electronics

MDPI

Review

A Survey on MAC-Based Physical Layer Security over Wireless Sensor Network

Attique Ur Rehman [1,2], Muhammad Sajid Mahmood [3], Shoaib Zafar [2], Muhammad Ahsan Raza [4], Fahad Qaswar [5], Sumayh S. Aljameel [6], Irfan Ullah Khan [6] and Nida Aslam [7,*]

[1] Department of Computer Science, School of System and Technology, University of Management and Technology, Lahore 54000, Pakistan
[2] Department of Computer Science, Lahore Garrison University, Lahore 54000, Pakistan
[3] Department of Informatics and Systems, School of System and Technology, UMT, Lahore 54000, Pakistan
[4] Department of Information Technology, Bahauddin Zakariya University, Multan 60000, Pakistan
[5] Faculty of Computing, College of Computing & Applied Science, University Malaysia Pahang, Pekan, Pahang 26600, Malaysia
[6] Department of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia
[7] SAUDI ARAMCO Cybersecurity Chair, Department of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia
* Correspondence: naslam@iau.edu.sa

Abstract: Physical layer security for wireless sensor networks (WSNs) is a laborious and highly critical issue in the world. Wireless sensor networks have great importance in civil and military fields or applications. Security of data/information through wireless medium remains a challenge. The data that we transmit wirelessly has increased the speed of transmission rate. In physical layer security, the data transfer between source and destination is not confidential, and thus the user has privacy issues, which is why improving the security of wireless sensor networks is a prime concern. The loss of physical security causes a great threat to a network. We have various techniques to resolve these issues, such as interference, noise, fading in the communications, etc. In this paper we have surveyed the different parameters of a security design model to highlight the vulnerabilities. Further we have discussed the various attacks on different layers of the TCP/IP model along with their mitigation techniques. We also elaborated on the applications of WSNs in healthcare, military information integration, oil and gas. Finally, we have proposed a solution to enhance the security of WSNs by adopting the alpha method and handshake mechanism with encryption and decryption.

Keywords: MAC; physical layer; wireless sensor network; attack; challenges; security; cryptography

Citation: Rehman, A.U.; Mahmood, M.S.; Zafar, S.; Raza, M.A.; Qaswar, F.; Aljameel, S.S.; Khan, I.U.; Aslam, N. A Survey on MAC-Based Physical Layer Security over Wireless Sensor Network. *Electronics* **2022**, *11*, 2529. https://doi.org/10.3390/electronics11162529

Academic Editors: Houbing Song and Jehad Ali

Received: 26 June 2022
Accepted: 28 July 2022
Published: 12 August 2022

1. Introduction

Science and technology have worked together to make our lives much easier and more comfortable than ever [1]. Due to its various inventions and discoveries, human life has become much more comfortable and modernized. Nowadays, we are always connected to our mobile phones and computers twenty-four hours a day, and our data is maintained or saved either in our devices or in our cloud storage [2]. Therefore, in order to save our data from unauthorized access and from hackers, we use the different security approaches to make a network secure [3]. This paper covers the basic concept of secure networks in wireless medium along with its advantages, disadvantages and applications [4].

Wireless sensor network security is the process of making our devices such as smart phones [5], tablets, computers and all the other handheld portable devices secure along with the network to which they are connected [6]. It helps us to prevent other users who are unauthorized from accessing our devices and data so that our data cannot be manipulated [7]. Since we are more focused on the wireless medium, the most common threat which needs to be addressed is therefore to make our devices secure while using the internet, and for that, we use Wi-Fi networks [8]. Therefore, in Wi-Fi networks we use Wi-Fi security that contains Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) [9].

Wired Equivalent Privacy (WEP) was developed for the security of networks which were running on wireless medium in September 1999 [10]. As the name applies, it was designed in such a way that it could provide the same level of security as the wired mediums, but it was very hard to configure and had many security flaws [11]. WEP also managed to be broken, which exposed our personal data and devices easily to the hackers all over the internet [12]. Due to its drawbacks, many devices were updated with different security protocols which were configured on WEP, and it was officially abandoned by the Wi-Fi alliances in 2004 [13].

WEP is a security algorithm for IEEE 802.11 wireless networks, and it mainly consists of 10 or 26 hexadecimal digits which makes 40 or 104 bits, respectively [14]. In 2004, WEP-40 and WEP-104 (128 and 256 bits) were declared "dead" because of the frequent attacks and flaws [15]. Basically, WEP used to run based on two algorithms [9].

The first algorithm was RC4-Key Scheduled Algorithm (KSA) which converts the key of length ranging from 1 to 256 bits to numbers 0 to N. It works as it contains the two numbers "i" and "j" which are used as pointers to the element of S [8,16].

The second algorithm is RC4-Pseudo Random Generation Algorithm (PGRA). This algorithm works by generating a byte of random or pseudorandom characters from internal state and then updates the internal state [17,18].

As mentioned earlier, WEP was exposed to many attacks which made it a vulnerable protocol when it comes to security, and some of them include packet injection, fake authentication, FMS attack, Chop attack, and Kore K attack [19].

Wireless sensor networks (WSNs) are now a hot topic for study. After being deployed in dangerous, hostile, or isolated places, the sensors are typically left unattended. These nodes are constrained by their finite and nonrenewable energy supplies. One of the primary design goals for these sensing devices is energy efficiency [20]. In this paper, we outline the difficulties in developing a medium access control protocol, which is a protocol for wireless sensor networks. We discuss several protocols for the WSNs, highlighting their advantages and disadvantages whenever feasible [21]. Some cluster-based networks are also used in a WSN especially, the main tendency in this scenario being either distributed decision making via sharing information with nearby nodes till the cluster and its members are picked, or centralized decision making at the base station for the selection of the cluster and its members [22]. Due to excessive broadcasting, particularly in large networks, as well as ensuring a higher until a final decision is made, both strategies dramatically increase energy usage [23]. Our cutting-edge layer-based hybrid approach for selecting cluster heads and cluster members results in a cutting-edge WSN communication architecture [24].

MCDA, or multilayer cluster designing algorithm, improves network lifespan performance. To accomplish the goal, new time slot allocation methods, cluster head complete candidate minimization, and cluster member-selecting node association to cluster head all play key roles. Transmissions are reduced as a result of these MCDA incorporations [25].

Wireless sensor network-based security threats comprise three major factors as shown in Figure 1.

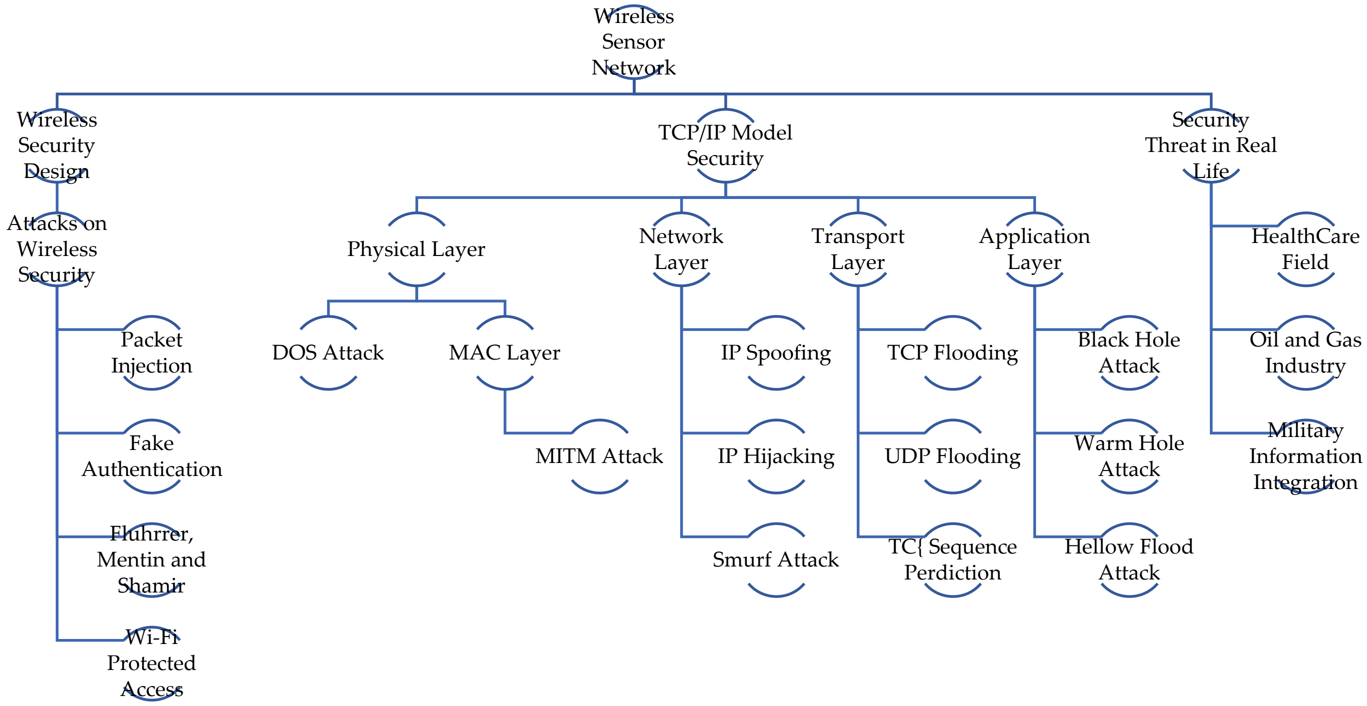

Figure 1. Wireless sensor network components-based security threats with types.

WSN-related literature are discussed in Section 2, and the technologies of wireless sensor network based on security attacks with its major components are presented in Section 3. An accurate discussion on a TCP/IP network model architecture based on five layers, with the different layers of security in the WSN used, is provided in Section 4. The industries currently providing useful, relevant information related to technologies that are necessary for investing in, in order to thwart WSN attacks, are explained in Section 5. Lastly, many aspects brought to light to improve the proposed solution to enhance the security of wireless networks, considering all its issues and challenges, are presented in Section 6.

