.

Generally, the best way to stay safe on unfamiliar WiFi networks is to use a Virtual Private Network (VPN) to encapsulate the WiFi session in another layer of security. If the attacker who made the Evil Twin attack is using these robots remotely, it seems very difficult to physically find the attacker because it is probably far away. In such a case, the thing to do is to apply for a legal remedy.

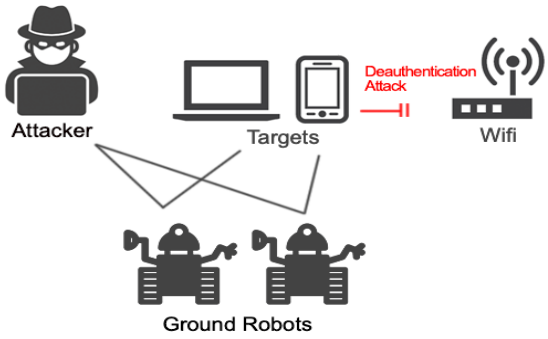

Figure 5. Evil Twin Attack using Tactical Ground Robots.

5.5. Eavesdropping Attack

Eavesdropping attacks, also known as sniffing or snooping attacks, have been troubling in the healthcare systems for 10 years [47]. They are easily implemented. The attacks may be passive or active attack [48]. These attacks have been used very commonly for stealing financial and business-related information. The attacker may reach the transmitting information by sniffing any node of the network path. These nodes may contain some weaknesses. The attacker may not require nether any active operation nor active connection through the network. Eavesdropping attacks are distinguished from MitM attacks since data always reach the target. Therefore, eavesdropping attacks are far more difficult to spot than MitM attack.

If we look at the medical sensors, they usually transmit their data over wireless networks. The attacker usually stays close to the hospital; therefore, it is within the range of hospital wireless network. Sensors on the patient's body transmit data to servers, so that eavesdropping may occur. Attackers may find the location of the patient who wears the medical sensors by eavesdropping. Therefore, this is one of the most dangerous consequences of eavesdropping attack [49]. Eavesdropping attack, the relation among patient's sensors and the corresponding servers are shown in Figure 6.

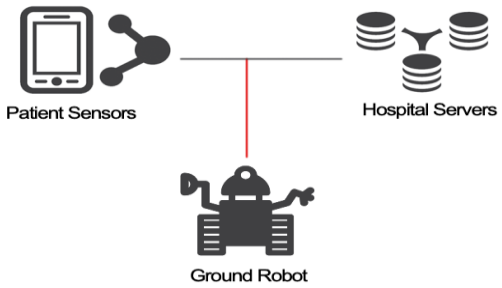

Figure 6. Flow analysis of eavesdropping attack.

5.6. False Data Injection Attack

Data Injection Attacks are one of the oldest and the most widespread method for attacking web applications, networks, or any kind of system that uses a database. It may cause data loss, data leakage, or loss of data integrity. This attack type is a common problem in E-health systems. In an injection attack, an attacker sends a malicious executable input in query format into to a targeted system. This malicious input is processed by the program. The target program considers this input as a part of a command or a query. In turn, this alters the execution of that program. According to [50], this attack is listed as the number one web application security risk in The Open Web Application Security Project (OWASP) Top 10. A Diagram of the injection attack is given in Figure 7.

A false data injection attack sends a malicious executable data input to the targeted network. This input is processed by the target processor as an ordinary program command. This command initiates an operation that will change the natural execution of the target program or network. Generally, cross-site scripting (XSS) and SQL injections are very common attacks on E-health systems. Depending on the query injected, the attack may redirect itself to other nodes and infect them. This spread causes systems battery power to exhaust and reduce network lifetime. The attack may also redirect the older system messages over and over again, which may lead to severe consequences.

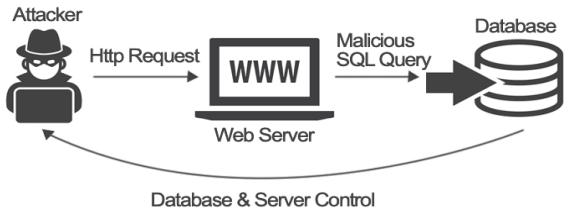

Figure 7. The diagram of Injection Attack.

Here, we have explained six attacks with ground robots. Actually, these attacks are the most common attack types that occur in the wild and significantly affects the society. As it is explained, each attack has different properties that have been used to compromise security requirements of systems. Additionally, DDOS attacks have become more common during COVID-19 pandemic, which has become a significant threat for human life.

6. Analysis of Security Attacks

6.1 DDoS Attack

There are four main steps of a successful DDoS attack:

- Recruiting agents by exploiting vulnerable devices.
- Propagation of attack toolkits into new agents.
- Establishing a DDoS network.
- Sending packets to conduct the attack [51].

DDoS attacks may target any layer of Open Systems Interconnection (OSI) reference model. Recently, network and transport layers are targeted in IoT networks, including wearable devices [52]. Specifically, attacks on wearable medical devices use transport layer to impair the communication between the wearable health device and the master device which sends data to a remote server. Robots initiate the attack by scanning the network in a medical center. These

networks are likely to have vulnerable devices such as smartphones and personal computers which may be exploited and recruited as agents or zombies. After the recruitment agents, robots may use some tools to automate this step.

