Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.036444
Review

Wireless Sensor Security Issues on Data Link Layer: A Survey

Muhammad Zulkifl Hasan*, Zurina Mohd Hanapi and Muhammad Zunnurain Hussain

Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Serdang, Selangor, 43400, Malaysia
*Corresponding Author: Muhammad Zulkifl Hasan. Email: gs58279@student.upm.edu.my
Received: 30 September 2022; Accepted: 12 January 2023

Abstract: A computer network can be defined as many computing devices connected via a communication medium like the internet. Computer network development has proposed how humans and devices communicate today. These networks have improved, facilitated, and made conventional forms of communication easier. However, it has also led to uptick in-network threats and assaults. In 2022, the global market for information technology is expected to reach $170.4 billion. However, in contrast, 95% of cyber security threats globally are caused by human action. These networks may be utilized in several control systems, such as home-automation, chemical and physical assault detection, intrusion detection, and environmental monitoring. The proposed literature review presents a wide range of information on Wireless Social Networks (WSNs) and Internet of Things (IoT) frameworks. The aim is first to be aware of the existing issues (issues with traditional methods) and network attacks on WSN and IoT systems and how to defend them. The second is to review the novel work in the domain and find its limitations. The goal is to identify the area's primary gray field or current research divide to enable others to address the range. Finally, we concluded that configuration. Message Rapid Spanning Tree Protocol (RSTP) messages have higher efficiency in network performance degradation than alternative Bridge Data Unit Protocol (BPDU) forms. The research divides our future research into solutions and newly developed techniques that can assist in completing the lacking component. In this research, we have selected articles from 2015 to 2021 to provide users with a comprehensive literature overview.

Keywords: Wireless sensor networks (WSN); internet of things (IoT); industrial revolution 4.0 (IR4.0); computer networks; network security

1 Introduction

The economy is being boosted by the modernization trend and the rising usage of cutting-edge technologies. Smart technologies are critical to long-term economic growth. They turn homes, workplaces, factories, and even cities into self-contained, autonomous systems that act without human intervention, saving humans from data collection and processing [1]. Cyber-physical systems are

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

transforming organizations [2]. Wireless sensor networks (WSNs) are among the most popular study areas.

Similar to WSN, which is composed of a large number of sensor nodes or a group of nodes, WSN is an environment-independent network. These networks might be used in a range of control systems, including surveillance, assault detection, home automation, and environmental monitoring. The core idea behind the Internet of Things (IoT) is to provide millions of small, linked devices that might work together to accomplish a common objective. These simple, yet intelligent, objects can wirelessly detect and converse [3]. The IoT is becoming a reality because of the growing number of these tiny, networked devices.

This research addressed the many security vulnerabilities in WSNs and IoT. WSN and IoT challenges and similarities are also discussed in this study. However, these attacks are further classified into network layers (Physical, Data Link, Network, Transport, and Application). Furthermore, this research reviewed the number of data-link problems, issues, and assaults, as well as a comparative study of data-link layer attacks to demonstrate the degrading efficiency of the attack on the network. From 2014 through 2026, millions of short-range and long-range IoT devices are anticipated to be deployed, according to Fig. 1.

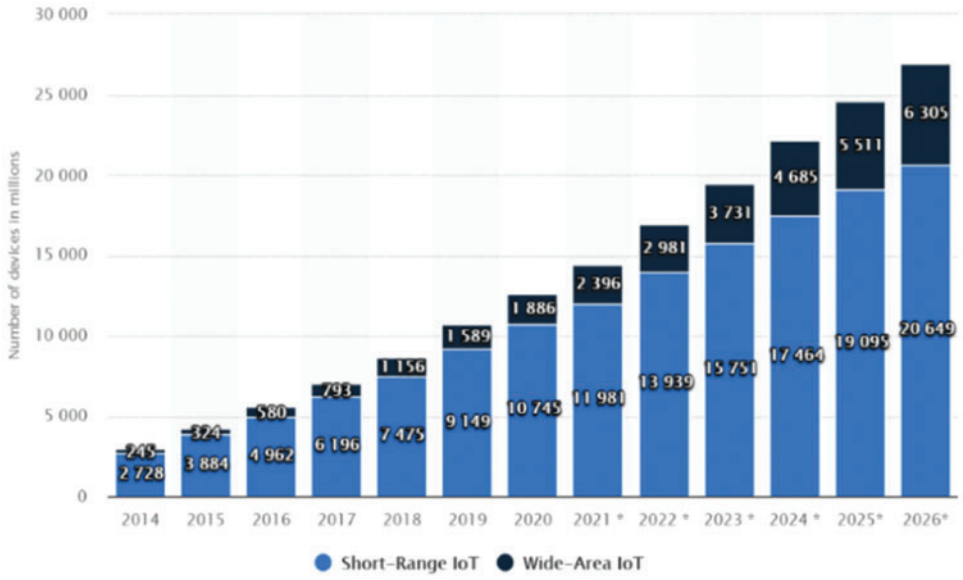

Figure 1: Total number of expected IoT and non-IoT devices till the year 2026 [4]

WSNs are a collection of nodes or many sensor nodes that may be put anywhere in the environment. These networks might be used in various control systems, including environmental monitoring, home automation, chemical, and physical assault detection, surveillance, and many more [5]. The downsizing of electronic equipment has aided WSN deployment to the point that excessive power consumption is no longer a barrier for large-scale, distant deployments. WSNs' range of applications has grown as their technical concerns have been resolved. Wireless sensor networks are generally set up ad hoc, making installing them simple [6].

Furthermore, IoT applications designed to aid the disabled or elderly are essential in delivering ease and mobility at varying degrees of unconventionality at a reasonable price [7]. The Internet of Things is quickly becoming necessary for many industrial and communication technology

applications. IoT has applications in various industries, including agribusiness, climate, clinical care, education, transportation, and finance. These improvements and advancements make our lives more accessible [8]. In today's competitive economy, the majority of supply chains struggle to retain their competitiveness in the global supply chain due to the increasing complexity of each level of supply chain operations. Businesses must use critical technologies to become more competitive and sustainable in the global supply chain, and operations must be better managed and automated wherever feasible [9,10]. One of the key concepts of Industry 4.0 is the "smart factory," which is envisioned as a fully connected manufacturing system that operates primarily without human intervention by generating, transferring, receiving, and processing all necessary data to perform all necessary tasks and produce all types of goods [11]. Using the Internet of Things (IoT), sensor networks, and wireless networks, Industry 4.0 is based on the interconnectedness of three key components: people, things, and businesses [12]. Market demands and new technologies are transforming manufacturing firms' business operations and creating smart factories and warehouses.

The current study emphasizes the importance of the "Internet of Things" concept in data collection and real-time information sharing [13]. IoT devices will be operational on a scale of over 10 billion by 2021. IoT devices will be operational on more than 25.4 billion different systems by 2030. Data generated by IoT devices will total 73.1 zettabytes (ZB) by 2025 [14]. Businesses in the IoT sector were expected to earn more than 450 billion dollars in sales in 2020. In 2021, it is predicted that the IoT market, which includes hardware, software, systems integration, and data services, would be worth $520 billion. According to estimates, the worldwide market for Internet of Things (IoT) technology will reach $1 trillion by 2022. By 2027, it is expected that the Internet of Things market would reach $2 trillion [15]. Fig. 1 states the expected number of installed short-range and long-range IoT devices in millions from the year 2014 to the year 2026 [16].