2. Related Work

Wired communication is more protected and secured as compared to wireless communication, due to the fact that the broadcast nature of a wireless interface is open to everyone even for the client and also for an unauthorized person, whereas wired communication acts like peer-to-peer communication because only the concerned devices or users are connected to each other through wires [26]. That means that with the advancement of technology and living standards, we are becoming more and more exposed to hackers over the internet, and our data is not as secure as it used to be [27].

According to research, nowadays, almost forty percent of the overall population worldwide uses the Internet in their daily lives, and the number of personal mobile users reached 6.8 million [28,29]. Obviously, the increment of these devices will also lead to more cyber-crime-related activities, and in a 2012 report by Norton cybercrime, it was reported that people lose around EUR 83 billion due to fake online transactions, hacking of their data, financial information theft and fraud [30]. There is no doubt that certain measures need to be taken as people are now dependent on the Internet for shopping, business, banking, etc. [31].

The software-defined networks (SDN) paradigm may offer flexible routing and accommodate the various wireless sensor network (WSN) communication patterns. However, it is not simple to apply this approach to resource-constrained networks, especially if secure services are needed [32]. With time, resource-constrained requirements have been addressed by existing SDN-based techniques for WSNs. They do not, however, incorporate security services with their planning or execution. A secure-by-design SDN-based architecture for wireless sensor networks is the core contribution of this study [33]. Key features that the framework must offer are secure network admissions and an end-to-end main stream to facilitate secure communication. In light of device and protocol restrictions, we discuss its definition, design, implementation, and experimentation [34].

Software-defined networks (SDN) play a prominent role in the orchestration, programmability, dynamic configuration, flexible interaction, application of the innovative protocols, scalability, and robustness of a wireless sensor network (WSN). This is because SDN obtains a global view of the WSN, due to central management through the controller, which can improve the QoS through the selection schemes as illustrated in [35–37], as the controller in SDN applies the policies for controlling the behavior of the network and forwarding packets if its flow rules are not found in the SDN switches. Hence, controller selection and placement in the network is important in various technologies such as IoT [38,39] to provision the end-to-end (E2E) quality of service [40] and manage link failures in the network [41].

Many real-world WSN applications, including smart grids, smart agriculture, and smart health, would necessitate the deployment of tens of thousands to hundreds of thousands of sensor networks and actuators [42]. An efficient WSN management system must be included in order to guarantee correct operation and performance in terms of throughput of such a network of sensor nodes [32,43]. However, implementing efficient traditional WSN management has proven difficult due to the inherent difficulties of WSNs, including sensor/actuator heterogeneity, application dependence, and resource limitations. As the WSN gets bigger, this management challenge gets harder. By enabling the segregation of the control system from the sensor nodes/actuators, software-defined Networks (SDN) offers a viable option in flexible management WSNs [42].

If we talk about the mechanism and working of these wireless networks, then it is based on the OSI model [44]. The OSI model was created for the communication between two devices while ensuring that all the standard protocols and standards are maintained as shown in Figure 2. In order to overcome the vulnerability and security threats of this model, protection is applied on every layer to make this model more effective and efficient for every day communication [45]. One of the most common and frequent methods to maintain authenticity, security and confidentiality of wireless communication is cryptography [34]. Although it improves the security of this medium, it requires additional power and time for the encryption and decryption of data at the sending and receiving ends [46].

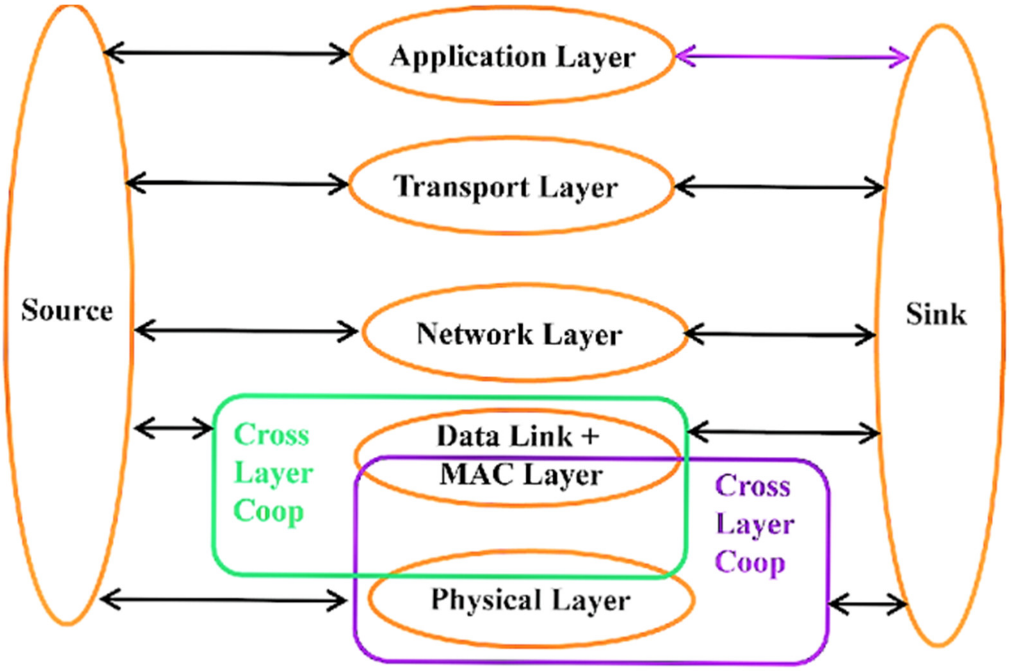

Figure 2. OSI layered model for MAC security.

Moreover, to guarantee that the communication is secure, some wireless networks follows multiple authentication approaches which are implemented at different layers of this model, namely, the MAC layer, network layer and transport layer [47]. The MAC layer of the model ensures that the data or packets are being transferred to the authentic MAC address [48]. In the network layer, the functionality of WPA and WPA 2 are used, whereas in the transport layer, SSL and TLS protocols are used [49]. This ensures that the communication is pretty much secure but the consumption of latency is very high, and it also leads to computational complexity [50]. Figure 3 (below) shows the design factors of a wireless sensor network [51]. This section of the paper covers the weaknesses and flaws which are commonly found in wireless networks.

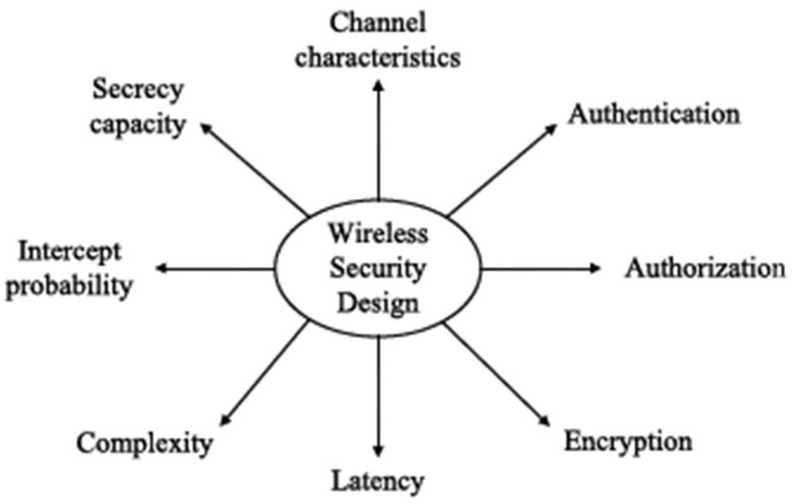

Figure 3. Security vulnerabilities in wireless network.

As mentioned earlier, every OSI layer has its own security to provide and enhance protection for communication in a wireless medium, and therefore, it leads to individual challenges and issues [52].

Due to the nature and requirements of contemporary industry, IWSNs (industrial wireless sensor network) have evolved into the next stage in the development of WSNs (wireless sensor networks) [53]. This kind of network enables the development of adaptable and scalable designs that can accommodate several traffic sources with various characteristics [21]. Due to the wide range of application scenarios, it is necessary to include extra capabilities that can ensure a sufficient degree of dependability and that may change to accommodate the dynamic behavior of the active applications [54]. The usage of SDNs (software-defined networks) expands the network's potential for control and makes it possible for its industrial-scale implementation [55]. Heavy signaling traffic must use the same channels as the data traffic between nodes and the controller. To get around this problem, the traffic can be divided at the MAC layer into flows, known as slices, and properly scheduled [56].

This article suggests the addition of a Time Slotted Channel Hopping (TSCH) Scheduler and the integration of a transport manager, a routing procedure that assigns various routes in accordance with various flows [43]. Additionally, the framework software-defined network solution for wireless sensor networks incorporates the TSCH (Time Slot Channel Hopping), and this protocol has been changed to convey the TSCH schedule. These components work together to segment and schedule the data that will be transmitted from the controller to the nodes in a single packet [43,57]. The results demonstrate how the combined use of the routing and the TSCH Scheduler, which enables the creation of slices by flows with varying quality of service needs, and increases flexibility, adaptability, and determinism [58]. In turn, this promotes the maintenance of the DMR (Deadline Miss Ratio), increases the packet delivery ratio for the flows with the greatest priority, and lengthens the network lifetime [59].

3. Attacks on Wireless Security

Sinkhole attacks are the most dangerous attacks in wireless sensor networks in which fake nodes distribute fake routing updates such as the shortest path to a sink node to disturb the network traffic. A comprehensive review is conducted by [60] to show the up-to-date sinkhole attacks along with their mitigation approaches. Furthermore, they also discussed the state-of-the-art challenges in the detection and prevention of sinkhole attacks in wireless sensor networks.

In wireless sensor networks, the node structure is restricted by memory, computation and energy limitations. The lifetime of a node having limited energy resources directly affects the overall performance of a wireless sensor network. Cluster head selection and data transmission strategy play a key role in the performance enhancement of WSNs. A new energy-aware as well as adaptive routing scheme was developed by [61], which is based on the fuzzy TOPSIS method and performs well in terms of energy efficiency, network life, less overhead on cluster head selection and data transmission.

We have categorized the attacks over wireless network equipment. Some categories are mentioned below in Figure 4.

