ALGERIAN DEMOCRATIC AND POPULAR REPUBLIC
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
UNIVERSITY KASDI MERBAH OUARGLA
FACULTY OF NEW INFORMATION AND COMMUNICATION
TECHNOLOGIES
DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION
TECHNOLOGY

MASTER THESIS

Specialty: Administration and Network Security

Presented by:

NASRI Hadil & ADEL Chaima

THEME

Proposing a DIO Suppression Attack in IoT Networks

COMMITTEE MEMBERS :

- Mr. BOUKHAMLA Akram   Supervisor   UKM Ouargla
- AZZAOUI Hanane   Examiner   UKM Ouargla
- BENKADEUR Med Kamel   President   UKM Ouargla

ACADEMIC YEAR: 2023/2024

Acknowledgment

First and foremost, we thank God who gave us the strength and will to accomplish this work.

We would like to extend our sincere thanks to our supervisor

Mr. Boukhamla Akram

who helped us during our work with his patience, precious advice, guidance and all these

constructive observations for the smooth running of our project.

Special thanks to the Dr. Guerbouz Tahar.

Likewise, we extend our respectful thanks to the members of the jury, who have done the

honor to participate in this jury and to examine this work.

We would like to thank all the faculty members in the Department of Computer Science for

the training they provided us throughout our academic career at the university

Finally, we would like to thank all those who helped us from near or far during all our studies

and in the preparation of this thesis, we extend to them all gratitude and respect.

Dedication 1

First and foremost, all praise and thanks are due to Allah, abundant in blessings and goodness, who granted me the ability and opportunity to achieve this accomplishment. Through His grace, I have overcome challenges and achieved my goals.

I would like to express my deep gratitude to my parents, who have been invaluable support throughout this journey. Thanks to their love and encouragement, I was able to fulfill my dream and reach this significant moment in my life.

I also want to thank my dear sister, IMANE, for her unwavering support, and her adorable children Yaakoubn and Razan, who have prayed for my success. I am also grateful to her husband, MOUNIR, for his encouragement and support.
A special appreciation goes to my sister, NIHAD, for her invaluable support and wise advice based on her experience, And I can't forget to mention my elder brother MOHAMED and my younger brother HOUDAYFA for standing by my side.

I am incredibly grateful for the friendships I've made during my university residency. These friendships have been a source of support, laughter, and growth throughout my time here. Sharing this experience with such wonderful friends has made my university residency truly memorable and fulfilling. Thank you all for being a part of my journey.

And to my best friend, IMAN DJENANE EDAR, I am deeply grateful for your unwavering support and companionship throughout every step of my journey.

I want to take a moment to appreciate and thank myself for the courage, resilience, and constant effort I've shown throughout this journey.
I look forward to carrying the lessons learned and memories shared into the next chapter of my life. Thank you all from the bottom of my heart.
ADEL CHAIMA

Dedication 2

At the outset, I must express my boundless gratitude to the Divine for His benevolent support and for facilitating my path through all endeavors that appeared daunting. Additionally, I bestow my deepest thanks and acknowledgment to my esteemed self, which has stood invincible and steadfast, notwithstanding the array of trials and impediments faced.

The vigor, stability, and determination of I harbor are ascribed to the relentless support of my loyal companion, who has been present for every venture and setback, from the genesis to the present. I am profoundly grateful for their consistent encouragement and infinite motivation. I offer them all my love and sincere gratitude, for without their enduring presence and charming inspiration, I would not have reached this juncture.

Finally, I render my sincere appreciation to my mother and father, who have unfailingly offered their support and have been my constant allies. I am indebted to them for all the sacrifices they've made for my well-being. 'This triumph is rightfully theirs; I am just a means '. My thankfulness to them knows no bounds.

Nasri Hadil

Abstract:

   The Internet of Things (IoT) represents a transformative force, enabling everyday objects to become "smart" by facilitating communication between them. By connecting countless devices to the Internet, IoT allows for the exchange of vast amounts of data through sensors, aiding in data delivery, analysis, and the creation of optimal solutions. IoT applications are increasingly adopted across diverse domains and systems.

   However, this rapid expansion introduces new challenges, such as the accelerated energy depletion due to increased data traffic within the network. To combat this issue, several protocols have been developed. One of the most significant is the RPL protocol, now the standard for routing in low-power and lossy networks (LLNs). Despite its widespread use, RPL is vulnerable to various attacks on its control messages, presenting a major security challenge for future IoT systems.