Intelligent factories and warehouses are emerging as a result of changes in the business operations of manufacturing organizations in response to market demands and new technologies. Due to the complexity of each level of supply chain operations in today's competitive market, the majority of supply chains are attempting to preserve their competitiveness in the global supply chain. Traditional approaches and systems are also prone to different forms of assaults, including worms, Trojan horses, viruses, and malware, as well as denial of service, distributed denial of service, hello flood, and replay attacks. As aforementioned, several works have been done in the literature regarding WSN and IoT. However, the contributions of the proposed work are listed as follows:

- Finally, that arrangement was decided. The objective is to pinpoint the main research gap or gray region in the area so that others may address it. Regarding network performance degradation, RSTP messages are more effective than other BPDU formats.
- The proposed study also highlights the assaults mentioned above, especially at the data link layer, to increase network security.

Based on the preceding explanation, the suggested effort focuses on three questions' and targets them as follows:

Q1. What security attacks have existed in WSNs?

Q2. What are the exciting issues in wsn and Iot frameworks?

Q3. What are common attacks in Data Link Layer?

Table 1 summarizes the investigation findings, and Fig. 2 shows the paper selection mechanism regarding the targeted domain.

Table 1: Research finding mechanism

Review questions	Q1. What security attacks have existed in WSNs? Q2. What are the existing issues in wsn and Iot frameworks? Q3. What are common attacks in data link layer?
Research selection criteria	• Journal articles, conference papers, reports • Research published during the period between 2014–2021 • Researchers must provide the answers to the research questions. • Research also contains the title, year, and source. • The survey targeted network security attacks, WSN issues, data link layer issues, WSN and IoT similarities, challenges of data link layer attack
Research exclusion criteria	• Summaries of events and seminars. • The publication is not in English.
Literature search	• Source: IEEE, Springer, peerj, and Scopus • Search equations: Data link layer issues, network security attacks, wsn issues, data link layer issues, WSN and IoT similarities, challenges of data link layer attack
Targeted area (No of studies) [reference]	• Background and statistics (15) [1–16] • Similarities of WSN And IoT (1) [17] • Issues In WSN and IoT frameworks (11) [18–31] • Network security attacks in IoT and WSNs (7) [32–47] • Issues of data link layer [48–54] • Challenges of data link layer attack(1) [49] • Attacks on the data link layer (2) [50,51] • Idea proposed (3) [52–54]

This research gave a broad review of several approaches and techniques used in WSNs. The academic papers chosen for discussion in this review research year by year from 2011 to the present are shown in Fig. 3.

The rest of the sections are organized as follows: The second section looks at network security assaults, and the third looks at vulnerabilities with WSNs and IoT frameworks. Section 4 then discusses the similarities between WSNs and the IoT; Section 5 then discusses data link layer issues; Section 6 challenges the data link layer attack; Section 7 then attacks the data link layer and discusses the proposed idea; Section 9 then provides a discussion based on research questions, and Section 10 concludes the paper.

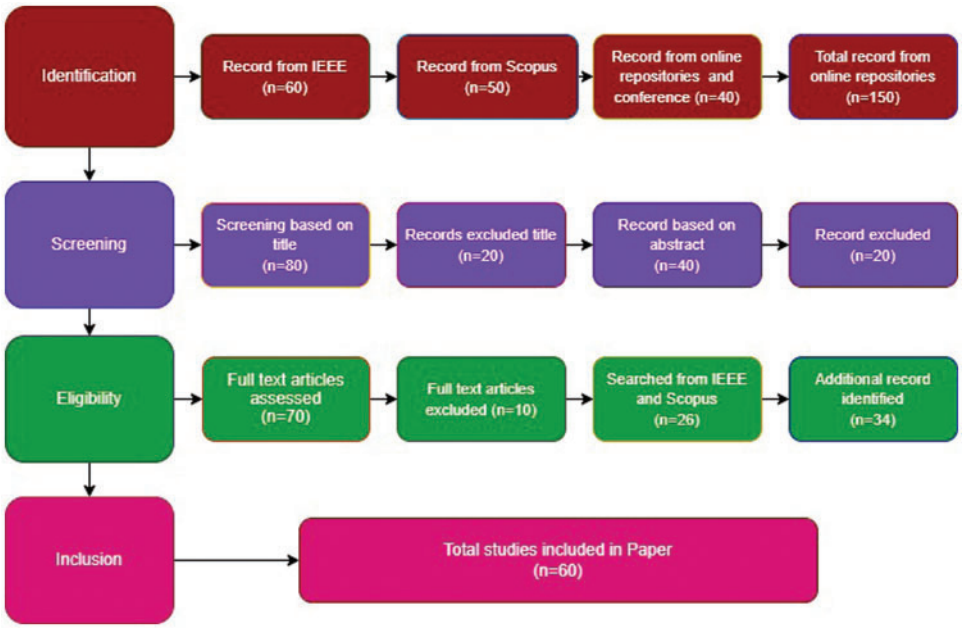

Figure 2: Research selection mechanism

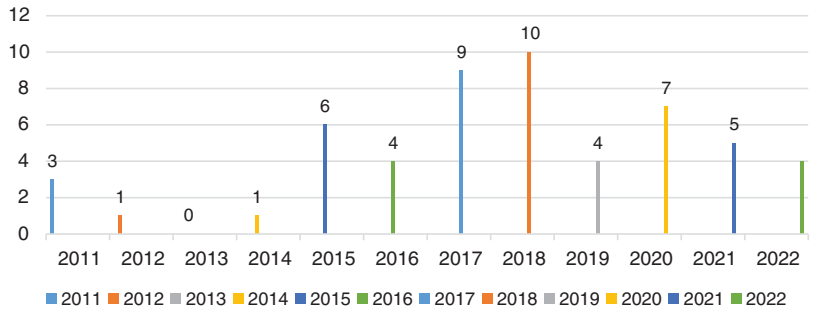

Figure 3: Distribution of these review papers by year of publication

2 Similarities of WSN and IoT

These two domains are intelligent and environment-friendly, with sensors connected via networking devices to collaborate and make human lives more manageable. The WSN is a driver of smart agriculture, while the IoT promotes agricultural output and efficiency. Both IoT and WSN have been accepted in the healthcare system, which may be because IoT and WSN may be used in a variety of equipment, such as cameras and beds, heat, stoves, and accelerometer sensors [17]. Implementation of a real-time monitoring system for meal carts using WSN and IoT. A comparison of the performance of both methods on real-world facilities.

Similarly, IoT installation results in significantly reduced latency. Therefore, the position of trolleys has no bearing on the latency of IoT installation. Furthermore, the IoT deployment results in longer battery life.

3 Issues in WSN and IoT Frameworks

In this section, various significant issues of WSN and IoT frameworks are mentioned, highlighting the importance of reducing and solving, creating an emerging area of research as well.