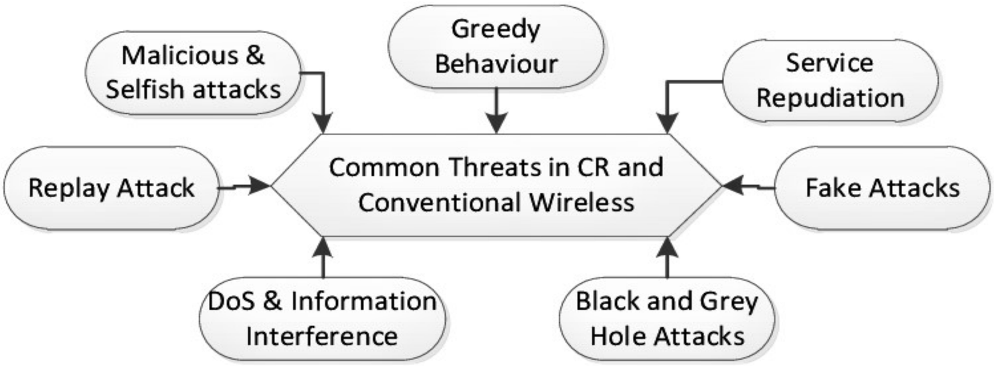

Figure 4. Common security threats in wireless network.

3.1. Packet Injection-Based Attacks

The packet injection attack is based on the concept of ARP request. In packet injection, the hacker or unauthorized user captures the packet of a targeted network of any type. That allows the user to produce and send a large amount of traffic to the network [62]. Although the packet over a network is always secured by encryption, the packet type can be figured out easily by the packet size [63]. The size of ARP packet is 28 bytes. By reinjecting a packet into a network, it sends packets to all the clients. Encrypted packets are captured by sending additional packets, and by sending out more packets, the hacker will probably be able to break out of WEP faster [64].

3.2. Fake Authentication-Based Attacks

Fake authentication is a method through which an attacker can break into the WEP-protected network even without having access of the root key [65]. This can be achieved in two ways:

1. Open system authentication: in this type of authentication, the user can access the system without any kind of user verification by the network [66]. It is also referred to as null verification because no kind of authentication takes place between the devices, and it is an exchange of frames (hellos) between the client and the AP.
2. Shared key authentication; this is the same as open system authentication but it includes a challenge (requires WEP keys to be matched) and response between AP and the user [67,68]. In this method, the key is delivered to wireless clients with the help of a secured and protected channel which is independent of any standard and protocols being used. The client or user just has to simply log in by submitting their credentials and can access the network [69].

3.3. Fluhrrer, Mantin And Shamir Attacks

The FMS attack, released in 2001 by Fluhrrer, Mantin and Shamir, is based on the weakness of RC4. This can be performed as the attacker tries to manipulate RC4, which allows him to guess the byte of the key. If the key is invalid, the attacker tries again, and in order to reach fifty percent probability, the attacker has to capture a large number of packets, which can reach approximately six million [70]. The key can be figured out as the bites are somehow related to each other; therefore, if the attacker manages to figure out the first bit of the key, they will manage to have a hint regarding the other bit, and that will eventually help him to get on the right track [71].

3.4. Wi-Fi Protected Access (WPA) Attacks

Wi-Fi Protected Access (WPA) was introduced as the updated version of WEP and became available in 2003. The main motive of WPA was to overcome and eliminate the vulnerabilities which failed to be handled by WEP protocol. From then onwards, it has been recognized as the standard of security for devices over a wireless network [72]. The most common WPA configuration is WPA-PSK, and the size of the key used in WPA is 256 bits. WPA includes an integrity check, which means that it validates and checks that no packet has been altered and/or captured by an unauthorized user between the end user and the access point [73].

Moreover, WPA contains the Temporary Key Integrity Protocol (TKIP), which is more secure and effective as compared to the fixed key system which is used in WEP. However, still there have been some attacks which managed to bypass the security of this protocol [74]. Some of the attacks include Back and Tew's Improved Attack, Ohigashi-Morii Attack, Michael Attacks, etc. [75]. There are three categories of WPA attacks, as discussed below in Figure 5.

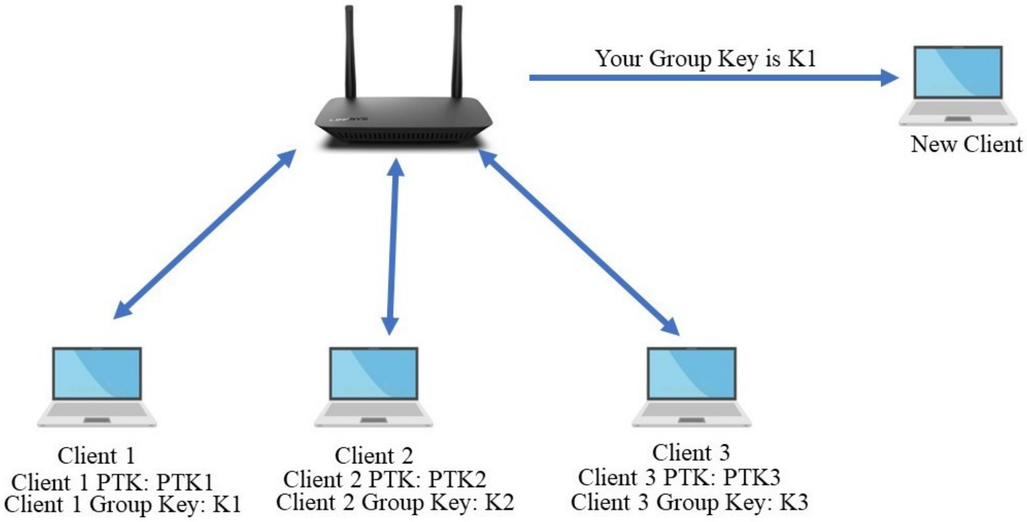

Figure 5. Each client has same copy of GTK in wireless network.

3.4.1. Back and Tew's Improved Attack

This attack is based on the poisoning of ARP. The attacker tries to exploit the weakness by decrypting the ARP and sending the flow of packets to the network, which leads to ARP poisoning [76]. Furthermore, this attack requires quality of service and allows consumption of several channels. Every channel has its own TKIP sequence counter, respectively, but channel 0 has the ability to hold down the most traffic [77].

3.4.2. Ohigashi-Morii Attack

This attack was introduced in 2009, and it was an improved version of Back and Tew's improved attack [78,79]. It was more efficient for all modes of Wi-Fi Protected Access (WPA).

3.4.3. Michael Attack

In 2010, Beck was able to discover that the internal state tends to reset if it reaches a certain point, causing the whole algorithm to start all over again. Due to this, an attacker might be able to insert some text in a packet, meaning that even though the content of the package was different, the result of the algorithm was still accurate [57]. However, the requirements of this attack were very high compared with Back and Tew's improved attack [80].

3.5. Wi-Fi Protected Access 2 (WPA2) Attacks

WPA2 replaced Wi-Fi Protected Access due to the advancements and security concerns for new technology and devices. The certification started in 2004, and by the end of March 2006, it was mandatory for every device to be compatible with and have the features of WPA2 [64]. The most important upgrade in this protocol was about the replacement of TKIP with the AES algorithm and the introduction of CCMP (AES CCMP, Counter Cipher Mode with Block Chain Message Authentication Code Protocol). However, one of the most common and frequent attacks which was found in this protocol was Hole196 [81].

3.5.1. KRACK Attack

The KRACK attack was discovered in 2016 by Mathy Vanhoef and Frank Piessens. This attack targets the four-way handshake procedure in WPA2 protocol, and it is one of the most severe replay attacks [82]. In this protocol, during disconnection from a Wi-Fi network, it is possible for the user to reconnect to the network by using the same key for a quick handshake, so that the connection can be quickly reconnected and can be continued [13]. Therefore, since it allows the user to reconnect without generating a new key, it is highly possible that a hacker or the defaulter can deploy a replay attack [83].

3.5.2. PMKID Attack

This attack was discovered on 4th August of 2014, and it is particularly dangerous for those protocols which consist of WPA/WPA-PSK (pre-shared Key). This attack allows the attacker to obtain the PSK key [84]. Moreover, this attack was discovered accidently while the protocol was being tested and new ways of failing this secure connection were being discovered. The thing which makes this attack unique and different from others is that the unauthorized person does not have to access the whole four-way hand shaking procedure [53,85]. However, it is performed with the help of an RSN IE (Robust Security Network Information System). Some of the benefits of this attack include:

1. The attacker might be able to have direct communication with the access point, and therefore, it is a client-less attack as it does not need to have a regular user for its deployment [82].
2. This attack is less time consuming because of the fact that the unauthorized person does not have to wait for the four-way handshaking process [86].
3. They are faster because it does not require replaying of counter values.
4. One of the key benefits is that the final data or result will not be shown in different format, but it will appear to be in regular hexadecimal format [67].
5. There is no loss of EAPOL frames, since the AP and client are too far away from the attacker.

4. TCP/IP Model Layers Attacks

The TCP/IP model has five layers, and every layer has its own security, as discussed in the sections below. However, unfortunately, attacks have also been performed over each layer, as mentioned below.

4.1. Physical Layer Attacks

The physical layer is the last layer which is present on the OSI model and it is responsible for the transmission of bits to the medium [87]. The two main types of attacks which are commonly found in the physical layer are the eavesdropping and jamming attacks. The concept of the eavesdropping attack is the interference of the unauthorized user by intercepting the communication of the clients or authorized user. As long as the coverage or communication lies in the range of the eavesdropper, the hacker can hack into it. Therefore, in order to make it secure, secret keys are used which use the concept of cryptography. In particular, SN and DN shares a secret key, and the text is encrypted with the help of cipher text. The main advantage of this is that even if the eavesdropper manages to access the data or text, it will still not manage to understand it since it will be encrypted and will only be accessible with the help of that specific special key [88].

The jamming attack is also known as the DoS attack, and in this kind of attack, the hacker tries to access the data with the help of a malicious node, as shown in Figure 6. The jammer helps and prevents the device from connecting to and accessing the authorized node, and instead of that, it allows the device to connect to a malicious node which is being controlled by the unauthorized user [82].