There are three common methods for propagation step, which are central source propagation, back-chaining propagation, and autonomous propagation [53]. In central source propagation, after the compromise of a vulnerable host, the code that enables the attacks is copied from a central server. In the back-chaining propagation, the code is copied from the attacking hosts into compromised hosts. Autonomous propagation does not require an extra step for the propagation.

The code that enables the agents to carry out attacks is sent when devices are exploited. All of these attack types are shown in Figure 8. For methods presented in this paper, the autonomous propagation is preferred as the handler robots that already has the attack toolkit. Additionally, it may freely send the tools to vulnerable hosts when they exploit them. After the attacker has recruited agents and has gotten all the necessary code into them, a secure network needs to be established in order to keep track of and manage the actions of all the devices included in the growing list of exploited devices.

There are three different methods a botnet to be constructed in terms of communication with agents, namely agent-handler model, Internet Relay Chat (IRC) model, and web-based model [54]. In the agent handler model, attackers use handlers to control agents and the communication is direct between handlers and attackers. In the IRC model, attackers make use of an online chat system to communicate directly with agents. An example of a botnet using this type of architecture may be agobot [55]. The last type of architecture is the web-based model which is the newer one of the three architectures. In this model, the attacker uses encrypted web communication and PHP scripts to control bots. This last architecture offers several improvements over the IRC model [56].

An attack is ready to be carried out after the network is set. The attacker simply sends a command to handlers, which tells agents to flood the network with an excessive number of unusual packets. There are different types of attack, such as TCP, Internet Control Message Protocol (ICMP), and User Datagram Protocol (UDP) floods. These attack types remain usually the same since the initial DoS attack may be used without any changes. The first countermeasure should be preventing DDoS attacks through various IP filtering techniques. History based IP filtering [57] is one of the ways IP filtering may be applied that may be successfully used with WBANs. Honeypots are another prevention technique that works by diverting the attack within a honeypot instead of the real target [58].

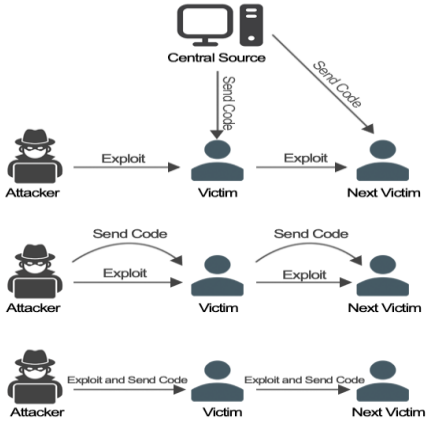

Figure 8. From top to bottom, central source propagation, back-chaining propagation, and autonomous propagation [53].

Prevention methods may not prevent all of the attacks so IDS should also be used to secure a network against attacks. IPv6 over low-power wireless personal area networks or 6LowPAN protocol is the common protocol used for wireless body area networks. Monitoring the energy consumption on 6LowPAN to detect unusual traffic is one of methods to detect DDoS attacks successfully [59]. Machine learning algorithms are also widely used for DDoS detection and simple supervised learning algorithms such as random forests may provide adequate results [60, 61]. Deep learning architectures have been the latest focus area in the intrusion detection research since they offer high accuracy and generality [62]. Different research showed that these architectures outperform the traditional machine learning algorithms [63, 64].

6.2. Jamming Attack

Normally, a jammer does not follow the MAC layer protocol as a regular wireless transmitter. Normal transmitters use Carrier-Sense Multiple Access (CSMA), which is a method used to avoid collisions during signal transmission between nodes. Jammers bypass this CSMA protocol by occupying the receiver with a stronger signal for long time intervals. This makes other transmitters inactive during this time slot. This approach prevents target response to the sources signals then blocks the communication [39]. This leads to packet drops, high packet error rates, reduced throughput, and long delay.

Jammers do not use MAC layer protocol that may interrupts active transmission traffic, which increases Bad Packet Ratio (BPR) and Energy Consumption Amount (ECA) and decrease Packet Delivery Ratio (PDR) [65]. The type of jamming attack determines the range of blocked transmission signals. Wireless sensor networks are prone to jamming attacks because of their limited memory, low battery resources, and slow processing capabilities. For a mobile contact tracing solution related to fighting COVID-19, jamming attack may be used to amplify extremely weak Global Positioning System (GPS) signals. Moreover, many E-health applications do not use any countermeasure against interference. Notch filter or adaptive notch filters may be used for GPS attack detection in contact tracing phones [66].

6.3. De-authentication Attack

The authentication process requests an active connection. After a successful authentication which has two acknowledged authentication frames, the client requests the association. Then, all management frames are broadcasted as plain-text. Therefore, the closest device finds the network and requests a connection. If an attacker captures this plain-text management frame, it can modify a package that seems to come from the victim [67]. This process is shown in Figure 9.

The access point, where the attack is made, has a channel, SSID, and station information. MAC addresses of devices connected to this access point are accessed prior to the attack. The client that connects to the MAC address found during the attack is removed from the network. This may be done easily using the already existing tools. At the same time, de-authentication packets are sent to the patient's device with the MAC address found using this tool, and the client is dropped from the network for a short time. The client in the system is the patient in our E-health system.