3.1 Security

One of the essential needs in run-time applications is to keep the WSN secure. The network should enforce access control to prevent unauthorized access. The hub should maintain access control to prevent unauthorized access. Privacy and information accuracy must be protected [18]. Increased security threats and new security issues arise as the number of linked devices to communication networks grow in the Internet of Things (IoT). Any node is connecting to the internet, whether a restricted or smart device, acquires security concerns [19]. Some of the crucial security criteria for the IoT are acceptance, confirmation, classification, confidence, and information security. Whether it uses basic or advanced technologies, each gadget linked to the internet has security issues [20]. Acceptance, confirmation, categorization, confidence, and information security are some of the essential security requirements in the IoT. Outsiders or employees within the company might be intruders. As a result, keeping up security with various organizational arrangements is extremely difficult for the flexible detecting gadget. Safeguarding information against dictatorial forces or illegal access is described as "security. Information security, often known as computer security, is critical to IoT security [21].

3.2 Data Privacy and Confidentiality

A major issue with IoT and network security is data confidentiality. The customer has access to the data and manages the system in IoT frameworks. The Internet of Things device should be able to confirm if the user or device has been granted access to the system [22]. Approval decides whether a person or device may receive assistance after presenting distinct evidence. Access management is the process of restricting access to properties by granting or denying authorization in accordance with a set of laws. In order to get system access, numerous clients, objects, and devices must first authenticate one another through trusted administrations. The challenge is figuring out how to manage the client's personality, possessions, and technology in a secure manner [23]. Privacy and confidentiality with IoT devices and frameworks are key problems due to the pervasiveness of IoT and WSN systems. Information protection is one of the major unknowns in the IoT due to the considerable danger of security flaws such sniffing and spoofing, unauthorized access, data modification, and forging with the unauthorized alteration of IoT and WSN nodes [24]. Security matters much in acquiring information, just as it does in sharing knowledge; therefore, the exploration problems must be addressed. An aggressor can utilize a variety of IoT administrations and apps to store sensitive and personal data. If they are exposed as unstable, sensitive data can be exposed to outsiders [25].

3.3 Data Gathering and Transmission

The primary goal of WSNs is to collect data and transfer it to where it is needed. Since data from the appropriate environment will be gathered and delivered to the base station, the sensors will be used sporadically. Data is collected and forwarded to the sink hub as part of the information collection process. At times, the obtained data is more than useless. Therefore, transferring it to the sink hub is unnecessary since it would consume energy. As a result, caution should be exercised when gathering and transmitting data [26]. In many instances, entities are linked, and information is sent and sold through the internet, offering client protection while posing numerous threats to sensitive data. The attacker can break a node or gather vital or unusual data that could be used against the system.

Additionally, the attacker can remove a node and steal it or replace it with a rogue node, harming the entire network [27].

3.4 Resource Limitations

If not correctly handled, a few restrictions on necessary resources in the WSN and IoT might influence network performance. The network makes use of sensors, which need energy to operate. The network also needs a communication channel to function because the nodes rely on the internet for data transfer. As a result, both are always required to maintain everything operating properly; otherwise, the network would collapse. Due of their inadequate computational, battery, and communication capacities, the nodes have restricted resources. This is a recurring issue regarding gadget-level security, as the expense of heavyweight security calculations, which need more assets to maintain network speed, cannot be afforded. As a result, a low-level, regulated security component is necessary to restrict force use during interruption identification measures. WSN's lifespan will be extended because of this. Numerous techniques have been developed to address node resource constraints [28,29].

3.5 QoS (Quality of Service)

The quality of service (QoS) indicates sensor networkability when gathering specific implementation parameters. QoS may be described as program-specific and network-specific [30]. Organizational involvement, the optimal number of dynamic sensors, efficiency, an estimate of sensor detail, dormancy, and delay accuracy are among the particular limitations of the QoS application. The QoS network's perspective refers to effectively managing resources and transmission power and fulfilling application requirements. WSN's QoS can also withstand expansion by canceling nodes. Because the enterprise's geography tends to evolve and data management is ambiguous, tracking QoS boundaries for sensor networks is difficult. However, a Computational Geometry method is adaptable to enhance the QoS [31].

3.6 Tampering

The sensor might be placed in a harsh climate, in a distant location with poor security, etc. In such an environment, the likelihood of a sensor being physically assaulted is significantly higher; therefore, physical protection cannot be guaranteed. Tampering with the network involves disconnecting or altering the current network, which is a (Denial of Service) DoS assault. The attacker can substitute a fake or malicious node for the original node. IoT and WSN networks are prone to stealing sensor hubs, allowing attackers to modify data or transmit malware throughout the network, causing significant harm. After demonstrating the actual theft of devices, the adversary may isolate sensitive data from the captured devices to launch subsequent attacks on the WSN and IoT architectures. Constant network monitoring is necessary to stop or control physical assaults and guarantee security so that the WSN cannot be tampered with and the network's performance stays stable.

3.7 Authentication and Authorization

Nodes are the building blocks of the Internet of Things that must be defined in the network or physically. IoT networks span a broad region to trace the transmission between devices and access the whole network. Without data consistency, the overall naming arrangement of nodes is unsafe. Attacks on domain name system (DNS) cache placement might harm the network's overall performance. Node identification is required for each target to be individually recognized. Because each mark represents a potential assault site, the fake node should be discovered as quickly as possible. Devices and their

data must be protected from physical and logical assaults on the network. Authentication necessitates the verification of the nodes' identities. The confidentiality and fairness of the messages transmitted cannot be guaranteed if communication with the proper node is not established. If authentication is not properly managed, an attacker can gain access to the network and make fraudulent claims. Authentication is difficult to achieve due to the abundance of wireless media and the nature of sensor networks. Validating that you are who you claim you are is what authentication implies. This is often performed through the use of a login and password authentication approach. However, this method is insufficiently secure. Passwords should be updated on a regular basis, and computers should not be left alone. Authentication also involves the use of an authentication method by both the sender and the recipient to authenticate the provenance of the messages.

4 Network Security Attacks in IoT and WSNs

The network security assaults on the IoT and WSN layers are described in Table 2. The attacks are categorized accordingly to the network layers they hit and cause damage to. The table also depicts how much IoT and WSN share common attributes within.

Table 2: Network security breach in the IoT and WSN layers

Sr #	Network layer	Attacks
1	Physical layer	Interception, Radio interference, Jamming, Tempering, Sybil attack
2	Data link layer	Replay attack, Spoofing, altering routing attack, Sybil Attack, collision, traffic analysis, monitoring, exhaustion.
3	Network layer	Blackhole attack, wormhole attack, sinkhole attack, grey hole attack, selective forwarding attack, hello flood attack, misdirection attack, internet smurf attack, spoofing attack.
4	Transport layer	De-synchronization, Transport layer flooding attack
5	Application layer	Spoofing, alter routing attack, false data ejection, Path-based DOS

4.1 Denial of Service Attack (DOS

A denial-of-service (DoS) attack is a sophisticated attack in which the perpetrator aims to make a machine or framework resource challenging or inaccessible to its intended user. It is accomplished by flooding the target with movement or sending it data that causes a collision with its authorized customers by rapidly or uncertainly exacerbating the network of a host connected to the internet. DoS attacks succeed in two ways: they deny authenticated clients access to services they expect [32].

4.2 Distributed Denial of Service Attacks (DDoS)

DDoS is a type of DoS assault in which many sites launch attacks simultaneously. By flooding the anticipated Uniform Resource Locators (URL) with more requests than the server can handle, a DoS attack tries to render an online site inaccessible to its users. Unlike a DoS assault, a DDoS attack needs several infected nodes to flood a single target with messages or connection requests, causing the device server or network resource to slow down or crash [33,34].