   This research focuses on proposing DIO suppression attacks in IoT networks. By implementing our proposal, we aimed to achieve a lower Packet Delivery Ratio (PDR), higher Average End-to-End Delay (AE2ED), and higher Average Power Consumption. The proposed algorithm was implemented and tested using the Cooja simulator.

Keywords: IoT, RPL, LLNs, DIO suppression attack, PDR, AE2ED

ملخص:

يمثل إنترنت الأشياء (IoT) قوة تحويلية، حيث يمكن الأشياء اليومية من أن تصبح "ذكية" من خلال تسهيل الاتصال بينها. من خلال توصيل عدد لا يحصى من الأجهزة بالإنترنت ، يسمح إنترنت الأشياء بتبادل كميات هائلة من البيانات من خلال أجهزة الاستشعار ، والمساعدة في تسليم البيانات وتحليلها وإنشاء الحلول المثلى. يتم اعتماد تطبيقات إنترنت الأشياء بشكل متزايد عبر مجالات وأنظمة متنوعة.

ومع ذلك ، فإن هذا التوسع السريع يقدم تحديات جديدة ، مثل استنزاف الطاقة المتسارع بسبب زيادة حركة البيانات داخل الشبكة. لمكافحة هذه المشكلة ، تم تطوير العديد من البروتوكولات. واحدة من أهمها هو بروتوكول RPL ، ، الذي أصبح المعيار الفعلي للتوجيه في الشبكات منخفضة الطاقة وفاقدة الحزم (LLNs). على الرغم من انتشاره الواسع ، فإن RPL عرضة لعدة هجمات تستهدف رسائل التحكم الخاصة به، مما يشكل تحدياً أمنياً كبيراً لأنظمة إنترنت الأشياء المستقبلية.

يتركز هذا البحث على اقتراح هجمات قمع DIO في شبكات الإنترنت من الأشياء. من خلال تنفيذ اقتراحنا، نهدف إلى تحقيق معدل تسليم الحزم(PDR) أقل، وتأخير متوسط بداية-إلى-نهاية أعلى(AE2ED)، واستهلاك طاقة متوسط أعلى. تم تنفيذ الخوارزمية المقترحة واختبارها باستخدام محاكيCooja

الكلمات المفتاحية: IoT, RPL, LLN, DIO suppression attack, PDR, AE2ED

Résumé :

   L'Internet des objets (IoT) représente une force transformatrice, permettant aux objets du quotidien de devenir "intelligents" en facilitant la communication entre eux. En connectant d'innombrables appareils à Internet, l'IoT permet l'échange de vastes quantités de données via des capteurs, aidant à la livraison, l'analyse des données et à la création de solutions optimales. Les applications de l'IoT sont de plus en plus adoptées dans divers domaines et systèmes.

   Cependant, cette expansion rapide introduit de nouveaux défis, tels que l'épuisement accéléré de l'énergie dû à l'augmentation du trafic de données au sein du réseau. Pour lutter contre ce problème, plusieurs protocoles ont été développés. L'un des plus significatifs est le protocole RPL, devenu la norme de facto pour le routage dans les réseaux à faible puissance et à perte (LLNs). Malgré son utilisation répandue, le RPL est vulnérable à diverses attaques ciblant ses messages de contrôle, posant un défi majeur pour la sécurité des systèmes IoT futurs.

   Cette recherche se concentre sur la proposition d'attaques de suppression DIO dans les réseaux IoT. En mettant en œuvre notre proposition, nous visons à obtenir un taux de livraison de paquets plus faible, un délai moyen de bout en bout (AE2ED) plus élevé, et une consommation moyenne de puissance plus élevée. L'algorithme proposé a été implémenté et testé à l'aide du simulateur Cooja.

Mots-clés : IoT, RPL, LLN, DIO suppression attack, PDR, AE2ED

LIST OF FIGURES:

LIST OF TABLES:

Sommaire

List of Acronyms:

6LoWPAN: IPv6 over Low-Power Wireless Personal Area Networks.

AE2ED: Average End-to-End Delay.

APC: Average Power Consumption

CoAP: Constrained Application Protocol.

DAO: Destination Advertisement Object.

DAO-ACK: Destination Advertisement Object Acknowledgment.

DDNS: Dynamic Domain Name System.

DIO: DODAG Information Object.