Another version of de-authentication attack is shown in Figure 10. The attack may be performed against the access point without specifying any connected client device. When a de-authentication attack is performed on patient's device, the client device droops from the network and tries to reconnect to the access point. As a result of the output obtained by using the tool like airodump-ng, target access points are detected. Later, an attack is made to the access point to obtain the hidden

SSID information from within the probe request frames. When our patient requests a connection to the network again, the real value of the hidden SSID is being found. For example, an attacker could create an unprotected active software access point (SoftAP) that carries the same SSID as the actual network. It may temporarily turn off all IoT devices by simulating broadcast authentication packets. Herein, IoT devices try to reconnect to the same SSID and SoftAP with the strongest signal. It has been argued that advanced operating systems may prevent attacks, but many IoT devices may be prone to this attack [68].

Since a ground robot is a type of Unmanned Ground Vehicle (UGV), de-authentication attack may be done to disconnect the patient to get it connected to the UGV [39]. One solution to prevent an authentication attack using a session management system involves the use of encryption [69]. Another solution is with DoS attack detection. The deauthentication attack is carried out using the WiFi Deauther program with an IDS program running in their gateway devices. These may identify the WiFi deauthentication, TCP SYN flood, and Mirai botnet attacks to protect the system by blocking the origin of these attacks [70].

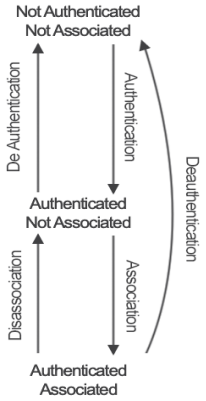

Figure 9. Authentication and Association steps of the system [67].

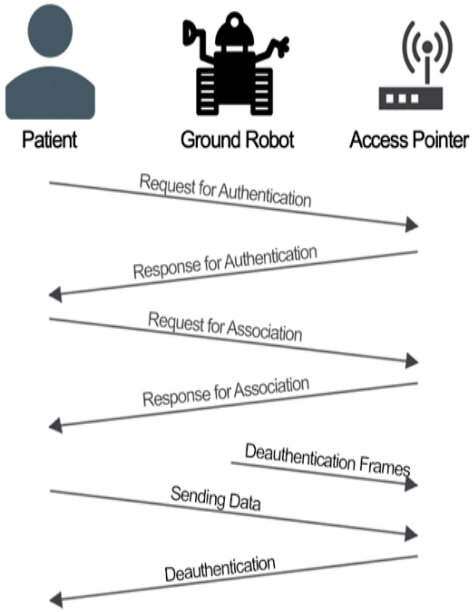

Figure 10. Flow analysis of de-authentication attack.

6.4. Evil Twin Attack

The steps of evil twin attack are as follows:

1) Network scan is performed.
2) The target network is selected.
3) Handshake data is collected.
4) A fake access point is created on the same channel with the same name.
5) Dynamic Host Configuration Protocol (DHCP) server setup is completed via an access point.
6) A DNS server is set up to direct all requests to the host side.
7) A mechanism is created for comparing passwords with handshake data.
8) De-authentication packets are sent to clients on the network to throw them from the network.
9) Victims are expected to fall into the trap. The password will appear on the screen as soon as they entered it correctly.

While the devices are connecting, they need to agree with each other. If the packets are confirmed by the receiving device during the packet transmission, the negotiation is successful, and the connection is established. Specifically, the device that connects to a wireless network sends the password to the modem and gets a response. If the password is correct, it connects to the modem and the Internet. The ground robot is not exactly inserting itself into the middle of a data stream between WiFi and a target device. The robot behaves like a receiver for wearable connected devices which may be phones, computers that are connected to wearable BAN and IMD devices. During an attack, tactical robots should be in a high position in the access range of the targeted network. Finally, the goal is to force patients to authenticate again to the system with remote control feature of robots to a fake access point.

WiFi Pineapple may be used in tactical robots which automates much of the labor required to set up an Evil Twin attack. Attackers start by broadcasting the same SSID when they are within range of the target SSID. It is simple to implement, even for smartphones that allow sharing of mobile WiFi access points. During the operation of the WiFi Pineapple, if the target SSID is busy, clients will connect to the evil twin AP. If the target is a private, Pre-Shared Key (PSK) encrypted SSID, then the attacker will need knowledge of the PSK. Patients are going to be the ones who connected to their access points with auto-join. The attack will finish if a patient is connected to the evil twin access point, which is a clone of the original one. The entire process is used to inject malware or backdoors onto devices that connect multiple wearable devices for remote access. When patients log in to their E-health account to access or check their health information, they may believe that the wearable IoT device is connected to the WiFi network, even though they are actually giving their credentials to an attacker.

6.5. Eavesdropping Attack

There are two type eavesdropping attacks, namely passive and active attacks. In passive attack, the attacker does not need to neither active connection nor an active implementation. This type of attack is more suitable for ground robot attacks as shown in Figure 11. An attacker may attempt to listen network communications at any point when a patient's body sensors try to connect with the hospital servers using an unsecured wireless network. The ground robot may locate the insecure wireless networks by a WiFi monitoring application. The robot may stroll around the hospitals or nearby neighborhoods to detect these insecure connections. Ground robots geared a simple WiFi

monitoring implementation that may be able to determine the exact GPS coordinates, network names or SSIDs, encryption, channels, and signal strengths of open local wireless networks. Steps to prevent eavesdropping attack:

- Change default SSIDs and passwords regularly.
- Update the firmware of the connected devices on the line, such as routers.
- Apply cooperative jamming [71].
- Improve on the relay value determination for the network [72].
- Use VPN on the body sensors' connection.
- Regularly review the logs of sensors and check suspicious logs of hospital.
- Directly utilize the patient's body as the transmission medium for the communication (Body-coupled communication) [73].
- Use advanced authentication tools for both login operations and the body sensor data transfer operations.
- Network segmentation.
- Implement a special agreement protocol only for sensor networks [74].