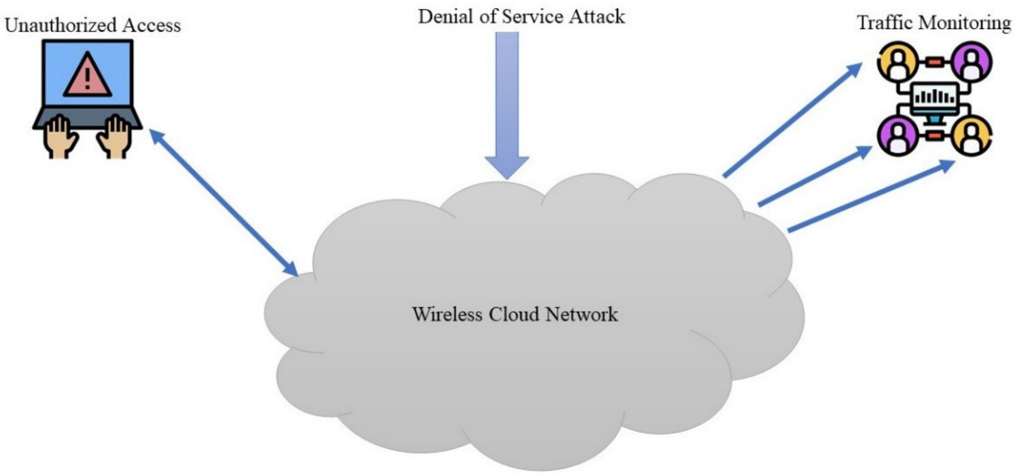

Figure 6. Network layer attacks.

Zero Day DdoS attacks are emerging types of attacks and are increasing in IoT-based systems which are empowered by WSNs. A machine learning-empowered honeypot-based sustainable framework is proposed by [89] for preventing Zero Day DdoS attacks.

4.2. MAC Layer Attacks

In recent years, a number of authentication methods have been published, although the majority of earlier plans do not offer enough privacy for these wireless connections. We suggest the Cogent fingerprint authentication scheme as an effective and lightweight authentication method to overcome the drawbacks of earlier methods (COBBAS). The suggested system employs lightweight procedures to improve the network's efficiency in terms of the time, capacity, and battery usage. It is dependent on biometric data. Burrows-Abadi-Needham logic is used in a formal security study of COBBAS to ensure that the system protocol offers safe mutual authentication [48].

Each network node is equipped with an NIC card which contains the MAC address of the device, which is unique worldwide [20]. This MAC address helps the user to be identified all over. MAC spoofing is performed by the hackers, allowing them to change the assigned MAC address of their devices over the Internet, and this is one of the primary attacks which target the MAC layer [90]. Although the MAC address is imprinted and hard coded, still they manage to hide their true identity and manage to have an alternative MAC address. Moreover, an unauthorized user may also be able to hear the ongoing communication between the two devices and might be able to steal and use the MAC address of another device; this kind of crime lies under identity-theft attack [70].

Moreover, MITM attacks and network injections are also quite common on this layer, as shown is Figure 7. In a MITM attack, the defaulter tries to break into the network with the help of sniffing, and then he tries to learn one of the MAC addresses of the communicating devices. Then, that person impersonates himself as one of the users and establishes the connection which helps them to access the data. It helps the hacker to control the whole communication environment, whereas for the users, it seems like a normal conversation as their communication is not interrupted [91]. On the other hand, the network injection consists of injecting commands in the switches and routers, which allows the devices to be re-configured. Therefore, it allows the network to be paralyzed, or it may even require the whole system to be rebooted as the configuration gets disturbed upon updating commands.

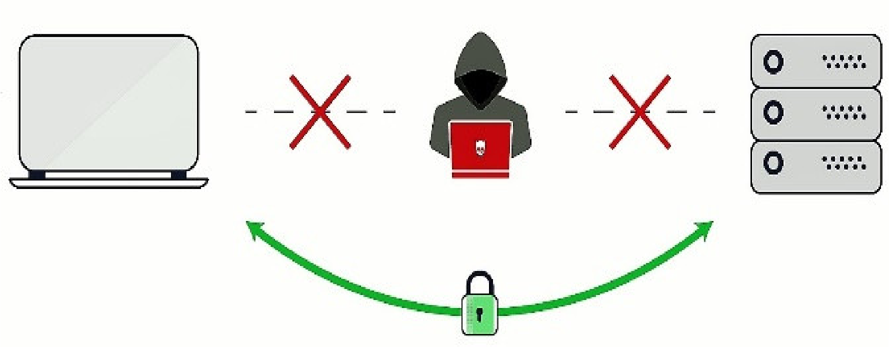

Figure 7. Man-in-the-middle attack in MAC layer.

4.3. Network Layer Attacks

The network layer is responsible for delivering the packets from source to destination and vice versa with the help of the IP address. The network layers basically target the weakness of the IP address, which leads to IP spoofing, IP hijacking and Smurf attacks [92].

In IP spoofing, the user creates an IP packet which has a changed address that helps either to hide the true IP address of the hacker or to represent itself as another device [70,91]. It is a common technique which is used to initiate DoS attack against a device or a network, as shown in Table 1.

Table 1. Network layer attacks.

Network Attacks	Characteristics and Features
IP Spoofing	Falsification of IP address
IP Hijacking	Impersonation of a legitimate users IP address
Smurf Attack	Paralyzation of a network by launching a huge number of ICMP requests

The Smurf attack is also a DoS attack in which the unauthorized user sends a huge number of ICMP packets to the network. Upon request, the victim needs to respond to all the requests and it replies back, which leads to excess traffic at the victim’s end. Due to the congestion produced by the large number of requests, it paralyzes the network of the victim. A possible solution to a Smurf attack is to make sure that we configure all the devices such as routers and switches individually, in a way that they do not respond to ICMA requests. Moreover, we can also use a firewall that will help to block the malicious packets [90].

4.4. Transport Layer Attacks

In a transport layer attack, the attackers mainly attack the User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). In short, TCP is a connection oriented protocol which is used for communication between server and client. Furthermore, it allows the maintenance of a virtual pipeline which provides a secure connection between the users and is mainly used in chat applications. Furthermore, UDP is a connectionless protocol in which the data travels in stream and it is mainly used in live streams where loss of data does not matter [92]. Both of these protocols are exposed when it comes to access by an unauthorized user with the help of flooding, and hackers can also get into the network by predicting the sequence number in the TCP protocol, as shown in Table 2. The UDP protocol is also exposed to flooding attacks as the attacker generates a large number of UDP packets [93]. Due to the large number of packets being generated at the victim's end, the victim will have to respond and reply to every malicious UDP packet, and it will become unreachable for other nodes.

Table 2. Transport layer attacks.

Transport Attacks	Characteristics and Features
TCP Flooding	Sending a huge number of ping requests
UDP Flooding	Launching an overwhelming number of UDP Packets
TCP Sequence Prediction Attack	Fabrication of a legitimate users data packets using the predicted TCP sequence index.

Similarly, the attacker can also hide its real identity from the other nodes by IP spoofing, and this might cause the decrement in the response rate of UDP packets. However, as in TCP, firewalls can be used in order to get rid of malicious packets which are requesting a reply from the victim's node, and it will help to block those requests.

4.5. Application Layer Attacks

In the OSI model, the application layer is responsible for providing end services to the users, which contain file transfers protocols, email configuration and services regarding the web pages. The main HTTP (web-based) attacks are Trojan horses, worms, ruses, cross-site scripting attacks and structure query language injection attacks. The SQL injections contain data-driven applications that contain SQL commands which allows the unauthorized person to access the sensitive data [94]. Moreover, in cross-site scripting attacks, client-side scripts are injected into web pages via an access control measure [95].

4.5.1. Active Attacks

Active attacks are those in which the hacker tries to gain access to communication information or to the network by interfering or interrupting and also changes the data as per the hacker's desire. The unauthorized person might update or alter the data and modify the data stream [69]. The most common types of these attacks are Wormhole attacks and Black hole attacks, which frequently and mostly target where wireless sensor networks are being used [73,78]. The concept of a Black hole attack is that one node of a network acts as a black hole, attracting all the network traffic to itself. The diagram below (Figure 8) shows the view of a Black hole attack when it is found in a network.

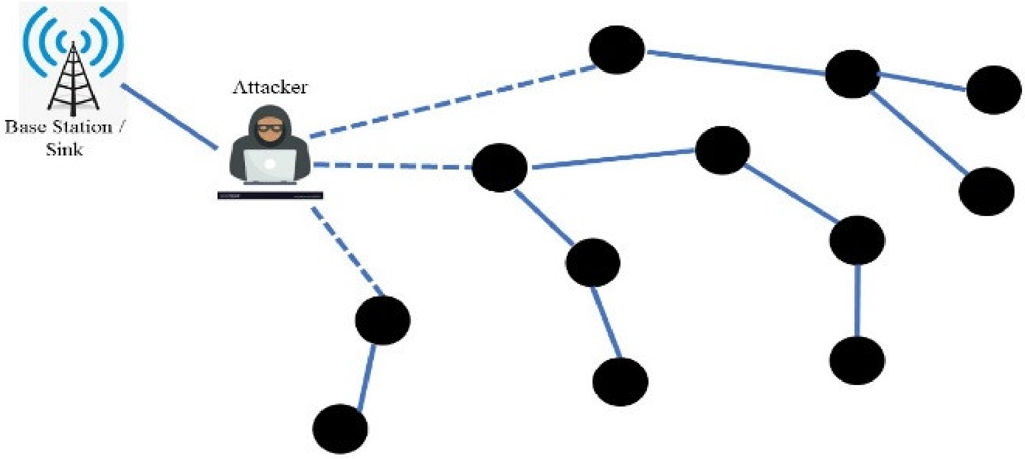

Figure 8. A Black hole attack.

In contrast, in the Wormhole attack, the attacker tries to keep a record of a packet at a single location and tunnels it through to another location [77]. Diagrammatically, the worm hole attack can be showed as below Figure 9.