DIS: DODAG Information Solicitation**.**

DODAG: Destination-Oriented Directed Acyclic Graph.

EXI: Efficient XML Interchange.

HTTP/HTTPS: HyperText Transfer Protocol / HyperText Transfer Protocol Secure.

IEEE: Institute of Electrical and Electronics Engineers.

IoT: Internet of Things.

IPv4:   Internet Protocol version 4.

IPv6:   Internet Protocol version 6.

LLNs: Low-Power and Lossy Networks.

LTE: Long Term Evolution.

OWL: Web Ontology Language.

PDR: Packet Delivery Ratio.

RDF: Resource Description Framework.

RFID: Radio Frequency Identification.

RPL: Routing Protocol for Low-Power and Lossy Networks.

WMNs: Wireless Mesh Networks.

WSNs: Wireless Sensor Networks.

GENERAL INTRODUCTION

The Internet of Things (IoT) utilizes internet connectivity to enhance functionality and intelligence, transforming interactions between objects and technologies. It includes various tangible entities with integrated sensors, linking them to enable communication and information exchange using multiple protocols, with each entity assigned a unique Internet Protocol (IP) address.

The Internet of Things (IoT) refers to the connectivity of various elements in our environment, such as smart cities, cell phones, and automobiles, to the Internet. IoT significantly enhances several industries by offering applications in smart cities, buildings, networks, and healthcare, thereby improving daily living and optimizing global resource allocation. However, the development of IoT is challenged by the need for reliable communication protocols to ensure successful network operations.

In IoT, information is routed through networks using protocols that ensure reliable data delivery. To address this, various routing protocols have been proposed for Wireless Sensor Networks (WSNs), The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) is essential for 6LoWPANs, but it is vulnerable to attacks that can significantly degrade performance in terms of Packet Delivery Ratio (PDR), Average End-to-End Delay (AE2ED), and Average Power Consumption, challenging the reliability and efficiency of RPL-based networks.

A DIO suppression attack disrupts RPL networks by replaying intercepted DIO messages, exploiting the Trickle algorithm's suppression mechanism. This leads to suppressed DIO messages, undetected nodes, degraded network path quality, and potential network fragmentation.

The primary objective of this project is to develop a new method that incorporates an attack within the network. By implementing our proposal, we aim to achieve a lower Packet Delivery Ratio (PDR), higher Average End-to-End Delay (AE2ED), and higher Average Power Consumption.

This thesis is organized into three chapters:

➢ The first chapter is devoted to introducing the Internet of Things (IoT), covering fundamental concepts, elements, common types of IoT networks, and IoT technologies.
➢ The second chapter introduces the security mechanisms of IoT and the RPL (IPv6 Routing Protocol for Low Power and Lossy Networks) communication protocol, which is widely used in the IoT domain. It also discusses various attacks based on the RPL protocol.
➢ The final chapter describes the experimental framework used to evaluate the proposed method and presents the evaluation results obtained using the Cooja simulator.

Chapter 1:
Overview of the Internet of Things

I.1 Chapter 1: Overview of The Internet of Things

I.2 Introduction:

Since Kevin Ashton first used the term "Internet of Things" in a 1999 Procter & Gamble presentation **[1]**, it has gained a lot of popularity and attention due to recent technological advancements.

The concept of the Internet of Things aims to make objects around us smart by enabling them to communicate with each other or the cloud through sensors, processing and operation, and the expansion of the Internet **[2].**

This chapter gives a general overview of the fundamental ideas behind the Internet of Things, with a focus on its definition and architecture, which includes its technologies, protocols, and applications.

I.3 Definition:

An advancement in the Internet progression is the Internet of Things, a network of actual physical objects that can interact and share data with other systems and objects. It acts as a foundation for communication between humans and machine **[3], [4]**.