Although Body-Coupled Communication (BCC) method is not applicable for all types of medical sensors or healthcare systems, it looks like a strong solution for eavesdropping attacks [73]. BCC has a limited communication range due to the proximity of the body that the sensors or the devices are used for treatment or monitoring of the patient [75]. It is one of the major advantages of the BCC to prevent eavesdropping. Implementation of BCC may also consume less power from the system since the transmitting is occurred directly over the body rather than the air [76].

The cooperative jamming method refers to increase the security on the network that the body sensor is connected. In the last decade, the physical layer security has shown that interference signals may result in decreasing the channel capacity [77, 78, 79, 80]. The decreasing operation happens at the physical layer among the transmitter and the possible attacker that tries to eavesdrop on the system. It is suggested that the defender should not determine the optimal cooperative jamming signals assuming the possible eavesdropper will occur over one channel [71].

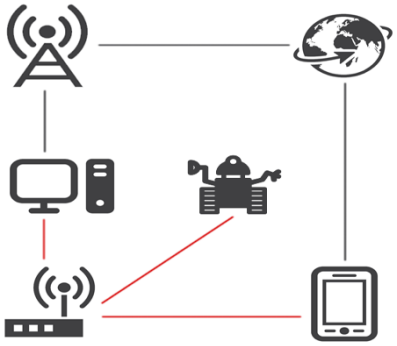

Figure 11. The diagram of injection attack.

6.6. False Data Injection Attack

False data Injection Attacks may cause severe damages to database of targeted systems. In this attack, an attacker sends a request to access the website just as a usual user. If the security of the website is not well protected, the attacker may send a query into the database from user allowed inputs like "username" or "password" sections. For example, Username: "SELECT * FROM users

WHERE username = ‘administrator’ AND password = ‘’”. This query is processed as an SQL query. It is sent to the database and retrieves the asked results to the attacker instantly.
Actually, there are different methods of injecting queries. But once the security is bypassed, the attacked may retrieve any information, or take control of the whole system. The attack may repeat itself by sending the same queries many times. This leads the system to have low availability.

We analyze the attacks with tactical ground robots, which may be controlled remotely and may play an active role in IoT attacks. These robots have comparatively small sizes, and they move easily in any terrain [81]. Specifically, we analyze six possible attacks with ground robots. DoS attacks prevent legitimate user or device to access services, or they simply reduce availability of targeted services [82]. A more complex version of DoS attacks is DDoS attack that initiates the attack from many different sources [83]. A jamming attack disrupts radio broadcasts, and it sends erroneous packets that affect signals during legitimate communications of wearable e-health devices [84, 85]. It is indicated that the first step in dealing with these attacks is to successfully detect attacks [86]. De-authentication attack is the third attack that we consider in this research. In this attack, attacker sends a de-authentication frame to clients to disconnect these clients from the network [87]. This attack may help to DoS attack by sending de-authentication frames to other parties in the system. Evil Twin attack is a type of MitM attack, which is referred as Fake Access Point [88]. In this attack, the attacker’s goal is to catch the connection between the device and the modem [89, 90]. In eavesdropping attack, attackers infiltrate a network and eavesdrop health information over wearable health devices from hospitals’ networks [91]. There exist two different types of eavesdropping attacks that may be used with wearable E-health devices, namely passive or active attacks [92]. False data injection attack infiltrates a network or a system. An attacker attempts to perform an injection by using ground robots. This attack exploits common database vulnerabilities that occur due to human mistakes, such as simple errors made by a database administrator or programmer who coded the system [93]. Briefly, the attack tries to disrupt the working E-health system by sending incorrect data.

Recently, COVID-19 pandemic has become the center of human life. We explore COVID-19 security cases on E-health systems that are related to attacks with ground robots. Our investigations show that there is an increase of attack on IoT based wearable devices during the pandemic [94, 95]. While many systems are being developed specifically for COVID-19 and similar systems, the security of these systems need to be analyzed carefully [96, 97]. Additionally, there are some specific security solutions for E-health systems that use COVID-19 data [98].

Security of E-health systems is a key issue for societies. The protection of wearable E-health devices and the prevention attacks are therefore a key challenge to secure E-health systems [99]. IoT and wearable E-health devices are still in their development stage, hence every improvement will have a significant effect on the security of the E-health [100]. Additionally, health professionals and patients are responsible to protect personal data [101, 102, 103, 104]. Thus, a huge effort is needed to protect wearable E-health devices against attacks with ground robots.

In this research, we analyze six attacks with ground robots that affects E-Health systems. Analyses results show that some attacks on E-health systems are going to increase considerably. Particularly, DDOS attacks are a very common type of attacks that targets E-health systems. Moreover, this type of attack on E-health systems have increased considerably since the beginning of COVID-19 pandemic. Additionally, the other five types of attacks have become popular to compromise E-health systems.