4.3 Hello Flood Attack

It's a type of network-layer assault. HELLO, packets are used as weapons in the Hello, flood assault to convince the wireless sensor network node. In this type of attack, an attacker with a significant radio transference value and network capacity delivers HELLO packets to numerous sensor hubs scattered throughout a large WSN. As a result, when transferring data to the base station, the unlucky victim nodes try to catch up with the aggressor. The culprit finally mocks them since they know it is their neighbor [34].

4.4 Replay Attack

It's a type of network-layer assault. The replay assault is a device attack directed by a specific class in which an aggressor defines an intelligence conversion and falsely has it postponed or rehashed. The sender or harmful material completes the delay or rehashing of the information transmission by capturing and retransmitting the information. When an attacker repeats a flood of messages between two gatherings and replays the stream to update their directing table on stale courses, this is known as a replay assault [35].

4.5 Worms, Trojans, Viruses, and Malware

Malicious software can be used by an attacker to alter data, steal information, or even assault a device with a denial-of-service attack. You can get a computer worm when you download a file or get an update. The worm then replicates and starts attacking other networked computers. Your computer becomes infected with the Trojan horse when you download and open a file. Unlike viruses, most Trojans can only be located on your computer. A virus affects your computer's host files when you transfer data over email, and it then spreads to other user [36,37]. Malware is any program that can affect the output and operation of your computer equipment, both locally and remotely. If data from IoT devices is compromised, malware might pollute the cloud or data centers [38].

4.6 Black Hole Attack

It is a network-layer assault known as a packet drop attack. In this network, a node sends an route request packet (RREQ) packet to all its neighbors. Throughout the way-finding process, a malicious node publicizes the erroneous routes as the appropriate way to the originating hub. When the source selects a path that includes the assailant hub, the activity begins to pass via the adversary hub, then dropping packages individually or in bulk. Many damaging assaults travel through the dark gap [4,39].

4.7 Sink Hole Attack

Attempts by nodes to attract system traffic by advocating its fake guiding reform were jeopardized by a kind of attack. A network-layer assault is referred to as a sinkhole attack. The sinkhole node tries to pull all system movement in its direction, which changes the information bundles, shortens the system lifetime, entangles the system, and eventually destroys it. Furthermore, it is frequently utilized to carry out novel assaults such as specific sending ambushes, perception satirizing strikes, left or changed directing data, and a hostile node generates forged guiding data. It poses as a genuine node for the course [40–44].

4.8 Data Integrity Attack

This is an example of a network layer intrusion. In a wormhole assault, an aggressor gathers bundles at a specific point in the system and tunnels them to another place in the framework. It

replicates them in the structure that starts there a little time later. Wormhole nodes in a system imitate a course, making it shorter than the original. This throws off the directing components, which rely on learning about node separation. Without understanding the system or trading off honest nodes, the aggressor may carry out this attack [45].

4.9 Selective Forwarding

In this network assault, malicious nodes fail to assist any data packets, preventing them from being sent to other nodes. The rogue node can change, drop, or selectively forward all communications to other network nodes. As a result, the data transmitted to the intended recipient is insufficient [46].

5 Issues of Data Link Layer

5.1 Services at the Network Layer

This service's primary objective is to deliver network-layer services. This layer's duty is to transfer data from the network layer of the source machine to the network layer of the destination machine. For communication between the two data layers, the Data Link Control Protocol is utilized. Many critical services are sent from the Data Link layer to the Network layer, including invisible c-less services, recognized help that does not require a connection, and well-known services [47].

5.2 Framing

The services offered to the network layer data connection are used by the physical layer. Data is sent in frames from the source machine to the destination machine. The destination computer should be able to see where the frame starts and ends so that it can quickly identify the structure. The bitstream is decoded and the layer checksums are computed by the data link layer. At the destination layer, the checksum is listed. By introducing blank spaces and temporal pauses, framing divides the bitstream. It is difficult and risky to keep track of the time and note the beginning and conclusion of each frame. There are several methods for framing [48].

5.3 Flow Control

Flow control is used to halt data transmission at the receiver's end. The frames will be sent from the transmitter to the receiver quickly. However, because the sender uses a lightly loaded machine, the receiver uses a densely packed machine, and the receiver will not take them as rapidly as the sender. As the frames arrive, the receiver will be unable to manipulate them. It makes no difference if the transmission is flawless at some point. Following are the ways to terminate transmission by requesting the transmitter block any wrong signals.

- Flow control based on feedback
- Flow control based on a rate

5.4 Error Control

The goal is to prevent copying and guarantee that the frames reach their destination without incident. As a result of reaching structures, both positive and negative acceptance messages are also sent. In light of this, the frame seems to be in fine shape if the sender experiences favorable acceptance. Positive look, on the other hand, denotes that the frame is in good condition; otherwise, it will be re-transferred. The sender and recipient both have timers configured. Moreover, a sequence number is given to the transmission's outbound data. Since it is a retransmitted frame, the receiver will be

able to tell right away. One of its main duties falls under the purview of the data connection layer [40–50]. Similarly, the data link layer deals with transmission problems; it provides transmission acknowledgment of frames to protect connections if a structure is lost and is also responsible for recognizing and eliminating duplicate frames.

5.5 Physical Address of Frames

The data connection layer adds the Data Link Layer (DLL) to the frame to describe the physical address of the sender or recipient. Denial of service (DoS), Media Access Control (MAC) cloning, and layer-2-based broadcasting are three assaults that affect the data connection layer. Address Resolution Protocol (ARP) answers that have been fake sent to network hosts constitute a broadcast assault. The broadcast address is substituted for the default gateway's MAC address in these ARP answers. In Layer 2-based DoS attacks, the attacker modifies the ARP caches of network hosts using MAC addresses that don't exist. The attacker utilizes the target host's MAC and Internet Protocol (IP) addresses after employing a DoS attack to disable it. A globally unique MAC address is expected to be assigned to each network interface device. Enabling MAC cloning, however, makes it simple to alter [51]. Because the interface between the host and the network systems is weak, attacks take place at the data link layer. The data connection layer guarantees effective data transmission between networked machines [52,53].

6 Challenges of a Data Link Layer Attack

Attacks on the DLL are also possible. An attacker may purposely breach the communication protocol, sending messages often to generate communication channel collisions [54]. Collisions of this nature would require the retransmission of any packets affected by the collision. An adversary might use this strategy to drain the power supply of a sensor node by including oversupply retransmission. In the data, there are seven possible risks. Denial-of-service attacks: the data link layer comprises collisions, unfairness, and battery fatigue. Denial of service attacks on the network layer include traffic misdirection, hello flood attacks, homing, selective forwarding, Sybil, wormholes, and acknowledge flooding.