Everything can now effortlessly connect to a place, time, thing, or person through any network or service thanks to the Internet of Things **[5].**
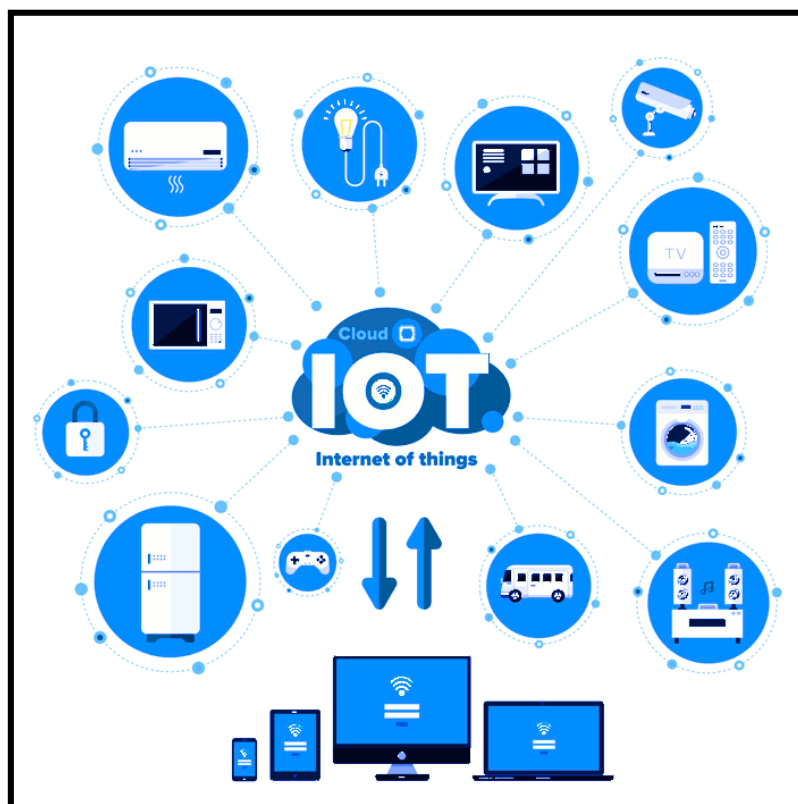
[6]

FIGURE 1 : INTERNET OF THINGS (IOT)

I.4   The architecture of the Internet of Things (IoT):

There is not just one widely recognized IoT architecture.
Over the past few decades, numerous proposals for Internet of Things architecture have been proposed.
The main IoT design suggests three and five-layered systems **[7].**
A three-layered architecture consists of the perception layer, network layer, and application layer. The processing and business layers are added to a three-layered architecture to create a five-layered architecture.
Ning and Wang used layers of the human brain processing system to design the Internet of Things architecture.
The modified manlike neural network (MLN), which gives people the ability to perceive, smell, think, investigate, remember, feel, make decisions, and react to their physical surroundings, served as their inspiration.
Ning and Wang **[7].[8]** claim that because both the Internet of Things and human brain processing are examples of complexity, sentient systems with the capacity for taste, feel, sight, control, and even decision-making, they are remarkably similar to each other. One way to think of the human brain is like a processing unit or data center.
A more concise way to think of the spinal cord is as smart gateways, or as a distributed network of data processing nodes. IoT sensors, actuators, and networking components can be thought of as akin to a network of nerves **[10] [11].**

The four most crucial layers, which are as follows, will now be presented:

I.4.1   Perception layer:

Similar to how people's eyes, hearing, and nose work, the sensor layer—also referred to as the perception layer—performs these functions. The primary function of the sensor layer is object recognition and data collection.
Numerous varieties of sensors are available for mounting on objects in order to gather data. The sensors must be chosen by the application.
These sensors are capable of recording movement, vibration, temperature, humidity, and other information **[12].**

I.4.2   Network layer:

IoT devices use the network layer to connect to clouds or each other.
To link devices, the network layer requires several communication protocols, including DDNS, MQTT 3.1/3.1.1, HTTP/HTTPS, IPv4, IPv6, CoAP, and others.
Information is safely transmitted from the perception layer to the middleware layer (processing layer) of the information processing system via the network layer **[13].**

I.4.3   Processing layer:

This layer, also known as the middleware layer, is responsible for processing, storing, and analyzing massive amounts of data.
This layer can calculate and process information autonomously, in addition to offering various services to the bottom layers.

Numerous technologies are used in the processing layer, such as big data processing and cloud computing **[14].**

I.4.4   Application layer:

Every application that makes use of or has deployed IoT technology is defined at the application layer.
IoT applications include tracking animals, smart cities, smart homes, and smart health. It is accountable for delivering the services to the apps. Because services rely on the data that is gathered by sensors, they could differ for each application **[15].**

Application layer
Smart grid , Smart healthcare , Smart building , Smart transport