7. Conclusion

In this research, we highlighted key issues and main vulnerabilities of IoT devices that are used in healthcare environments. Moreover, we provided a guideline for security requirements, vulnerabilities, attacks, and countermeasures in wearable E-health devices. Additionally, we investigated attacks with ground robots on wearable E-health devices. Particularly, we focused on the following four issues:

- A detailed overview of a typical wearable healthcare devices and their architecture were presented.
- Potential security and privacy attacks on healthcare devices by using ground robots in the military field were investigated.
- Analysis of existing attacks and their existing solutions were analyzed and discussed in order to mitigate the attacks.
- Security attacks on E-health systems that contain COVID-19 data was analyzed.

To sum up, the paper contains a comprehensive survey about security attacks with ground robots on wearable E-health devices. Moreover, the survey covers attacks that have had significant effects on E-health systems processing COVID-19 data.

Authors' Contributions

All authors read and approved the final manuscript.

Competing Interests

The authors declare that they have no competing interests.

References

[1]. Butpheng C., Yeh K., and Xiong H., Security and privacy in IoT-cloud-based e-health systems—a comprehensive review, Symmetry, 2020, 12:1191.
[2]. Ahmed M., and Ullah A. SSM. B., False data injection attacks in healthcare, In Australasian Conference on Data Mining, Springer, 2017, 192–202.
[3]. Islam S. M. R., Kwak D., Kabir M. H., Hossain M., and Kwak H., The internet of things for health care: A comprehensive survey, IEEE Access, 2015, 3:678–708.
[4]. Holler J., Tsiatsis V., Mulligan C., Karnouskos S., Avesand S., and Boyle D., From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence, Academic Press, Inc. 6277 Sea Harbor Drive Orlando, FL, United States, 2014.
[5]. Yu L., Lu Y., and Zhu X. J., Smart hospital based on internet of things, 2012, Journal of Networks, 7(10):1654-1661.
[6]. Efe A., Aksoz E., Hanecioğlu N, and Yalman Ş. N., Smart security of IoT against to ddos attacks, International Journal of Innovative Engineering Applications, 2019, 2:35 – 43.
[7]. Al-Issa Y., Ottom M. A., and Tamrawi A., E-health cloud security challenges: A survey, Journal of Healthcare Engineering, 2019, 2019:1–15.
[8]. Kintzlinger M., and Nissim N., Keep an eye on your personal belongings! the security of personal medical devices and their ecosystems, Journal of Biomedical Informatics, 2019, 95:103233.

[9]. McCall M. K., Skutsch M. M., and Honey-Roses J., Surveillance in the COVID-19 normal: Tracking, tracing, and snooping–trade-offs in safety and autonomy in the e-city, International Journal of E-Planning Research, 2021, 10(2):27–44.
[10]. Hiremath S, Yang G., and Mankodiya K., Wearable Internet of things: Concept, architectural components and promises for person-centered healthcare, 4th International Conference on Wireless Mobile Communication and Healthcare, Athens, Greece, November 3-5, 2014, 304–307.
[11]. Otto C., Milenkovic A., Sanders C., and Jovanov E., System architecture of a wireless body area sensor network for ubiquitous health monitoring, Journal of Mobile Multimedia, 2006, 1:307–326.
[12]. Al-Janabi S., Al-Shourbaji I., Shojafar M., and Shamshirband S., Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications, Egyptian Informatics Journal, 2017, 18(2):113–122.
[13]. Karmakar N. C., Yang Y., and Rahim A., Microwave Sleep Apnoea Monitoring, Series in BioEngineering, Springer, 2018.
[14]. Darwish A., and Hassanien A. E., Wearable and implantable wireless sensor network solutions for healthcare monitoring, Sensors, 2011, 11(6):5561–5595.
[15]. Milenkovic A., Otto C., and Jovanov E., Wireless sensor networks for personal health monitoring: Issues and an implementation, Computer Communications, 2006, 29:2521–2533.
[16]. Fu K., and Xu W., Risks of trusting the physics of sensors, Communications of the ACM, 2018, 61(2):20–23.
[17]. Halperin D., Heydt-Benjamin T. S., Ransford B., Clark S.S., Defend B., Morgan W., Fu K., Kohno T., and Maisel W. H., Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses, In 2008 IEEE Symposium on Security and Privacy (SP 2008), Oakland, California, USA, 2008, 129–142.
[18]. Trippel T., Weisse O., Xu W., Honeyman P., and Fu K., Walnut: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks, In 2017 IEEE European symposium on security and privacy (EuroS&P), Paris, France, 3–18, April 26-28, 2017.
[19]. Xue Q., and Chuah M. C., New attacks on RNN based healthcare learning system and their detections, Smart Health, 2018, 9:144–157.
[20]. Ly B., and Ly R., Cybersecurity in unmanned aerial vehicles, Journal of Cyber Security Technology, 2020, 1–18.
[21]. Kristiyanto Y., and Ernastuti E., Analysis of de-authentication attack on IEEE 802.11 connectivity based on IoT technology using external penetration test, Communication and Information Technology Journal, 2020, 14(1):45–51.
[22]. Sethuraman S. C., Vijayakumar V., and Walczak S., Cyber-attacks on healthcare devices using unmanned aerial vehicles, Journal of medical systems, 2020, 44(1):1–10.
[23]. Hanspach M., and Goetz M., On covert acoustical mesh networks in air, arXiv preprint arXiv:1406.1213, 2014.
[24]. Karchowdhury S., and Sen M., Survey on attacks on wireless body area network", International Journal of Computational Intelligence & IoT, Forthcoming, 2019, 638-644.
[25]. Eian I. C., Yong L. K., Li M. J. X., Qi Y. H., and Fatima Z., Cyber-attacks in the era of COVID -19 and possible solution domains, Preprints, 2020.
[26]. Khan N. A., Brohi S. N., and Zaman N., Ten deadly cyber security threats amid COVID-19 pandemic, Preprints, 2020.
[27]. Kamal M, Aljohani A., and Alanazi E., IoT meets COVID-19: Status, challenges, and opportunities, arXiv preprint arXiv:2007.12268, 2020.
[28]. Lallie H. S., Shepherd L. A., Nurse J, Erola A., Epiphaniou G., Maple C., and Bellekens X., Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic, arXiv preprint arXiv:2006.11929, 2020.
[29]. Gvili Y., Security analysis of the COVID-19 contact tracing specifications by apple inc. and google inc, IACR Cryptol. ePrint Arch., 2020, 2020:428.