7 Attacks on the Data Link Layer

Intrusion detection systems usually operate at layer 3 or higher on the Transmission Control Protocol (TCP)/Internet Protocol (IP) stack since layer 2 protocols in local area networks are trusted. For the same reason, layer 2 capabilities of existing firewall technologies are quite limited. Physical access control to network connections has always been the cornerstone of trust in layer 2 protocols. New applications of these protocols, however, extend layer 2 networks' reach beyond the physical custody of a single company. In addition, one of the biggest threats is from insiders. From the perspective of the network layer, the effect of denial-of-service attacks on a layer 2 routing protocol is examined [55]. We discovered considerable performance and resilience decrease in our trials. We also look into topological engagement attacks, which undermine the concept of traffic separation in switched local area networks by enabling layer 2 traffic spying without setting off layer 3 alarms. To lessen the effects of such attacks, various safety measures are suggested. Finally, we provide concrete experiments to show how effective the suggested countermeasures are. Because of the vulnerability of the interface between the host and network systems, attacks take place at the data connection layer. The data connection layer guarantees effective data transmission between networked machines [56]. Table 3 shows the data link layer attacks.

Table 3: Popular data link layer attacks with description

Attack name	Description
MAC attacks (CAM table flooding)	A switch is inundated with MAC addresses randomly. As a result, the switch's table fills up. The switch is compelled to function as a hub.
Spanning Tree Protocol (STP) attacks	Switches are sent incorrect BPDU packets to modify the spanning-tree topology. If the topology is often limited, a Dos attack can be initiated.
Cisco Discovery Protocol (CDP) attacks	Incorrect CDP information is supplied to switches and routers, causing them to malfunction.
Virtual local area networks (VLAN) attacks	By transmitting incorrect VLAN information to switches, either network Configurations are modified, or ii) network functioning is badly harmed.
Dynamic Host Configuration Protocol (DHCP)	Attacks on networks are made by interfering with DHCP processes. Attacks such as a man in the middle are possible.
ARP attacks	Attacks on networks are made by interfering with ARP operations. The operation of a network can be significantly harmed in these assaults (for example, a rogue router can become the network's default gateway).

7.1 Data Link Layer

Fig. 4 shows the classification of attack in more detail. The type is based on three categories: common attacks, widespread attacks, and layer 2 (data-link layer attack) attacks. Table 4 Shows the STP security as well as attacks.

7.2 Spanning Tree Protocol

In this phase prevention/security of STP as well as different attacks are dicussed, whease the spaning tree protocol is show in Fig. 5.

7.3 Wireless LANs

Fig. 6 shows the wireless LAN along-with types, attacks, and wired equivalent privacy:

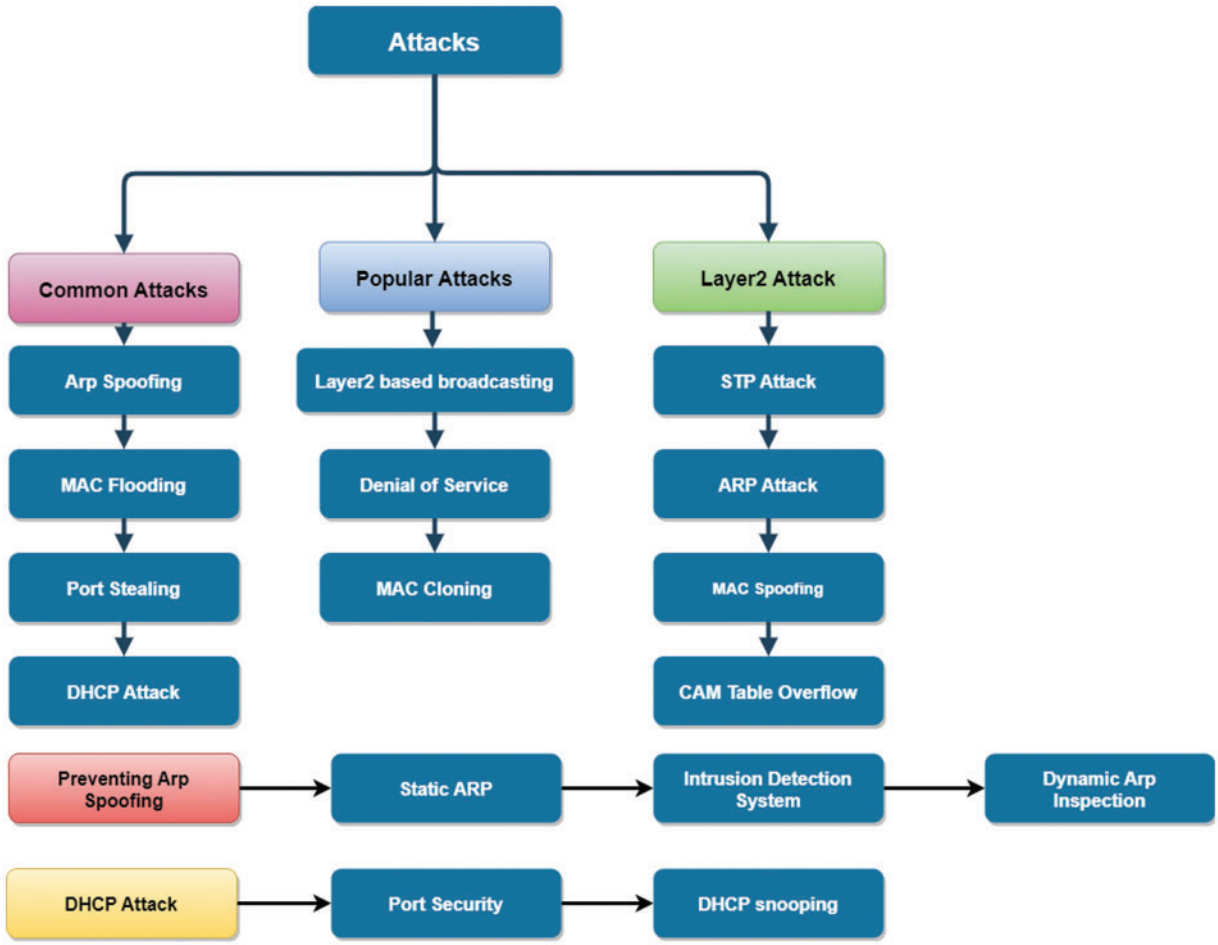

Figure 4: Data-link layer attacks

Table 4: Spanning Tree Protocol (STP) security and attacks

Security	Attacks
STP ensures no data flow loops occur when a network includes redundant links.	Taking over the root bridge attack is disruptive, mainly at layer 2.
The network's resilience is ensured through the use of redundant paths.	Any BPDU is accepted by the LAN switch, which sends neighboring BPDUs to face value every 2 s.
STP is a layer 2 connection management protocol.	The attacking switch does not attempt to take over as root due to the DoS employing a flood of configuration BPDUs.
They can create fatal loops in the network, resulting in a DoS attack.	Creates a significant number of BPDUs per second, causing the switches' CPUs to be overworked.

Figure 5: Spanning tree protocol

Figure 6: Wireless LANs

7.4 Results of Attacks

Based on parameters such as attack description, recovery, target, packet loss, BPDU/s, and Pings. After analyzing or reviewing several studies, we draw the results of several attacks based on the parameters above. Table 5 discusses the results of several attacks.