Processing Layer
Cloud Computing , Database

Network Layer
ZigBee , WIFI , Blutetooth , 3G

Perception Layer
RFID , Sensor , Camera , Actuator
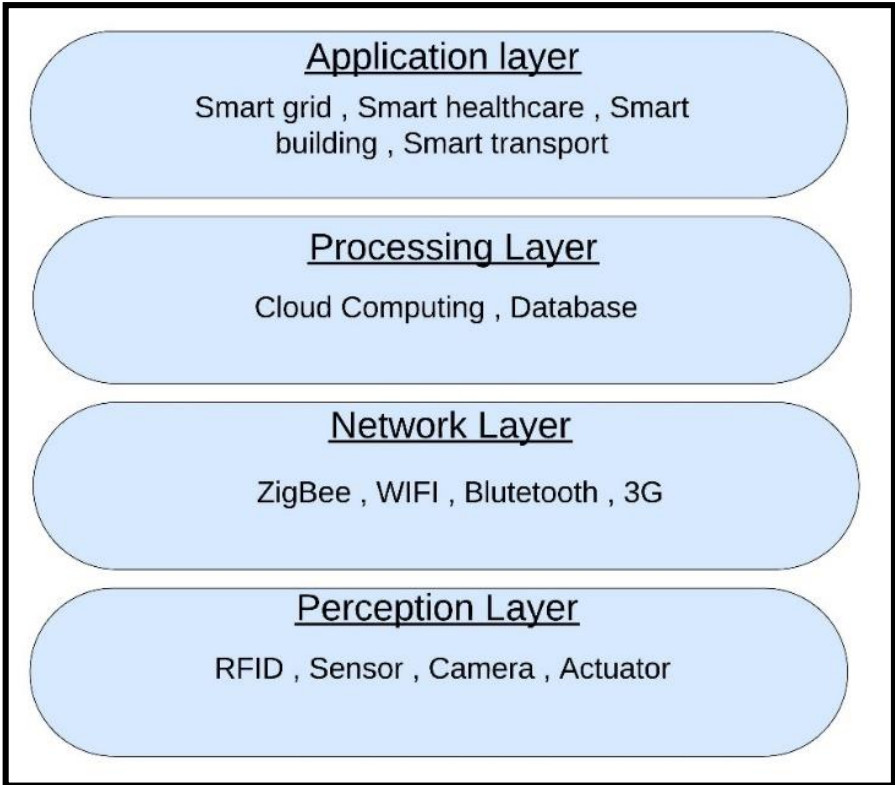
FIGURE 2: INTERNET OF THINGS (IOT) ARCHITECTURE FOUR LAYERS

I.5   IoT Protocols:

In our modern world, there are many interconnected devices via the Internet of Things. To facilitate communication among these devices, we need a common language and set of guidelines.

we can ensure that devices work together optimally, leading to fewer programming requirements, less power consumption, reduced memory usage, and efficient data transmission.

I.5.1   Network Layer:

RPL and 6LowPAN are the two most significant protocols in this layer. IPv6 is utilized by 6LowPAN, a low-power wireless personal area network. Mesh routing needs both the destination and intermediate addresses.

However, routing over low power, or RPL, requires incredibly little power. RPL's primary focus is routing, in contrast to 6LowPAN, and it is intended to collect sensor data **[16].**

A. 6LoWPAN :

The IPv6 Low-Power Wireless Personal Area Network is specially made to make it possible for IPv6 packets to be transmitted via low-power wireless networks, which are frequently used in Wireless Sensor Networks (WSNs) and the Internet of Things (IoT)**[17].** The 6LoWPAN stack has six layers: Physical Layer, Data Link Layer, Adaptation Layer, Network Layer, Transport Layer, and Application Layer**[18].**

B. IPv6:

which is the next generation of Internet communication protocols, is a development of IPv4. IPv6 mitigates IPv4 is impending address scarcity by virtue of its vastly larger address space than IPv4.

In addition, IPv6 allows for more sophisticated features and functionalities to meet the increasing needs of contemporary Internet-connected devices while also improving network security **[19].**

C. RPL:

The RPL (Routing Protocol for Low-Power and Lossy Networks) protocol is a customized routing system that has been carefully designed to accommodate the peculiar needs of low-power and lossy networks, which are common in Wireless Sensor Networks (WSNs) and the Internet of Things (IoT).

RPL tackles the issues of low power, memory, and bandwidth by primarily providing effective routing operations in resource-constrained contexts, guaranteeing strong connectivity and communication dependability.