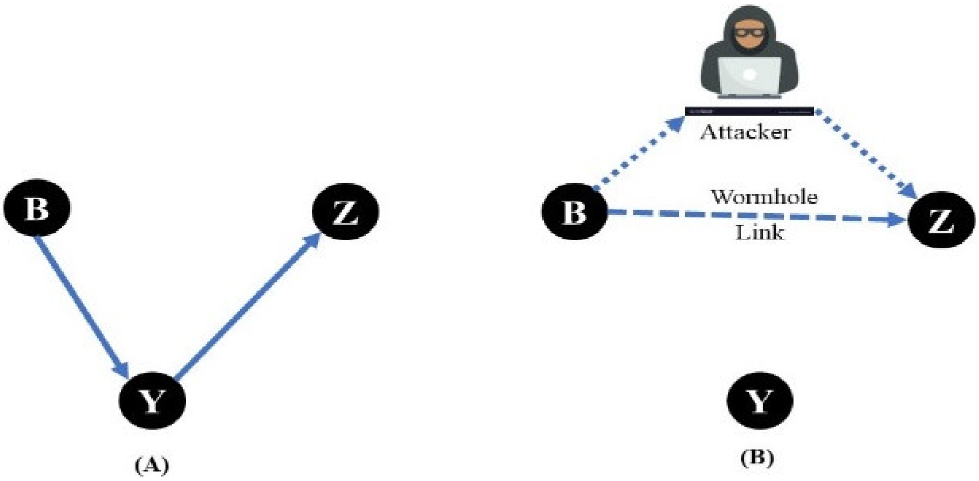

Figure 9. (**A**) Wireless Sensor Network with three locations. (**B**) Wormhole attack by attacker.

In wireless sensor networks, the nodes send a special message that is known as a "hello" message. These messages are used in order to discover the nodes in a network and also to insert a new node into a network. While attacking this kind of network, the attacker tries to produce congestion in the network by overloading the network, which allows the attacker to consume all the energy of the nodes which are there in the network [82,83]. Figure 10 (below) shows a diagram of a Hello Flood attack.

Through this procedure, the unauthorized uses a powerful antenna to generate hello packets into the network, and all the neighbors of that node in the network try to answer it. Due to the reply, it will allow the energy of the nodes to be consumed [85]. Figure 10 (below) shows the image of the hello flood attack.

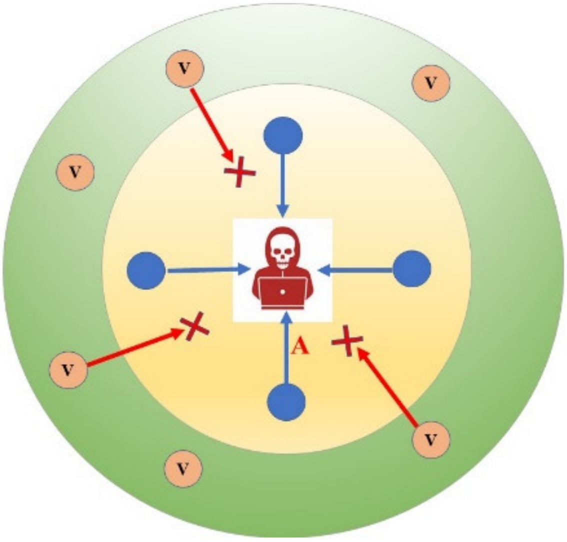

Figure 10. A Hello Flood attack.

Similarly, one of the examples of an active attack is a path-based DoS attack, as shown in Figure 11, which includes the injection of fake or replayed packets into the system [70,88].

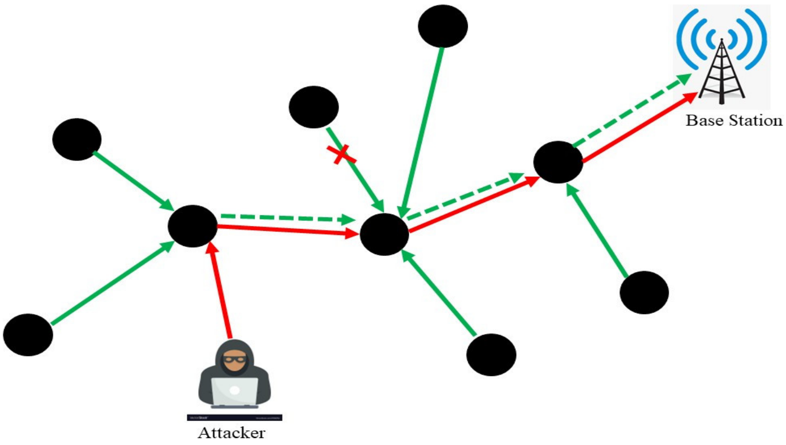

Figure 11. A path-based DoS Attack.

As a result of this, the other nodes will forward those spoiled packets, resulting in wastage of bandwidth [96]. It can also prevent other nodes from sending data further ahead and can cause disturbance in the network [97].

5. Security Threats in Real Life

We have discussed some daily life security threats which we face in different environments, as mentioned below.

5.1. Healthcare Field

WSNs are important because we believe that they can help us in future in such a way that will make our lives much easier and will give solutions to problems which we face in real life [98,99]. WSNs with nanotechnology and AI with computing can benefit us when it comes to major issues regarding healthcare. We can achieve physiological data collection of a patient, such that the sensors can collect the behavioral data of the patient and can also store it [100]. It can be used in an appointment with a doctor and can be used to detect the behavior or mood of an elderly person, as shown in Figure 12. A small sensor device can be implanted in patients, which can track his/her heartbeat or blood pressure. Similarly, a doctor can also carry a sensor node which will track down his/her location inside a hospital.

Figure 12 (A) is maintaining the connection setup phase in between the patient and medical servers. End user first request to the adversory for connection with hospital server rooms, after maintaining the connection in Figure 12 (B) patient interact with doctor and check all patient history, record and request/ response.

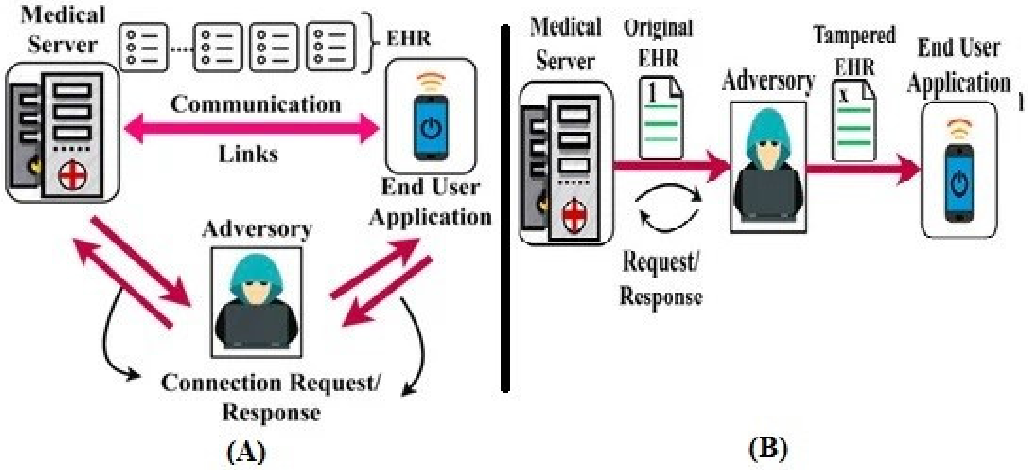

Figure 12. (**A**) Connection Setup in between end user App and Medical server. (**B**) Medical server response to end user App [80].

We have biosensors that tracks electrocardiograms, electromyography, and electrodermal activity, as shown in Figure 12.

However, due to the numerous advantages, WSNs are also exposed when it comes to malicious activities [101]. There are several issues, for instance, illegally obtaining access to medical records and the data of the hospital, which could lead to the incorrect insertion of data as the attacker tries to change the saved record of the particular patient. In order to overcome this, the network must allow privacy and power of decisions for the authorities in power. Furthermore, intrusion decision must be introduced in these devices, which will help the management and authorities to track down the malicious nodes and can inform the management by generating an alarm [102,103]. Therefore, secure application is needed so that people can trust the importance of these kind of networks and can also adopt this technology in their everyday lives.

5.2. Oil and Gas Industries

The ocean covers 70% of our planet, Earth, which contains rivers and lakes and is also responsible for our wellbeing. Pollution is one of the major issues of our planet and we have been noticing climatic changes throughout the whole world. Furthermore, ocean pollution is not only disturbing humans, but it is also having negative effects on aquatic life [104]. The major sources which lead to oceanic pollution include oil spills by ships during transportation or the search for oil reserves. Similarly, oil dumping during cleaning is also responsible for ocean pollution [105]. It is estimated that oil spills total more than 4.5 million tons annually, and 2 million tons of oil is introduced into oceans annually, which equates to one full tanker per week. Moreover, it is not easy to monitor oceanic pollution since it can be life threatening as divers have to go deep inside the ocean, and due to ocean behavior, it is also costly since gadgets are required along with boats, ships, etc. [106]. Therefore, the idea of autonomous underwater vehicles has been proposed, which uses wireless sensor networks and unmanned vehicles that can roam freely. They receive data periodically and forward it to base, which is handy for oceanic data collection. It can be also used for oceanic disaster, pollution monitoring and tactical surveillance [107].

In addition to monitoring pollution, these wireless networks can also provide services for safety as well as carrying out multiple tasks. They can be used with sensors to measure the temperature, humidity, pipelines, and conditions of the equipment which are being used on site [108]. Moreover, they can be used to maintain- and standardized the pressure and parameters in oil and gas industries where any leakage can lead to health risks. That means that this will require maximum authenticity and reliability of these wireless networks so that no one will be able to breach the security, and in order to enhance and maintain secure networks, encryption and decryption might be used so that no one will be able to easily break into the network. This can be achieved with the help of cryptography and by using the right ciphers and algorithms along with public and private keys which will optimize the security and results [109]. Furthermore, RSA and Diffie-Hellman cryptographic curves can also be used in order to maximize performance as it decreases the computational time and the amount of data to be transmitted and stored. This will allow our network to remain flawless, and with the help of small keys, we will be able to achieve good results [110].

5.3. Military Information Integration

These wireless networks can play a key role in assisting armies and the military in accomplishing their targets and attacking their opponents. Furthermore, it allows the improvement of scalability and real time processing for remote sensing. Through these sensors, threats and attacks can also be detected with the help of a Common Operating Picture (COP) [20]. Furthermore, with the help of these networks and sensors, we can make sensor-fused weapons, wireless sensor pods, autonomous drones or aerial vehicles such as the Rotomotion SR50 and Cyber Bug.