[30]. Chamola V., Hassija V., Gupta V., and Guizani M., A comprehensive review of the COVID-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact, IEEE Access, 2020, 8:90225– 90265.
[31]. Rahman A., Hossain M. S., Alrajeh N A., and Alsolami F., Adversarial examples–security threats to COVID-19 deep learning systems in medical IoT devices, IEEE Internet of Things Journal, 2020, 99:1-1.
[32]. Pranggono B., and Arabo A., COVID-19 pandemic cybersecurity issues, Internet Technology Letters, 2020, 4(2):1-6, 2020.
[33]. Wueest C., The continued rise of DDOS attacks. White Paper: Security Response" Symantec Corporation, 2014.
[34]. Mirkovic J., and Reiher P., A taxonomy of DDOS attack and DDOS defense mechanisms, ACM SIGCOMM Computer Communication Review, 2004, 34(2):39–53.
[35]. Pathan A. K., Lee H., and Hong C. S., Security in wireless sensor networks: issues and challenges, In 2006 8th International Conference Advanced Communication Technology, Phoenix Park, Korea, 1043-1048, 20-22 Feb., 2006.
[36]. Chadd A., Ddos attacks: past, present and future, Network Security, 2018, 2018(7):13–15.
[37]. Zaroo P., A survey of ddos attacks and some ddos defense mechanisms, Advanced Information Assurance (CS 626), 2002.
[38]. Mpitziopoulos A., Gavalas D., Konstantopoulos C., and Pantziou G., A survey on jamming attacks and countermeasures in WSNS, IEEE Communications Surveys & Tutorials, 2009, 11(4):42– 56.
[39]. Chamola V., Kotesh P., Agarwal A., Gupta N. N., and Guizani M., A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques, Ad Hoc Networks, 2021, 111:102324.
[40]. Chuyang Z., Shang G., Jianyi X., Jianwen H., Qiang L., Kaitong H., Jutao H., and Ruiwen M., Method research and realization of noise fm jamming based on DDS technology, Journal of Physics: Conference Series, 2020, 1437, 012122.
[41]. Zheng F., Haitao L., and Yiming Q., Cognitive anti-jamming receiver under phase noise in high frequency bands, Journal of Systems Engineering and Electronics, 2018, 29(1):31–38.
[42]. Kolias C., Kambourakis G., Stavrou A., and Gritzalis S., Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset, IEEE Communications Surveys & Tutorials, 2015, 18(1):184–208.
[43]. Cho E. J., Kim J. H., and Hong C. S., Attack model and detection scheme for botnet on 6lowpan, Management Enabling the Future Internet for Changing Business and New Computing Services, Springer, Berlin, Heidelberg, 2009, 515–518.
[44]. Krimmling J., and Peter S., Integration and evaluation of intrusion detection for coap in smart city applications, In 2014 IEEE Conference on Communications and Network Security, San Francisco, CA, USA, 2014, 73–78.
[45]. Gong S., Ochiai H., and Esaki H., Scan based self-anomaly detection: Client-side mitigation of channel-based man-in-the-middle attacks against wi-fi, In 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 1498–1503, 13-17 July, 2020.
[46]. Modi V., and Parekh C., Detection & analysis of evil twin attack in wireless network, International Journal of Advanced Research in Computer Science, 2017, 8(5).
[47]. Das S. K., Kant K., and Zhang N., Handbook on securing cyber-physical critical infrastructure, Elsevier, 2012.
[48]. Zeadally S., Isaac J. T., and Baig Z., Security attacks and solutions in electronic health (e-health) systems, Journal of medical systems, 2016, 40(12):1– 12.
[49]. Al Ameen M., Liu J., and Kwak K., Security and privacy issues in wireless sensor networks for healthcare applications, Journal of medical systems, 2012, 36(1):93–101.