RPL is essential to smooth data transmission and network operation in IoT and WSN installations because it optimizes routing choices and adjusts to sporadic network connectivity**[20].**

I.6 Elements of the Internet of Things:

Elements of the Internet of Things are as follows:

a) **Hardware**:
  - It consists of sensors, actuators, and embedded communication hardware.

b) **Middleware:**
  - Storage and computing tools for data analytics are available on demand.

c) **Presentation:**
  - Includes innovative, simple visualization and interpretation tools.
  - Accessible across multiple platforms and intended for a variety of applications.**[21]**

I.6.1 Identification

Identification in the context of IoT refers to the process of identifying and distinguishing particular devices or objects within a network. This component is critical for effective communication, data management, and control in IoT systems. To identify devices and enable smooth interaction, a variety of identification mechanisms are used, such as unique identifiers, tags, and addresses. These identification mechanisms ensure that data created by IoT devices is appropriately credited, recorded, and managed across the whole network.

Identification also makes it easier to implement security features like access control, authentication, and encryption to safeguard data integrity and privacy. Overall, robust identification techniques are critical for ensuring the reliability and security of IoT networks.**[22]**

I.6.2 Communication:

This element plays a very significant task in IoT, allowing for cloud access. It acts as a conduit for machine-sensed data to be transferred to cloud-based services for further processing. This seamless information transfer enables real-time monitoring, analysis, and decision-making, allowing IoT applications to respond efficiently to changing situations. Effective communication protocols and technologies provide consistent data sharing between IoT devices and cloud platforms, allowing for more efficient resource use and supporting IoT deployment scalability. In essence, communication serves as the foundation of IoT systems, allowing them to leverage the power of cloud computing for more functionality and intelligence.**[23]**

I.6.3 Devices/sensors

The Internet of Things (IoT) relies heavily on devices and sensors to enable data gathering and transmission in a variety of contexts. They feature a variety of sensors that collect real-time data, such as temperature, humidity, motion, and light. Actuators interact with their surroundings using sensor data, and inbuilt communication technology enables these devices to connect and communicate via networks. Modern sensors are meant to be low-power and efficient, with wireless communication capabilities. These devices form the IoT's hardware backbone, allowing for data monitoring, analysis, and response. This enables smart applications in healthcare, agriculture, and urban planning.**[21], [24].**

I.6.4 Cloud-based capture and consolidation.

Cloud-based capture and consolidation are the systematic collecting, storage, and processing of data from various Internet of Things (IoT) devices and sensors using cloud computing resources. This approach has various benefits, including scalability to support big data volumes and extensive storage capacities to manage massive amounts of created data. The cloud architecture provides tremendous computational capacity, allowing for complicated data analysis and real-time processing. Furthermore, it provides data accessibility from any place, allowing for efficient remote monitoring and administration of IoT devices.**[25]**

The integration of several data sources into a single platform improves comprehensive insights and informed decision-making. Furthermore, cloud services are cost-effective since they eliminate the need for large physical infrastructure. They provide strong security features including data encryption and secure access controls, which protect data integrity and privacy. The cloud also offers real-time analytics, allowing for immediate interpretation and action based on collected data. Finally, automated backup and recovery methods built into cloud storage provide data security and reliability, reducing the chance of data loss.**[26]**

I.6.5 Services

IoT applications provide a variety of services divided into four major categories.**[27]** First and foremost, identity-related services are critical in determining the identities of objects starting network requests. Second, information aggregation services help to collect data from a variety of sources while also carrying out processing duties. Third, collaborative services use aggregated data to make informed decisions and then send appropriate answers to related devices. Finally, ubiquitous services exemplify dynamic responsiveness, free of temporal or physical limits, permitting rapid interactions with devices as required by real-time exigencies.**[15]**

I.6.6 Semantics

It is the role of IoT to help users by carrying out their tasks. It is the most significant component of IoT for carrying out its tasks. It serves as the brain of the Internet of Things. It receives all information and makes appropriate decisions before sending responses to the devices **[28].**

TABLE 1: THE ELEMENTS AND KEY TECHNOLOGIES OF IOT.

IoT elements	Technologies
Identification	Electronic, Prodect Code, Ucode Ipv4, and Ipv6
Sensing	Smart, Sensors, RFID tags, Wearable Sensing Devices and Actuators
Communication	Radio Frequency Identification, wireless Sensor Network, Near Field Communication (NFC), Bluetooth, Long Term Evolution (LTE)
Computation Hardware Software	Audrino,Raspberry Pi,Intel Galil Operating System
Services	Identity-Related, Information Aggregation, Collaborative-Aware and Ubiquitous
Semantics	RDF, OWL, EXI

I.7 Common Types of IoT Networks:

There are various sorts of IoT networks, each with its own set of requirements and limits. The three most prevalent forms of IoT networks are Low-Power and Lossy Networks (LLNs), Wireless Sensor Networks (WSNs), and Wireless Mesh Networks (WMNs).