These type of networks can also play a key role in the detection of individual soldiers when it comes to teammates and as well as enemies. This can be possible by using cameras and sensors that will allow us to protect military sites and buildings [29]. Moreover, there are Early Attack Reaction Sensors (EARS) that detect gunshots or a blast within a range and can update the user with the coordinates. These use a small microphone array and have been tested several times in open field, leading to good and satisfactory results. Similarly, the ASW concept, which uses low-cost acoustic sensors for littoral anti-submarine warfare, consists of sensors which help to locate and detect submarines which are operating on batteries [63]. Although they are not costly, they have to be deployed in large numbers in order to operate with high sensitivity and to note down any malicious activity.

Rather than this, these wireless networks can be very handy in order to find out and trace the position of a sniper, which can save human life, especially when it comes to the battlefield.

6. Proposed Solution to Enhance Security of Wireless Sensor Networks

There is no doubt that wireless networks are used in many fields, such as the applications mentioned above, and they can help us in many ways. Therefore, in order to increase WSN reliability and dependency so that it can be widely used without any security threats, several models and principles are being studied and introduced, with the aim being that these networks will be flawless and can be used without any fear of loss of data.

This proposed model is free from the all types of key reinstallation attack. In order to understand this model, let us suppose an example through a message flow that is as follows:

Message1: Encpt [AMAC, ANonce, SN, and α = TRUE] Message2: Encpt [SMAC, SNonce, and PTK] Message3: Encpt [AMAC, SNonce, and SN + 1] Message4: Encpt [AMAC, SN + 1 and MIC].

The attacker tries to act like a middle man when breaking into the network between the sender and receiver. Furthermore, it allows message 3 and prevents message 4 from reaching the destination during the handshake process. As a result, the supplicant needs to reinstall the already-in-use packet, which resets the data protection or confidentiality protocol.

In order to tackle this solution, we need to make sure that our network is encrypted during the handshaking process during the communication between sender and receiver. Similarly, we need to make sure that our network contains a Boolean variable that is responsible to check the four-way handshaking communication.

Initially, the AP generates the ANonce, sets the Boolean variable to true and encrypts every message with an encryption/decryption key. The supplicant then tries to decrypt the message by using the decryption key and stores the Boolean variable.

The second step includes the supplicant combining the SMAC and encrypting it. Once the receiver receives the message and decrypts it, it then resets package 3 and sends it back, else it will terminate the handshake process.

To make sure that the process remains fault free and no one tries to break in, the supplicant decrypts the message and checks the value of Alpha. If the value is true, then that means that the communication was successful and without any problems, otherwise it will discontinue the ongoing communication.

7. Conclusions

In this survey, we have discussed the various security threats and attacks on different layers of the TCP/IP model for wireless sensor networks. Security plays a vital role in obtaining people's trust in order to adopt this technology. Wireless Networks are playing a key role in making our lives much easier and more comfortable, but it also brings a number of challenges for practitioners of WSNs. We have presented the vulnerabilities and threats of WSNs by considering wireless security design parameters. Furthermore, the available security techniques for WSNs are highlighted along with some real life applications in military, oil and gas. Finally, we have proposed a solution for WSN security enhancement by adopting a handshaking mechanism with the alpha method. In future, we will implement and analyze the performance of the proposed method.

Author Contributions: Conceptualization, A.U.R. and M.S.M.; methodology, A.U.R.; software, S.Z.; validation, S.Z., M.A.R. and F.Q.; formal analysis, S.S.A.; investigation, I.U.K.; resources, N.A.; data curation, I.U.K.; writing—original draft preparation, A.U.R.; writing—review and editing, A.U.R and N.A.; visualization, S.S.A.; supervision, M.S.M.; project administration, S.Z.; funding acquisition, N.A. All authors have read and agreed to the published version of the manuscript.

Funding: We would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Dwiputriane, D.; Engineering, S.H.-J. No. 3. Authentication for 5G Mobile Wireless Networks: Manuscript Received: 5 January 2022, Accepted: 8 February 2022, Published: 15 March 2022. *J. Eng. Technol. Appl. Phys.* **2022**, *4*, 16–24.
2. Masher, N.; ul Mahjoob, K. IOT SECURITY THREATS AND CHALLENGES. Available online: https://www.irjmets.com/uploadedfiles/paper/issue_2_february_2022/19081/final/fin_irjmets1644942131.pdf (accessed on 24 June 2022).
3. Waqas, M.; Tu, S.; Halim, Z.; Rehman, S.; Abbas, G.; Abbas, Z. H. *The Role of Artificial Intelligence and Machine Learning in Wireless Networks Security: Principle, Practice and Challenges*; Springer: Berlin/Heidelberg, Germany, 2022.
4. Li, J.; Ma, H.; Li, K.; Cui, L.; Sun, L.; Zhao, Z.; Wang, X. *Wireless Sensor Networks*; 2018.
5. Yadav, R.; Varma, S.; journal, N.M.-U.; A survey of MAC protocols for wireless sensor networks. *UbiCC J.* **2009**, *4*, 827–833.

6. Ismail, A.S.; Wang, X.F.; Hawbani, A.; Alsamhi, S.; Abdel Aziz , S. Routing protocols classification for underwater wireless sensor networks based on localization and mobility. *Wirel. Netw.* **2022**, *28*, 797–826. https://doi.org/10.1007/S11276-021-02880-Z.
7. Raja Basha, A. A Review on Wireless Sensor Networks: Routing. *Wirel. Pers. Commun.* **2022**, 1–41. https://doi.org/10.1007/S11277-022-09583-4.
8. Moessner, K.; Majid, M.; Habib, S.; Rehman Javed, A.; Rizwan, M.; Srivastava, G.; Reddy Gadekallu, T.; Chun-Wei Lin, J. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. *Sensors* **2022**, *22*, 2087. https://doi.org/10.3390/s22062087.
9. Temene, N.; Sergiou, C.; Georgiou, C.; Vassiliou, V.; Sergiou, C. A survey on mobility in Wireless Sensor Networks. *Ad Hoc Netw.* **2022**, *125*, 102726. https://doi.org/10.1016/j.adhoc.2021.102726.
10. Zhu, L.; Xiang, H.; Zhang, K. A Light and Anonymous Three-Factor Authentication Protocol for Wireless Sensor Networks. Symmetry (Basel). 2022, 14, doi:10.3390/SYM14010046.
11. Cao, L.; Wang, Z.; Neuroscience, Y.Y.-C.I. and; Analysis and Prospect of the Application of Wireless Sensor Networks in Ubiquitous Power Internet of Things. *Comput. Intell. Neurosci.* **2022**, *2022*, 9004942.
12. Computing, S.E.K. Wireless sensor networks: A survey, categorization, main issues, and future orientations for clustering protocols. *Wirel. Pers. Commun.* **2022**, *104*, 1775–1837.
13. Mezrag, F.; Bitam, S.; Mellouk, A. An efficient and lightweight identity-based scheme for secure communication in clustered wireless sensor networks. J. Netw. Comput. Appl. 2022, 200, doi:10.1016/J.JNCA.2021.103282.
14. Choi, J.; Ha, J.; Personal, H.J. Physical layer security for wireless sensor networks. Available online: https://ieeexplore.ieee.org/document/6666094?arnumber=6666094 (accessed on 20 July 2022).
15. Engineering, F.A. Energy-efficient collision avoidance MAC protocols for underwater sensor networks: Survey and challenges. *J. Mar. Sci. Eng.* **2021**, *9*, 741. https://doi.org/10.3390/jmse9070741.
16. Gulati, K.; Sarath Kumar Boddu, R.; Kumar Boddu, S.; Kapila, D.; Bangare, S.L.; Chandnani, N.; Saravanan, G. A review paper on wireless sensor network techniques in Internet of Things (IoT). *Mater. Today* **2022**, *51*, 161–165. https://doi.org/10.1016/j.matpr.2021.05.067.
17. Rajasoundaran, S.; Prabu, A.V.; Kumar, G.S.; Malla, P.P.; Routray, S. Secure Opportunistic Watchdog Production in Wireless Sensor Networks: A Review. *Wirel. Pers. Commun.* **2021**, *120*, 1895–1919. https://doi.org/10.1007/S11277-021-08542-9.
18. Daanoune, I.; Abdennaceur, B.; Ballouk, A. A comprehensive survey on LEACH-based clustering routing protocols in Wireless Sensor Networks. *Ad Hoc Netw.* **2021**, *114*, 102409.
19. Chander, B.; Gopalakrishnan, K. Secure, Efficient, Lightweight Authentication in Wireless Sensor Networks. *Lect. Notes Electr. Eng.* **2021**, *749*, 303–312. https://doi.org/10.1007/978-981-16-0289-4_22.
20. Shiu, Y.; Chang, S.; Wu, H.C.; Huang, S.C.H.; Chen, H.H. Physical layer security in wireless networks: A tutorial. *IEEE Wirel. Commun.* **2011**, *18*, 66–74.
21. Ahmad, A.; Rathore, M.; Paul, A.; Chen, B.W. Data transmission scheme using mobile sink in static wireless sensor network. *J. Sens.* **2015**, *2015*
22. Jabbar, S.; Paul, A.; Rho, S.; Minhas, A.A. Multilayer cluster designing algorithm for lifetime improvement of wireless sensor networks. *J. Supercomput.* **2014**, *70*, 104–132. https://doi.org/10.1007/s11227-014-1108-y.
23. Pinto, A.; Farooq, M.S.; Idrees, M.; Rehman, A.U.; Khan, M.Z.; Abunadi, I.; Assam, M.; Althobaiti, M.M.; Al-Wesabi, F.N. Formal Modeling and Improvement in the Random Path Routing Network Scheme Using Colored Petri Nets. *Appl. Sci.* **2022**, *12*, 1426. https://doi.org/10.3390/app12031426.
24. Din, S.; Paul, A.; Ahmad, A.; Kim, J.H. Energy efficient topology management scheme based on clustering technique for software defined wireless sensor network. *Peer-Peer Netw. Appl.* **2019**, *12*, 348–356. https://doi.org/10.1007/S12083-017-0607-Z.
25. Jabbar, S.; Minhas, A.A.; Gohar, M.; Paul, A.; Rho, S. E-MCDA: Extended-multilayer cluster designing algorithm for network lifetime improvement of homogenous wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 902581.
26. Tropea, M.; Spina, M.; Rango, F. De; Gentile, A. Security in Wireless Sensor Networks: A Cryptography Performance Analysis at MAC Layer. *Future Internet* **2022**, *14*, 1–20. https://doi.org/10.3390/fi14050145
27. Meshram, C.; Imoize, A.L.; Jamal, S.S.; Aljaedi, A.; Alharbi, A.R. SBOOSP for Massive Devices in 5G WSNs Using Conformable Chaotic Maps. Comput. Mater. Contin. 2022, 71, 4591–4608, doi:10.32604/CMC.2022.022642.
28. Ahmad, I.; Rahman, T.; Zeb, A.; Khan, I.; Ullah, I.; Hamam, H.; Cheikhrouhou, O. Analysis of security attacks and taxonomy in underwater wireless sensor networks. *Wirel. Commun. Mob. Comput.* **2021**, *2021.*
29. Singh, S.; Saurabh, R.; Maitra, T.; Giri, D. Security in Communication for Intelligent Wireless Sensor Networks: Issues and Challenges. *Comput. Intell. Wirel. Sens. Netw.* **2022**, *1*, 175–192.
30. Yu, D.; Kang, J.; Dong, J. Service attack improvement in wireless sensor network based on machine learning. *Microprocess. Microsyst.* **2021**, *80*, 103637. https://doi.org/10.1016/j.micpro.2020.103637.
31. Alves, R.; Oliveira, D.; Pereira, G.C., Albertini, B.C., Margi, C.B. WS3N: Wireless secure SDN-based communication for sensor networks. *Secur. Commun. Netw.* **2018**, *2018*.
32. Abood, M.S.; Wang, H.; Mahdi, H.F.; Hamdi, M.M.; Abdullah, A.S. Review on secure data aggregation in Wireless Sensor Networks. *IOP Conf. Ser. Mater. Sci. Eng.* **2021**, *1076*, 012053.
33. de Carvalho, J.A.R.P.; Veiga, H.; Ribeiro Pacheco, C.F. Extended performance research on IEEE 802.11a WPA2 multi-node laboratory links. *IAENG Int. J. Comput. Sci.* **2020**, *47*, 296–301. https://doi.org/10.1007/978-981-15-8273-8_14.