Table 5: Complete results of several attacks

Attack description	Recover	Target	Packet loss	BPDU/sec	Pings
Connection Manager (CM) STP messages	75 s	3	69%	120 K	$3 \Rightarrow 2, 4 \Rightarrow 3, 6 \Rightarrow 3$
CM RSTP messages	47 s	3	100%	119 K	$3 \Rightarrow 2, 4 \Rightarrow 3, 6 \Rightarrow 3$

(Continued)

Table 5: Continued

Attack description	Recover	Target	Packet loss	BPDU/sec	Pings
CM STP & RSTP	74 s	3	100%	120 K	3 ⇒ 2, 4 ⇒ 3, 6 ⇒ 3
CM & Topology Change Notification (TCN) STP & Connection Manager Topology Change Notification (CM RSTP)	91 s	3	99%	122 K	3 ⇒ 2, 4 ⇒ 3, 6 ⇒ 3
Topology Change Notification Spanning Tree Protocols (TCN STP) messages	3 s	3	23.6%	131 K	3 ⇒ 2, 4 ⇒ 3, 6 ⇒ 3
CM STP messages	97 s	5	80%	121 K	3 ⇒ 2, 4 ⇒ 2, 2 ⇒ 6
Connection Manager Rapid Spanning Tree Protocol (CM RSTP) messages	30 s	5	100%	120 K	3 ⇒ 2, 4 ⇒ 2, 2 ⇒ 6
CM STP & RSTP	52 s	5	97%	120 K	3 ⇒ 2, 4 ⇒ 2, 2 ⇒ 6
CM & TCN STP & CM RSTP	61 s	5	88.3%	123 K	3 ⇒ 2, 4 ⇒ 2, 2 ⇒ 6
CM STP messages	89 s	4 (Root)	93.6%	121 K	1 ⇒ 5, 3 ⇒ 5, 2 ⇒ 6
CM RSTP messages	54 s	4 (R)	100%	120 K	1 ⇒ 5, 3 ⇒ 5, 2 ⇒ 6
CM STP & RSTP	78 s	4 (R)	97.3%	120 K	1 ⇒ 5, 3 ⇒ 5, 2 ⇒ 6
CM & TCN STP & CM RSTP	71 s	4 (R)	96%	125 K	1 ⇒ 5, 3 ⇒ 5, 2 ⇒ 6
TCN STP messages	60 s	4 (R)	91%	132 K	1 ⇒ 5, 3 ⇒ 5, 2 ⇒ 6

In Table 5, the results are organized by experiment number, attack description, number of BPDU messages generated per second with the attack tool, origin and destination of the sets of pings, hierarchical level of the target switch in the spanning tree, percentage of packet loss (as measured by pings after 5 min of flooding), and time is taken for the target switch to become responsive to Internet Control Message Protocol (ICMP) traffic after the attack was suspended. As indicated in Table 5, the pings were sent from station 5 to station 3. The recovery period is revealed in experiment Table 4 by pings delivered from station 4 to station 6 immediately following the break-up of the attack. In conclusion, Table 6 demonstrates that the pings were transmitted from station 3 to station 6. As seen in Table 4, the network's performance suffers dramatically if an attacker bombards any network bridge with fictitious, painstakingly crafted STP and RSTP messages. The target switch is positioned higher in the tree hierarchy, as shown in Table 4, the more successful the flooding assault is. This tendency could be accounted for by the fact that certain switches statistically carry more trunk traffic than switches

at lower scale levels. Due to the increased amount of traffic arbitration decisions that these switches must make in addition to the computational burden brought on by the flow of BPDU messages, these switches must use additional CPU resources (constant in attacks on Tables 4 and 5). Configuration message RSTP messages are more effective in preventing a decline in network performance than other BPDU formats (namely, configuration message and topology change notification RSTP).

8 Idea Proposed

In terms of networking, Layer 2 occasionally acts as a weak link. A security system is only as strong as its weakest link. The Layer 2 security methods covered in this chapter assist in defending a network from a variety of dangers. The most popular Layer 2 attack methods highlight the level's weaknesses and emphasize that the other tiers are aware of the problem. To safeguard the higher levels of the Open Systems Interconnection Model) (OSI) reference model, network-level tools like firewalls, intrusion prevention systems (IPS), and programs like antivirus and host-based intrusion protection are all employed (HIPS). If your network doesn't use Ethernet as its layer 2 protocol, some of these attacks might not be applicable to you, even if a network like that is likely to be vulnerable to a variety of assaults [57]. The attacker may intercept communications, alter data, stop the flow of information, or employ a mix of the aforementioned techniques. These options pose a serious danger to crucial infrastructure, state institutions, or governmental processes even when no malice is intended. The internet controls some crucial infrastructure, which is maintained by landline and mobile communications companies [58,59].

9 Discussion

In this study, we explored a variety of security assaults that occurred at network layers, such as physical, data link, network, transport, and application. However, particular attacks connected to specific layers are indicated in the table. Researchers can readily identify layer-based assaults this way. Similarly, certain typical assaults, such as DoS, DDOS, and black holes, are examined in greater depth in this research. Then, significant issues like security, data confidentiality, authorization, and so on are discussed.

Furthermore, this study emphasizes data link layer assaults, classified into three types (common attacks, layer 2 attacks, and widespread attacks), and some protection techniques shown in Fig. 2. DHCP assaults are frequent, and attacks on networks are carried out by interfering with DHCP procedures. A man-in-the-middle attack is a possibility. STP attacks are described while addressing Layer 2 attacks, in which switches are delivered erroneous BPDU packets to change the spanning-tree topology. DoS attacks can be launched if the topology is often altered. However, infamous assaults and typical attacks such as denial of service are mentioned, which might be triggered by imbalanced traffic. At the same time, the comparison and overall results reveal that STP-related attacks are more efficient in terms of network performance degradation.

10 Conclusion

This research discusses several security issues at different network levels, including physical, data connection, network, transport, and application. The chart does, however, note specific assaults related to different levels. This makes layer-based attacks easy to recognize for researchers. In the same way, specific common attacks like DoS, DDOS, and black holes are more thoroughly

investigated in this study. The discussion then turns to fundamental problems like security, data privacy, authorization, etc.

Furthermore, this study focuses on data link layer attacks, which are grouped into three groups (common attacks, layer 2 attacks, and widespread attacks) and specific defense mechanisms illustrated in Fig. 2. STP attacks are discussed in the context of Layer 2 assaults, in which switches are sent erroneous BPDU packets in order to modify the spanning-tree topology. DHCP attacks are common in which attacks on networks are carried out by interfering with DHCP operations. A man-in-the-middle assault is conceivable. DoS attacks are possible if the topology is often changed. However, prominent and common attacks like denial of service are highlighted, which may be caused by unbalanced traffic. At the same time, the comparison and overall results show that STP-related attacks are more effective in terms of degrading network performance.

According to industry trends, numerous internet service providers are investigating Layer 2 (L2) services for the final mile to the consumer. Despite administrative solid and economic considerations, a universal L2 switching architecture threatens to replace L3 switching and dynamic routing protocols in large corporate Local Area Networks (LANs) and Controller Area Network (CANs). Performance arguments must also be guaranteed to assure the success of this flat L2 architecture. In this context, several challenges stemming from the lack of robustness of STP implementations have substantially impacted services that are important to our society [24]. If the attack tool successfully creates loops in the topology (STP) or inhibits tree formation, the investigated network architecture will perform much worse (RSTP). In both circumstances, RSTP appears to be of unquestionable benefit in leveraging system administrative requirements. This research discusses further assaults on R/STP that substantially impact their resilience. The attacks are intended to interfere with the regular operation of the protocol by taking advantage of the BPDU packets' lack of authentication.