I.7.1 Low-Power and Lossy Networks (LLNs):

Low-Power and Lossy Networks are specialized networks designed to meet the unique requirements of limited devices and harsh environmental conditions seen in the Internet of Things (IoT) ecosystem. These networks of interconnected nodes function under harsh restrictions such as restricted power availability, processing capacity, and unreliable communication connectivity. LLNs use protocols such as IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) or IEEE 802.15.4 to permit wireless communication among devices. LLNs have tight power management measures to extend battery life, tolerance for lossy communication links that are prone to packet loss and delays, and adherence to resource-efficient protocols designed for devices with limited computational capabilities and memory.**[29]**

Dynamic network topologies, driven by factors like as device mobility and intermittent connectivity, need adaptive protocols like the Routing Protocol for Low-Power and Lossy Networks (RPL). Standardization groups, such as the Internet Engineering Task Force (IETF), have created protocols such as RPL and CoAP to solve the unique issues of LLNs while allowing for efficient communication, routing, and management capabilities.**[30]**

9

I.7.2 **Wireless sensor networks (WSN)**

Wireless Sensor Networks (WSNs) are made up of distributed sensor nodes that monitor and report environmental variables like temperature, humidity, and motion. These nodes communicate wirelessly and frequently use multi-hop communication to send data to a central base station. Because sensor nodes are typically powered by batteries, energy efficiency is critical in WSNs; techniques such as duty cycling and efficient routing protocols aid in energy conservation. Routing protocols in wireless sensor networks can be flat, hierarchical, or location-based, each with advantages and disadvantages.**[31]**

Security is also a key worry because of the possibility of attacks such as eavesdropping or denial of service. A DIO suppression attack, for example, can interrupt communication in RPL-based networks by preventing key routing messages from being sent. Monitoring tools and performance routines can assist in detecting and mitigating such attacks, maintaining the network's stability and lifespan. Understanding these concepts is critical for creating strong and efficient WSNs for a variety of applications, including environmental monitoring and industrial automation.**[32]**

I.7.3 **Wireless Mesh Networks (WMNs)**

Wireless Mesh Networks are a versatile and scalable solution to wireless communication in which nodes relay data collectively to increase network coverage and dependability. Unlike traditional wireless networks, WMNs are decentralized, allowing each node to operate as a router, dynamically constructing and optimizing communication routes. Because of their self-configuring nature, WMNs can adapt to changing network circumstances and topologies, making them ideal for dynamic environments like cities or disaster recovery scenarios **[33].**WMNs provide resilience against node failures and interference by utilizing several hops between nodes, ensuring ongoing communication even in adverse circumstances.

Furthermore, because of their versatility and scalability, WMNs may serve a wide range of applications, including wireless internet access, surveillance systems, and smart grid infrastructure. As wireless technology advances, WMNs will play an increasingly important role in extending connection and enabling creative applications in a wide range of sectors **[34].**

I.8   Applications of the Internet of Things:

The Internet of Things has many application domains:
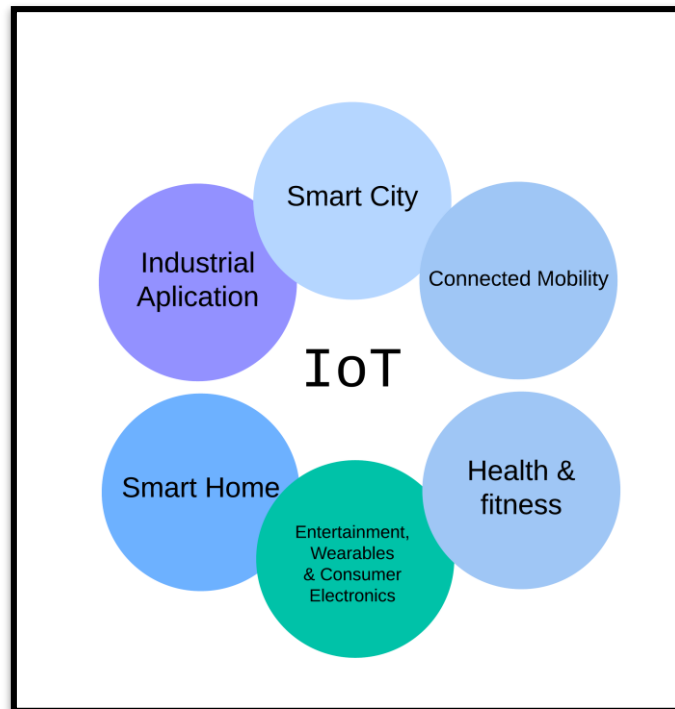
FIGURE 3 : APPLICATIONS OF INTERNET OF
THINGS