[50]. Muscat I., What are injection attacks. Dostopno prek, https://www. acunetix. com/blog/articles/injectionattacks, 2017.
[51]. Long N., and Thomas R., Trends in denial-of-service attack technology, CERT Coordination Center, 2001, 648–651.
[52]. Perakovic D., Perisa M., and Cvitic I., Analysis of the iot impact on volume of ddos attacks., XXXIII Simpozijum o novim tehnologijama u postanskom i telekomunikacionom saobracaju–PosTel, 2015, 2015:295–304.
[53]. Mahjabin T., Xiao Y, Sun G, Jiang W., "A survey of distributed denial-of-service attack, prevention, and mitigation techniques", 2017, International Journal of Distributed Sensor Networks, 13(12):1550147717741463.
[54]. Alomari E., Manickam S., Gupta BB., Karuppayah S., and Alfaris R., Botnetbased distributed denial of service (DDOS) attacks on web servers: classification and art, arXiv preprint arXiv:1208.0403, 2012.
[55]. McLaughlin L., Bot software spreads, causes new worries, IEEE Distributed Systems Online, 2004, 5(6):1.
[56]. Hoque N., Bhattacharyya D. K., and Kalita J. K., Botnet in DDOS attacks: trends and challenges, IEEE Communications Surveys & Tutorials, 2015, 17(4):2242–2270.
[57]. Peng T., Leckie C., and Ramamohanarao K., Protection from distributed denial of service attacks using history-based ip filtering, In IEEE International Conference on Communications, 2003. ICC '03., Anchorage, AK, USA, 1:482–486, 20 June, 2003.
[58]. Weiler N., Honeypots for distributed denial-of-service attacks, In Proceedings. Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Pittsburgh, PA, USA, 109–114, 12 June, 2002.
[59]. Lee T., Wen C., Chang L., Chiang H., and Hsieh M., A lightweight intrusion detection scheme based on energy consumption analysis in 6lowpan, Advanced Technologies, Embedded and Multimedia for Human-centric Computing, 2014, 1205–1213.
[60]. Bindra N., and Sood M., Detecting DDOS attacks using machine learning techniques and contemporary intrusion detection dataset, Automatic Control and Computer Sciences, 2019, 53(5):419–428.
[61]. Al-Gethami K. M., Al-Akhras M. T., and Alawairdhi M., Empirical evaluation of noise influence on supervised machine learning algorithms using intrusion detection datasets, Security and Communication Networks, 2021, 2021:1-28.
[62]. Liu H., and Lang B., Machine learning and deep learning methods for intrusion detection systems: A survey, Applied Sciences, 2019, 9(20):4396.
[63]. Yin C., Zhu Y., Fei J., and He X., A deep learning approach for intrusion detection using recurrent neural networks, IEEE Access, 2017, 5:21954– 21961.
[64]. Khan M. A., Karim M., and Kim Y., A scalable and hybrid intrusion detection system based on the convolutional-lstm network, Symmetry, 2019, 11(4):583.
[65]. Cheng M., Ling Y., and Wu W. B., Time series analysis for jamming attack detection in wireless networks, In GLOBECOM 2017, IEEE Global Communications Conference, Singapore, 1–7., 4-8 December, 2017.
[66]. Dar A. B., Lone A. H., Zahoor S., Khan A. A., and Naaz R., Applicability of mobile contact tracing in fighting pandemic (COVID-19): Issues, challenges and solutions, Computer Science Review, 2020, 100307.
[67]. Milliken J., Selis V., Yap K. M., and Marshall A., Impact of metric selection on wireless deauthentication dos attack performance, IEEE Wireless Communications Letters, 2013, 2(5):571–574.
[68]. Kolias C., Stavrou A., Voas J., Bojanova I, and Kuhn R., Learning internet of-things security hands-on, IEEE Security & Privacy, 2016, 14(1):37–46.
[69]. Arora A., Preventing wireless deauthentication attacks over 802.11 networks, arXiv preprint arXiv:1901.07301, 2018.

[70]. Remesh A., Muralidharan D., Raj N., Gopika J., and Binu P. K., Intrusion detection system for IoT devices, In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2020, 826–830.
[71]. Park N., Sun K., Foresti S., Butler K., and Saxena N., Security and Privacy in Communication Networks, Springer SecureCom2020, Washington DC, USA, 21-23 October, 2020.
[72]. Zou Y., and Wang G., Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack, IEEE Transactions on Industrial Informatics, 2016, 12(2):780–787.
[73]. Li C., Raghunathan A., and Jha N. K., Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system, In 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, Location: Columbia, MO, USA, 13-15 June, 2011, 150–156.
[74]. Challa S., Das A. K., Odelu V., Kumar N., Kumari S., Khan M. K., and Vasilakos A. V., An efficient ecc-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks, Computers Electrical Engineering, 2018, 69:534–554.
[75]. Yoo H., Song S., Cho N., and Kim H., Low energy on-body communication for BSN, In 4th International Workshop on Wearable and Implantable Body Sensor Networks (BSN 2007), Aachen University, Germany, 26-28 March, 2007, 15–20.
[76]. Baldus H., Corroy S., Fazzi A., Klabunde K., and Schenk T. Human-centric connectivity enabled by body-coupled communications, IEEE Communications Magazine, 2009, 47(6):172–178.
[77]. Goel S., and Negi R., Guaranteeing secrecy using artificial noise, IEEE transactions on wireless communications, 2008, 7(6):2180–2189.
[78]. Rabbachin A., Conti A., and Win M. Z., Intentional network interference for denial of wireless eavesdropping, In 2011 IEEE Global Telecommunications Conference-GLOBECOM 2011, Houston, Texas, USA, 5-9 December, 2011, 1–6.
[79]. Tang X., Liu R., Spasojevic P., and Poor H. V., Interference assisted secret communication, IEEE Transactions on Information Theory, 2011, 57(5):3153–3167.
[80]. Tekin E., and Yener A., The gaussian multiple access wire-tap channel: wireless secrecy and cooperative jamming, In 2007 Information Theory and Applications Workshop, La Jolla, CA, USA, 29 Jan.-2 Feb., 2007, 404–413.
[81]. Endo Y., Arkin R. C., and Collins T. R., Tactical mobile robot mission specification and execution, Georgia Tech, 1999, 150-163.
[82]. Donno M. D., Dragoni N., Giaretta A., and Spognardi A., Analysis of DDOS-capable IoT malwares, 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), Prague, Czech Republic, 3-6 September, 2017, 807–816.
[83]. Dulik M., Network attack using TCP protocol for performing dos and ddos attacks, In 2019 Communication and Information Technologies (KIT), Tatranské Zruby, SK, 9-11 October, 2019, 1–6.
[84]. Bengag A., Moussaoui O., and Moussaoui M., A new ids for detecting jamming attacks in wban, In 2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS), Marrakech, Morocco, 28-30 October, 2019, 1–5.
[85]. Xu W., Ma K., Trappe W., and Zhang Y., Jamming sensor networks: attack and defense strategies, IEEE Network, 2006, 20(3):41–47.
[86]. Namvar N., Saad W., Bahadori N., and Kelley B., Jamming in the internet of things: A game-theoretic perspective, In IEEE Global Communications Conference (GLOBECOM 2016), Washington, DC, USA, 4-8 December, 2016, 1–6.
[87]. Raghuprasad A., Padmanabhan S., Babu M. A., and Binu P. K., Security analysis and prevention of attacks on IoT devices, In 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 28-30 July, 2020, 0876–0880.