Furthermore, the network's ability to survive is gravely endangered by the attack tool's capacity to play an active part in the topology. Significant consequences of this attack include Layer 3 transparent traffic surveillance and Virtual local area networks (VLAN). The discovery of protocol issues has led to offering new possible RSTP enhancements. Although they could impact performance, these innovations take on a challenging task: reducing design flaws in the initial specifications of the protocols. The validity and effectiveness of the suggested treatments are therefore evaluated using a comprehensive set of studies. The scope of this study will also be expanded to include resource restriction strategies, the use of cryptographic and digital signatures, and the optimization of WSN MAC protocols.

Funding Statement: This work is partly supported by the Malaysian Ministry of Education under Research Management Centre, Universiti Putra Malaysia, Putra Grant scheme with High Impact Factor under Grant Number UPM/700–2/1/GPB/2018/9659400.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] N. Sun, X. Wang, G. Han, Y. Peng and J. Jiang, "Collision-free and low delay MAC protocol based on multi-level quorum system in underwater wireless sensor networks," *Computer Communications*, vol. 173, no. March, pp. 56–69, 2021.

[2] Y. Ashibani and Q. H. Mahmoud, "Cyber-physical systems security: Analysis, challenges, and solutions," *Computers & Security*, vol. 68, pp. 81–97, 2017.

[3] H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo *et al.,* "A review of iot sensing applications and challenges using RFID and wireless sensor networks," *Sensors (Switzerland)*, vol. 20, no. 9, pp. 1–18, 2020.
[4] P. Osterrieder, L. Budde and T. Friedli, "The smart factory as a key construct of industry 4.0: A systematic literature review," *International Journal of Production Economics*, vol. 221, pp. 107476, 2020. https://doi.org/10.1016/j.ijpe.2019.08.011
[5] R. Sharma and S. Prakash, "Enhancement of relay nodes communication approach in WSN-IoT for underground coal mine," *Journal of Information and Optimization Science*, vol. 41, no. 2, pp. 521–531, 2020. https://doi.org/10.1080/02522667.2020.1724616
[6] B. Rashid and M. H. Rehmani, "Applications of wireless sensor networks for urban areas: A survey," *Journal of Network and Computer Applications*, vol. 60, pp. 192–219, 2016.
[7] U. Tandale, B. Momin and D. P. Seetharam, "An empirical study of application layer protocols for IoT," in *2017 Int. Conf. on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, India, pp. 2447–2451, 2018.
[8] M. Farsi, A. Daneshkhah, A. Hosseinian-Far and H. Jahankhani, *Internet of Things Digital Twin Technologies and Smart Cities*, Germany: Springer, 2020.
[9] H. Oliff and Y. Liu, "Towards industry 4.0 utilising data-mining techniques: A case study on quality improvement," *Procedia CIRP*, vol. 63, pp. 167–172, 2017.
[10] A. A. Kumar S., K. Ovsthus and L. M. Kristensen, "An industrial perspective on wireless sensor networks-a survey of requirements, protocols, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1391–1412, 2014.
[11] S. Sanuk, S. Grabowska and B. Gajdzik, "Social expectations and market changes in the context of developing the industry 4.0 concept," *Sustain.*, vol. 12, no. 4, pp. 1362, 2020.
[12] B. Jovanović, "Key IoT statistics," *DataProt*, 2021. Key IoT Statistics. 2021. Available online: https://dataprot.net/statistics/iot-statistics/ (accessed on 20 December 2022).
[13] A. Multiple, "30 internet of things–IoT stats from reputable sources in 2021," *AI Multiple*, 2021. https://research.aimultiple.com/iot-stats/ (Accessed May 30, 2021).
[14] S. O'Dea, "Wide-area and short-range IoT devices," *Statistica*, 2021. https://www.statista.com/statistics/1016276/wide-area-and-short-range-iot-device-installed-base-worldwide/ (accessed May 29, 2021).
[15] M. Wollschlaeger and T. Sauter and J. Jasperneite, "The future of industrial communication: Automation networks in the Era of the internet of things and industry 4.0," *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 17–27, 2017.
[16] A. A. Kumar S., K. Ovsthus and L. M. Kristensen, "An industrial perspective on wireless sensor networks-a survey of requirements, protocols, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1391–1412, 2015.
[17] IEEE 802.1X-2001 IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control (EAPOL), 2001.
[18] S. Raza, M. Faheem and M. Genes, "Industrial wireless sensor and actuator networks in industry 4.0: Exploring requirements, protocols, and challenges—A MAC survey," *International Journal of Communication System*, vol. 32, no. 15, pp. 1–32, 2019.
[19] C. Wittenberg, "Cause the Industry 4.0 in the automated industry to new requirements on the user interface," In: M. Kurosu (Ed.), *Human-Computer Interaction, Part III, HCII 2015, LNCS*, vol. 9171, pp. 238–245, Cham, Switzerland: Springer, 2015.
[20] H. Stverkova and M. Pohludka, "Business organisational structures of global companies: Use of the territorial model to ensure long-term growth," *Social Sciences*, vol. 7, no. 6, pp. 98, 2018.
[21] S. K. Rao and R. Prasad, "Impact of 5G technologies on industry 4.0," *Wireless Personal Communications*, vol. 100, no. 1, pp. 145–159, 2018.