34. Ali, J.; Roh, B.H. Quality of service improvement with optimal software-defined networking controller and control plane clustering. *Comput. Mater. Contin*. **2021**, *67*, 849-875.
35. Ali, J.; Roh, B.H.; Lee, S. QoS improvement with an optimum controller selection for software-defined networks. *PLoS ONE* **2019**, *14*, e0217631. https://doi.org/10.1371/JOURNAL.PONE.0217631.
36. Ali, J.; Roh, B.H. A Novel Scheme for Controller Selection in Software-Defined Internet-of-Things (SD-IoT). *Sensors* **2022**, *22*, 3591. https://doi.org/10.3390/s22093591.
37. Ali, J.; Lee, B.; Oh, J.; Lee, J.; Roh, B.H. A novel features prioritization mechanism for controllers in software-defined networking. *Comput. Mater. Contin*. **2021**, *69*, 267–282.
38. Ali, J.; Roh, B.H. An Effective Approach for Controller Placement in Software-Defined Internet-of-Things (SD-IoT). *Sensors* **2022**, *22*, 2992.
39. Ali, J.; Roh, B.H. An effective hierarchical control plane for software-defined networks leveraging TOPSIS for end-to-end QoS class-mapping. *Ieee Access* **2020**, *8*, 88990–89006.
40. Ali, J.; Lee, G.M.; Roh, B.H.; Ryu, D.K.; Park, G. Software-defined networking approaches for link failure recovery: A survey. *Sustainability* **2020**, *12*, 4255. https://doi.org/10.3390/su12104255.
41. Ndiaye, M.; Hancke, G.P.; Abu-Mahfouz, A.M. Software defined networking for improved wireless sensor network management: A survey. *Sensors* **2017**, *17*, 1031. https://doi.org/10.3390/s17051031.
42. Orozco-Santos, F.; Sempere-Payá, V.; Albero-Albero, T.; Silvestre-Blanes, J. Enhancing sdn wise with slicing over tsch. *Sensors* **2021**, *21*, 1075. https://doi.org/10.3390/s21041075.
43. Mohammed, A.; Al-Dulaimi, K.; Khodayer, M.; Al-Dulaimi, H. Analysis for modulation and coding scheme with data rate traffic over IEEE 802.11 AC and 802.11 N in wireless multimedia. *Int. J. Comput.* **2021**, *20*, 2021–2109. https://doi.org/10.47839/ijc.20.1.2099.
44. Badhwar, R. Next Gen Wi-Fi and Security. *CISO's Next Front.* **2021**, 213–218. https://doi.org/10.1007/978-3-030-75354-2_25.
45. Ahmed, N.; De, D.; Barbhuiya, F.A.; Hussain, M.I. MAC Protocols for IEEE 802.11 ah-based Internet of Things: A Survey. *IEEE Internet Things J.* **2021**, *9*, 916–938.
46. Frontier, R.B. *Next Gen Wi-Fi and Security*; Springer: Berlin/Heidelberg, Germany, 2021.
47. Ahmed, N.; Roy, A.; Misra, S.; Tandur, D. Programmable IEEE 802.11 ah Network for Internet of Things.In Proceedings of the *ICC 2021—IEEE International Conference on Communications,* 2021. https://doi.org/10.1109/ICC42927.2021.9500610.
48. Butt, T.M.; Riaz, R.; Chakraborty, C.; Rizvi, S.S.; Paul, A. Cogent and energy efficient authentication protocol for wsn in iot. *Comput. Mater. Contin*. **2021**, *68*, 1877–1898.
49. Reddy, S.N. Industrial Safety Applications Using Wireless Access Panels. *Turk. J. Comput. Math. Educ. (TURCOMAT)* **2021**, *12*, 1573–1577.
50. Carvalho, J.; Veiga, H.; Pacheco, C.F.; Reis, A.D. *Extended Performance Research on IEEE 802.11 a WPA Multi-Node Laboratory Links;* Springer: Berlin/Heidelberg, Germany, 2021.
51. Dunkels, A.; Alonso, J.; Voigt, T.; Ritter, H.; Schiller, J. Connecting wireless sensornets with TCP/IP networks. *Lect. Notes Comput. Sci. (Incl. Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinform.)* **2004**, *2957*, 143–152. https://doi.org/10.1007/978-3-540-24643-5_13.
52. Paliwal, G.; Mudgal, A.P.; Taterh, S. A study on various attacks of TCP/IP and security challenges in MANET layer architecture. *Adv. Intell. Syst. Comput.* **2015**, *336*, 191–203. https://doi.org/10.1007/978-81-322-2220-0_16.
53. Kwon, E.; Cho, Y.; Chae, K.J. Integrated transport layer security: End-to-end security model between WTLS and TLS. Available online: https://ieeexplore.ieee.org/document/905331 (accessed on 24 June 2022).
54. Fall, K.; Stevens, W. *TCP/IP Illustrated, Volume 1: The Protocols*; 2011.
55. Zhang, Y. A multilayer IP security protocol for TCP performance enhancement in wireless networks. *IEEE J. Sel. Areas Commun.* **2004**, *22*, 767–776.
56. Fu, B.; Xiao, Y.; Deng, H.; Zeng, H. A survey of cross-layer designs in wireless networks. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 110–126. https://doi.org/10.1109/SURV.2013.081313.00231.
57. Farid, S.; Rehman, A.U. Enhancement in Quality of Services Using Integrated Services in 4G Cellular Network. *Tech. J.* **2018**, *23*, 82–93.
58. Perkins, C.; Jagannadh, T. DHCP for mobile networking with TCP/IP. https://doi.org/10.1109/SCAC.1995.523675.
59. Ali, M.; Nadeem, M.; Siddique, A.; Ahmad, S.; Ijaz, A. Addressing Sinkhole Attacks in Wireless Sensor Networks-A Review. *Int. J. Sci. Technol. Res. (IJSTR)* 2020, 9.
60. Hussain, A.; Ali, M.; Razzaq, A.; Ijaz, A.; Saeed Khan, N. Development of an Adaptive Energy Aware Routing Scheme for Wireless Sensor Networks. *Int. J.Emerg. Technol.* **2020**, *11*, 381–388.
61. Shang, W.; Yu, Y.; Droms, R.; Zhang, L. Challenges in IoT networking via TCP/IP architecture. *NDN Project* 2016. Available online: https://named-data.net/publications/techreports/ndn-0038-1-challenges-iot/ (accessed on 24 June 2022).
62. Chan, M.C.; Ramjee, R. Improving TCP/IP performance over third-generation wireless networks. *IEEE Trans. Mob. Comput.* **2008**, *7*, 430–443.
63. Poongodi, T.; Krishnamurthi, R.; Indrakumari, R.; Suresh, P.; Balusamy, B. Wearable devices and IoT. *Intell. Syst. Ref. Libr.* **2020**, *165*, 245–273, doi:10.1007/978-3-030-23983-1_10.
64. Dunkels, A.; Alonso, J.; Voigt, T.; Ritter, H.; Schiller, J. Connecting wireless sensornets with TCP/IP networks. In *International Conference on Wired/Wireless Internet Communications*; Springer: Berlin, Heidelberg, 2004.