[88]. Lovinger N., Gerlich T., Martinasek Z., and Malina L., Detection of wireless fake access points, 12th International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), Brno, Czech Republic, 5-7 October, 2020, 113– 118.
[89]. Gonzales H., Bauer K., Lindqvist J., McCoy D., and Sicker D., Practical defenses for evil twin attacks in 802.11, IEEE Global Telecommunications Conference GLOBECOM 2010, Miami, FL, USA, 6-10 December, 2010, 1–6.
[90]. Asaduzzaman M., Majib M. S., and Rahman M., Wi-fi frame classification and feature selection analysis in detecting evil twin attack, In 2020 IEEE Region 10 Symposium (TENSYMP), Dhaka, Bangladesh, 5-7 June, 2020, 1704–1707.
[91]. Damghani H., Damghani L., Hosseinian H., and Sharifi R., Classification of attacks on IoT, In 4th International Conference on Combinatorics, Cryptography, Computer Science and Computation, Tehran, Iran, 20-21 November, 2019.
[92]. Yang W., Zheng Z., Chen G., Tang Y., and Wang X., Security analysis of a distributed networked system under eavesdropping attacks, IEEE Transactions on Circuits and Systems II: Express Briefs, 2019, 67(7):1254–1258.
[93]. Bostami B., Ahmed M., and Choudhury S., False data injection attacks in internet of things, In Performability in Internet of Things, Springer, 2019, 47–58.
[94]. Javaid M., and Khan I. H., Internet of things (IoT) enabled healthcare helps to take the challenges of COVID-19 pandemic, Journal of Oral Biology and Craniofacial Research, 2021, 11(2):209-2014.
[95]. Ndiaye M., Oyewobi S. S., AbuMahfouz A. M., Hancke G. P., Kurien A. M., and Djouani K., IoT in the wake of COVID-19: A survey on contributions, challenges and evolution, IEEE Access, 2020, 8:186821–186839.
[96]. Scott B. K., Miller G. T, Fonda S. J., Yeaw R. E., Gaudaen J. C., Pavliscsak H. H., Quinn M. T., and Pamplin J. C., Advanced digital health technologies for COVID-19 and future emergencies, Telemedicine and e-Health, 2020, 26(10):1226–1233.
[97]. Sust P. P., Solans O., Fajardo J. C., Peralta M. M., Rodenas P., Gabalda J, Eroles L. G., Comella A., Munoz C. V., and Ribes J. S., Turning the crisis into an opportunity: digital health strategies deployed during the COVID-19 outbreak, JMIR public health and surveillance, 2020, 6(2):e19106.
[98]. Pappot N., Taarnhøj G. A., and Pappot H., Telemedicine and e-health solutions for COVID-19: patients' perspective, Telemedicine and e-Health, 2020, 26(7):847–849.
[99]. Abie H., and Balasingham I., Risk-based adaptive security for smart IoT in e-health, In Proceedings of the 7th International Conference on Body Area Networks, Oslo Norway, 24-26 September, 2012, 269–275.
[100]. Blobel B., Comparing approaches for advanced e-health security infrastructures, International Journal of Medical Informatics, 2007, 76(5-6):454–459.
[101]. Haşıloğlu A, Yücel Altay S, and Ertaş U., Sağlık Hizmetlerinde Aykırı Dataların Kestirimi İçin Mekansal Zamansal Veri Madenciliğinin Kullanımı, El-Cezerî Journal of Science and Engineering, 2017, 4(3): 411-428.
[102]. Wilkowska W., and Ziefle M., Privacy and data security in e-health: Requirements from the user's perspective, Health Informatics Journal, 2012, 18(3):191–201.
[103]. Simpson T. S. L., and Lane B., Security and privacy in e-health: Is it possible?, In 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services, Lisbon, PT, 9-12 October, 2013, 249–253.
[104]. Güvernoğlu E., and Razbonyalı C., The Creation of Maze in Order to Hide Data, and the Proposal of Method Based on AES Data Encryption Algorithm, El-Cezerî Journal of Science and Engineering, 2019, 6(3):668-680.