[22] S. Shahbazi, M. Wiktorsson, M. Kurdve, C. Jönsson and M. Bjelkemyr, "Material efficiency in manufacturing: Swedish evidence on potential, barriers, and strategies," *Journal of Cleaner Production*, vol. 127, pp. 438–450. 2016.
[23] J. Radel, "Organizational change and industry 4.0 (id4). A perspective on possible future challenges for human resources management," 2017. [Online]. Available: https://www.researchgate.net/publication/319102143_Organizational_Change_and_industry_40_id4_A_perspective_on_possible_future_challenges_for_Human_Resources_Management (accessed on 19 December 2020).
[24] N. Yurtoğlu, "History studies," *International Journal of History*, vol. 10, pp. 241–264, 2018. http://www.historystudies.net/dergi//birinci-dunya-savasinda-bir-asayis-sorunu-sebinkarahisar-ermeni-isyani20181092a4a8f.pdf, https://doi.org/10.9737/hist.2018.658
[25] [Online]. Available: https://shiverware.com/iot/iot-vs-wsn.html. [Accessed: 17-Nov-2021].
[26] [Online]. Available: http://www.save9.com/home/products-and-services/internet-and-wireless-networks/wireless-sensor-networks/. [Accessed: 17-Nov-2021].
[27] [Online]. Available: https://www.tutorialspoint.com/design-issues-in-data-link-layer. [Accessed: 17-Nov-2021].
[28] M. A. A. Majeed and T. D. Rupasinghe, "Internet of things (IoT) embedded future supply chains for industry 4.0: An assessment from an ERP-based fashion apparel and footwear industry," *International Journal of Supply Chain Management*, vol. 6, no. 1, pp. 25–40, 2017.
[29] B. Waters, A. Juels, J. A. Halderman and E. W. Felten, "New client puzzle outsourcing techniques for dos resistance," in *Proc. 11th ACM Conf. on Computer and Communications Security*, Toronto Canada, ACM Press, pp. 246–256, 2004.
[30] T. Hussain, B. Yang, H. U. Rahman, A. Iqbal and F. Ali, "Improving source location privacy in social internet of things using a hybrid phantom routing technique," *Computers & Security*, vol. 123, pp. 102917, 2022.
[31] G. Misra, V. Kumar, A. Agarwal and K. Agarwal, "Internet of things (IoT): A technological analysis and survey on vision, concepts, challenges, innovation directions, technologies, and applications," *American Journal of Electrical and Electronic Engineering*, vol. 4, no. 1, pp. 2332, 2016.
[32] S. Devi, A. Sangwan, A. Sangwan, M. A. Mohammed, K. Kumar *et al.,* "The use of computational geometry techniques to resolve the issues of coverage and connectivity in wireless sensor networks," *Sensors*, vol. 22, no. 18, pp. 7009. 2022.
[33] G. Misra, V. Kumar, A. Agarwal and K. Agarwal, "Internet of things (IoT): A technological analysis and survey on vision, concepts, challenges, innovation directions, technologies, and applications," *American Journal of Electrical and Electronic Engineering*, vol. 4, no. 1, pp. 2332, 2016.
[34] M. Faheem, M. Z. Abbas, G. Tuna and V. C. Gungor, "Edhrp: Energy-efficient event-driven hybrid routing protocol for densely deployed wireless sensor networks," *Journal of Network and Computer Applications*, vol. 58, pp. 309–326, 2015.
[35] G. Tuna and V. C. Gungor, "A survey on deployment techniques, localization algorithms, and research challenges for underwater acoustic sensor networks," *International Journal of Communication Systems*, vol. 30, no. 17, pp. e3350, 2017.
[36] M. Faheem, G. Tuna and V. C. Gungor, "Lrp: Link quality-aware queue-based spectral clustering routing protocol for underwater acoustic sensor networks," *International Journal of Communication Systems*, vol. 30, no. 12, pp. e3257 2017.
[37] L. Parra, S. Sendra, J. Lloret and J. J. Rodrigues, "Design and deploy an intelligent system for data gathering in aquaculture tanks using wireless sensor networks," *International Journal of Communication Systems*, vol. 30, no. 16, pp. e3335, 2017.
[38] H. Ghayvat, S. Mukhopadhyay, X. Gui and N. Suryadevara, "WSN-and IoT-based smart homes and their extension to intelligent buildings," *Sensors*, vol. 15, no. 5, pp. 10350–10379, 2015.
[39] M. Periša, T. M. Kuljanić, I. Cvitić and P. Kolarovszki, "Conceptual model for informing user with an innovative smart wearable device in industry 4.0," *Wireless Networks*, vol. 27, no. 3, pp. 1615–1626, 2019.

[40] P. Angueira, I. Val, J. Montalban, I. Seijo, E. Iradier *et al.,* "A survey of physical layer techniques for secure wireless communications in the industry," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 810–838. 2022.
[41] K. K. Goyal and P. K. Jain, "Design of reconfigurable flow lines using MOPSO and maximum deviation theory," *International Journal of Advanced Manufacturing Technology*, vol. 84, no. 5–8, pp. 1587–1600, 2016.
[42] D. Zhang, Y. Qian, J. Wan and S. Zhao, "An efficient RFID search protocol based on clouds," *Mobile Networks and Applications*, vol. 20, no. 3, pp. 356–362, 2015.
[43] R. Dogra, S. Rani, J. Shafi, S. Kim and M. F. Ijaz, "ESEERP: Enhanced smart energy efficient routing protocol for internet of things in wireless sensor nodes," *Sensors*, vol. 22, no. 16, pp. 6109, 2022.
[44] P. Sharma, R. P. Singh, M. A. Mohammed, R. Shah and J. Nedoma, "A survey on holes problem in wireless underground sensor networks," *IEEE Access*, vol. 10, pp. 7852–7880. 2021.
[45] O. A. Mahdi, Y. B. Al-Mayouf, A. B. Ghazi, A. A. Wahab and M. Y. I. B. Idris, "An energy-aware and load-balancing routing scheme for wireless sensor networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 3, pp. 1312–1319, 2018.
[46] P. Arroyo, J. Lozano and J. Suárez, "Evolution of wireless sensor network for air quality measurements," *Electronics*, vol. 7, pp. 342, 2018.
[47] T. Aura, P. Nikander and J. Lewis, "Dos-resistant authentication with client puzzles," in *Revised Papers from the 8th Int. Workshop on Security Protocols*, London, UK, Springer-Verlag, pp. 170–177, 2001.
[48] M. Figueroa, "VLAN layer 2 attacks: Their Relevance and their kryptonite," *Poster Session Presented at Defcon 16*, Las Vegas, NV, 2007.
[49] W. Hsieh, C. Lo, J. Lee and L. Huang, "VLAN layer 2 attacks: Their relevance and their kryptonite," 2004 [Online]. Available: https://www.cs.dartmouth.edu/~sergey/netreads/L2-security-Bootcamp.pdf
[50] W. C. Hsieh, C. C. Lo, J. C. Lee and L. T. Huang, "The implementation of a proactive wireless intrusion detection system," in *Proc. the Fourth Int. Conf. on Computer and Information Technology*, Toronto Canada, IEEE Computer Society, pp. 581–586, 2004.
[51] C. Valli, "Wireless Snort-A WIDS in progress," In *Australian Computer, Network & Information Forensics Conference*, pp. 112–116, 2004.
[52] L. Christopher, "SANS Institute Understanding Wireless Attacks and Detection," [Online]. Available: http://www.sans.org/reading_room/whitepapers/detection/understanding-wirelessattacks
[53] K. H. Yeung, D. Fung and K. Y. Wong, "Tools for attacking layer 2 network infrastructure," in *Proc. of the Int. Multiconference of Engineers and Computer Scientists,* vol. 2, pp. 1–6, 2008.
[54] M. Malekzadeh, A. An, A. Ghani and S. Subramaniam, "Protected control packets to prevent denial of services attacks in IEEE 802.11 wireless networks," *EURASIP Journal on Information Security 2011*, 2011. http://jis.eurasipjournals.com
[55] N. Kamel, N. Hamdy and S. H. Ahmed, "A proposed intrusion detection system for encrypted computer networks," in *Third Int. Conf. on Informatics and Systems*, Giza, Egypt, pp. 19–22, 2005. http://www.cs.purdue.edu/homes/nkahmed/papers/ahmed-infos05.pdf
[56] C. K. Kumar, G. J. Arul Jose, C. Sajeev and C. Suyambulingom, "Safety measures against man-in-the-middle attack in key exchange," *Asian Research Publishing Network (ARPN)*, vol. 7, no. 2, pp. 243–246, 2012.
[57] H. C. Chaudhari and L. U. Kadam, "Wireless sensor networks: Security, attacks, and challenges," *International Journal of Networking*, vol. 1, no. 1, pp. 04–16, 2011.
[58] M. P. Pawar, H. R. Nielsen, N. R. Prasad, S. Ohmori and R. Prasad, "Behavioural modelling of WSN MAC layer security attacks: A sequential UML approach," *Center for TeleInFrastruktur, Aalborg University*, vol. 1, no. 1, pp. 65–82, 2012.
[59] T. G. Lupu, "Main types of attacks in wireless sensor networks," in *Proc. 9th WSEAS Int. Conf. on Signal, Speech and Image Processing, and 9th WSEAS Int. Conf. on Multimedia, Internet & Video Technologies*, Timisoara, Romania, pp. 180–185, 2009.