65. Faria, D.B.; Cheriton, D.R. Detecting identity-based attacks in wireless networks using signalprints. *WiSE 2006—Proc. 5th ACM Work. Wirel. Secur.* **2006**, *2006*, 43–52. https://doi.org/10.1145/1161289.1161298.
66. Masud, M.; Gaba, G.S.; Choudhary, K.; Hossain, M.S.; Alhamid, M.F.; Muhammad, G. Lightweight and Anonymity-Preserving User Authentication Scheme for IoT-Based Healthcare. IEEE Internet Things J. 2022, 9, 2649–2656, doi:10.1109/JIOT.2021.3080461.
67. Mahamune, A.A.; Chandane, M.M. TCP/IP Layerwise Taxonomy of Attacks and Defence Mechanisms in Mobile Ad Hoc Networks. *J. Inst. Eng. Ser. B* **2022**, *103*, 273–291, doi:10.1007/S40031-021-00627-0.
68. Messai, M.-L. Classification of Attacks in Wireless Sensor Networks. *arXiv* **2014**, arXiv:1406.4516.
69. Hu, Y.; Perrig, A.; Johnson, D.B. Wormhole attacks in wireless networks. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 370–380.
70. Lupu, T.G. Main types of attacks in wireless sensor networks. In Proceedings of the 9th WSEAS International Conference on Signal, Speech and Image Processing, and 9th WSEAS International Conference on Multimedia, Internet & Video technologies. Septembet 3–5, 2009, Budapest, Hungary.
71. Yu, B.; Xiao, B. Detecting selective forwarding attacks in wireless sensor networks. In Proceedings 20th IEEE International Parallel & Distributed Processing Symposium.
72. Noman Riaz, M.; Buriro, A.; Mahboob, A. Classification of Attacks on Wireless Sensor Networks: A Survey. *Int. J. Wirel. Microw. Technol.* **2018**, *8*, 15–39, doi:10.5815/IJWMT.2018.06.02.
73. Yang, J.; Chen, Y.; Trappe, W.; Cheng, J. Detecting mobile agents using identity fraud. *SpringerBriefs Comput. Sci.* **2014**, *0*, 43–66, doi:10.1007/978-3-319-07356-9_5.
74. Shahzad, F.; Pasha, M.; Ahmad, A. A survey of active attacks on wireless sensor networks and their countermeasures. *Int. J. Comput. Sci. Inf. Secur.* **2017**, *14*, 12.
75. Patel, M.; Aggarwal, A. Security attacks in wireless sensor networks: A survey. In Proceedings of the 2013 International Conference on Intelligent Systems and Signal Processing (ISSP).
76. Anwar, R.; Bakhtiari, M.; Zainal, A.; Abdullah, A.H.; Qureshi, K.N. Security issues and attacks in wireless sensor network. *World Appl. Sci. J.* **2014**, *30*, 1224–1227. https://doi.org/10.5829/idosi.wasj.2014.30.10.334.
77. Mahamune, A.A.; Chandane, M.M. TCP/IP Layerwise Taxonomy of Attacks and Defence Mechanisms in Mobile Ad Hoc Networks. *J. Inst. Eng. Ser. B* **2022**, *103*, 273–291. https://doi.org/10.1007/S40031-021-00627-0.
78. Sinha, P.; Jha, V.K.; Bhushan, B.; Rai, A.K.; Jha, V.K. A Review of Machine Learning Solutions to Denial-of-Services Attacks in Wireless Sensor Networks. 2017. https://doi.org/10.1109/CSPC.2017.8305855.
79. Bouabdellah, M.; Kaabouch, N.; El Bouanani, F.; Ben-Azza, H. Network layer attacks and countermeasures in cognitive radio networks: A survey. *J. Inf. Secur. Appl.* **2018**, *38*, 40–49.
80. Proano, A.; Lazos, L. Selective jamming attacks in wireless networks. In Proceedings of the 2010 IEEE International Conference on Communications.
81. Singh, R.; Prasad, A.; Moven, R.M.; Deva Sarma, H.K. Denial of service attack in wireless data network: A survey. *Dev.Integr. Circuit (DevIC)* 2017, 354–359.
82. Edigar, M.B.; Rao, P. V. Modeling of lightweight security framework for identifying efficient route for secure communication in WSN. Int. J. Intell. Unmanned Syst. 2022, 10, 129–144, doi:10.1108/IJIUS-09-2020-0051.
83. Isha, A.M.; Raj, G. Dos attacks on tcp/ip layers in wsn. *Int. J. Comput. Netw. Commun. Secur.* **2013**, *1*, 40–45.
84. Zhang, L.; Restuccia, F.; Melodia, T.; Pudlewski, S.M. Taming cross-layer attacks in wireless networks: a Bayesian learning approach. *IEEE Trans. Mob. Comput.* **2018**, *18*, 1688–1702.
85. Wang, L.; Wyglinski, A.M. A combined approach for distinguishing different types of jamming attacks against wireless networks. In Proceedings of 2011 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing.
86. Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S.V. Denial of service attacks in wireless networks: The case of jammers. *IEEE Commun. Surv. Tutor.* **2010**, *13*, 245–257.
87. Ali, M.; Siddique, A.; Hussain, A.; Hassan, F.; Ijaz, A.; Mehmood, A. A Sustainable Framework for Preventing IoT Systems from Zero Day DDoS Attacks by Machine Learning. *Int. J. Emerg. Technol.* **2021**, *12*, 116–121.
88. Eriksson, J.; Krishnamurthy, S. V.; Faloutsos, M. Truelink: A practical countermeasure to the wormhole attack in wireless networks. In Proceedings of the 2006 IEEE International Conference on Network Protocols.
89. Zhang, Z.; Wu, J.; Deng, J.; Qiu, M. Jamming ACK attack to wireless networks and a mitigation approach. In Proceedings of the IEEE GLOBECOM 2008–2008 IEEE Global Telecommunications Conference.
90. Kanawat, S.; Parihar, P. Attacks in wireless networks. *Int. J. Smart Sens. Adhoc Netw.* **2011**, *1*, 17. https://doi.org/10.47893/IJSSAN.2011.1033.
91. Kadhim, A.N.; Sadkhan, S.B. Security Threats in Wireless Network Communication-Status, Challenges, and Future Trends. In Proceedings of the 2021 International Conference on Advanced Computer Applications (ACA).
92. Sardar, R.; Anees, T. Web of things: Security challenges and mechanisms. *IEEE Access* **2021**, *9*, 31695–31711.
93. Taleb, H.; Nasser, A.; Andrieux, G.; Charara, N.; Motta Cruz, E. Wireless technologies, medical applications and future challenges in WBAN: A survey. *Wirel. Netw.* **2021**, *27*, 5271–5295.
94. Zaman, S.; Alhazmi, K.; Aseeri, M.A.; Ahmed, M.R.; Khan, R.T.; Kaiser, M.S.; Mahmud, M. Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. *IEEE Access* **2021**, *9*, 94668–94690.
95. Raza, M.; Bukht, T.; Ali, M.; Rehman, A.U.; Idrees, M. Analyzing the Behaviour of DDOS Cyber Attacks. *Tech. J.* **2021**, *26*, 46.

96. Najmi, K.; AlZain, M.; Masud, M.; Jhanjhi, N.Z.; Al-Amri, J.; Baz, M. A survey on security threats and countermeasures in IoT to achieve users confidentiality and reliability. Available online: https://www.sciencedirect.com/science/article/pii/S221478532102469X (accessed on 24 June 2022).
97. Khalid, L.; Ameen, S. Secure Iot integration in daily lives: A review. *J. Inf. Technol. Inform.* **2021**, *1*, 6–12.
98. Hassija, V.; Chamola, V.; Bajpai, B.C.; Zeadally, S. Security issues in implantable medical devices: Fact or fiction? *Sustain. Cities Soc.* **2021**, *66*, 102552.
99. Ahmad, I.; Niazy, M.; Ziar, R.; Khan, S. Survey on IoT: Security threats and applications. **J. Robot. Control 2021**, *2*. https://doi.org/10.18196/jrc.2150.
100. Nayak, P.; Mohapatra, S.K.; Sharma, S.C.M. *Privacy and Security Issues in IoT Cloud Convergence of Smart Health Care*; 2022. https://doi.org/10.1007/978-3-030-97929-4_20.
101. Chatterjee, U.; Ray, S. Security Issues on IoT Communication and Evolving Solutions. *Stud. Comput. Intell.* **2022**, *988*, 183–204. https://doi.org/10.1007/978-981-16-4713-0_10.
102. Rahmani, A.M.; Bayramov, S.; Kiani Kalejahi, B. Internet of Things Applications: Opportunities and Threats. *Wirel. Pers. Commun.* **2022**, *122*, 451–476. https://doi.org/10.1007/S11277-021-08907-0.
103. Balogh, Z.; Francisti, J.; Fodor, K. Effectiveness of Selected Wireless Sensor Protocols and Their Security. Available online: https://www.researchgate.net/profile/Kristian_Fodor2/publication/361189368_Effectiveness_of_Selected_Wireless_Sensor_Protocols_and_Their_Security/links/62a1f80955273755ebe071b5/Effectiveness-of-Selected-Wireless-Sensor-Protocols-and-Their-Security.pdf (accessed on 24 June 2022).
104. Kalra, V.; Rahi, S.; pawar, N.; Tanwar, P.; Sharma, M.S. A Tour Towards the Security Issues of Mobile Cloud Computing: A Survey. *Lect. Notes Electr. Eng.* **2022**, *875*, 577–589. https://doi.org/10.1007/978-981-19-0284-0_42.
105. Chaudhary, M.M.; Biswas, S.S.; Nafis, M.T.; Tanweer, S. Study of Security Issues on Open Channel. *Smart Sustain. Approaches Optim. Perform. Wirel. Netw.* **2022**, 279–282. https://doi.org/10.1002/9781119682554.CH16.
106. Chaudhary, M.; Biswas, S.; Nafis, M.; Tanweer, S. *Study of Security Issues on Open Channel*; Wiley Online Library: 2022.
107. Pico-Valencia, P.; Holgado-Terriza, J.A. Agentification of the Internet of Things: A systematic literature review. *Int. J. Distrib. Sens. Networks* **2018**, *14*, doi:10.1177/1550147718805945.
108. Neware, R.; Ulabhaje, K.; Karemore, G.; Lokhande, H.; Dandige, V. Survey on Security Issues in Mobile Cloud Computing and Preventive Measures. *Adv. Intell. Syst. Comput.* **2020**, *767*, 89–100, doi:10.1007/978-981-13-9680-9_6.
109. Butun, I.; Osterberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 616–644, doi:10.1109/COMST.2019.2953364.
110. Li, Y.; Yu, Y.; Susilo, W.; Hong, Z.; Guizani, M. Security and Privacy for Edge Intelligence in 5G and Beyond Networks: Challenges and Solutions. *IEEE Wirel. Commun.* **2021,** *28*, 63–69.