The applications and use of IoT in the different domains are what drive and explain the development of this new trend, leading to the acceptance of IoT by the new world[35]**.** The study of IoT applications improves the understanding and enhancement of IoT technology, and thus, the design of new systems for newly developed cases[36]**.**
The concept of IoT can be summarized as generating daily information from an object and transferring it to another one. Therefore, enabling communication between objects makes the range of IoT applications extensive, variable, and unlimited.

We can find many applications of the Internet of Things in almost all fields. The Internet of Things is an Intelligent network of different smart devices that can be identified, positioned, tracked, monitored, and managed remotely.
A few applications of the Internet of Things are as follows, Smart parking systems, Electro Magnetic level detection systems, Structural Health monitoring systems, Urban noise maps, Smartphone Detection, Traffic congestion, and Smart lighting systems. Waste Management system, Smart roads[37]

I.8.1   Smart Cities:

IoT technologies are used to optimize urban infrastructure and services, such as waste management, public safety, energy and transportation systems, and environmental monitoring, improving the quality of life for locals and promoting sustainability**.[38]**

I.8.2   **Smart Home:**

The automation and control of HVAC, lighting, security, and appliance systems in homes are made possible by IoT devices, which improve comfort, convenience, and energy efficiency.**[39]**

I.8.3   **Healthcare**:

IoT gadgets that provide real-time health monitoring, tailored therapies, and better patient care delivery include wearable fitness trackers, medical sensors, and remote patient monitoring systems.**[40]**

I.8.4   **Vehicles:**

Vehicles that are connected to the internet allow users to get data about the car's maintenance and even pay tolls electronically**[41].**

I.8.5   **Fitness Trackers:**

Most commonly utilized in healthcare and sports. Users can use these gadgets to monitor their blood pressure, heart rate, and other physical activity parameters.

I.9   IoT Technologies

The Internet of Things was initially inspired by members of the RFID community, who referred to the possibility of discovering information about a tagged object by browsing an internet address or database entry that corresponds to a particular RFID or Near Field Communication technology**[37].**

In the research paper "Research and application on the smart home based on component technologies and Internet of Things", the included key technologies of IoT are RFID, sensor technology, nanotechnology, and intelligence embedded technology.

Among them, RFID is the foundation and networking core of the construction of the Internet of Things**[38].**

I.9.1   **Radiofrequency identification (RFID):**

RFID systems comprise one or more readers and several RFID tags. It uses radiofrequency electromagnetic fields to send data attached to it**[42].**RFID technology is being used in various applications such as supply chain management, access control, identity authentication, and object tracking.

The RFID tag is attached to the object to be tracked and the reader detects and records its presence when the object passes by it. In this manner, object movement can be tracked and RFID can serve as a search engine for smart things **[43].**

I.9.2   **Bluetooth**

Bluetooth is a widespread wireless communication technology based on the IEEE 802.15.1 standard. It is suitable for low-power and low-cost devices and it is operating at the 2.4 GHz

band. Bluetooth can support star topology Personal Area Networks (PAN), with lower power consumption, low setup time, and with unlimited number of nodes**[44]** The BLE protocol stack is similar to the stack used in classic Bluetooth technology**[43].**

I.9.3   WIFI

Wi-Fi. Wireless fidelity (Wi-Fi) is a wireless local area network (WLAN) that adheres to the IEEE 802.11 standard. Compared to Bluetooth, it has a longer communication range (within 70 feet). Wi-Fi creates a network quickly and effortlessly. As a result, hospitals are the primary settings for its application. Wi-Fi's widespread use stems from its ease of connectivity with cellphones, as well as its ability to enable strong security and control. However, it consumes substantially more power, and the network functions inconsistently.**[45]**
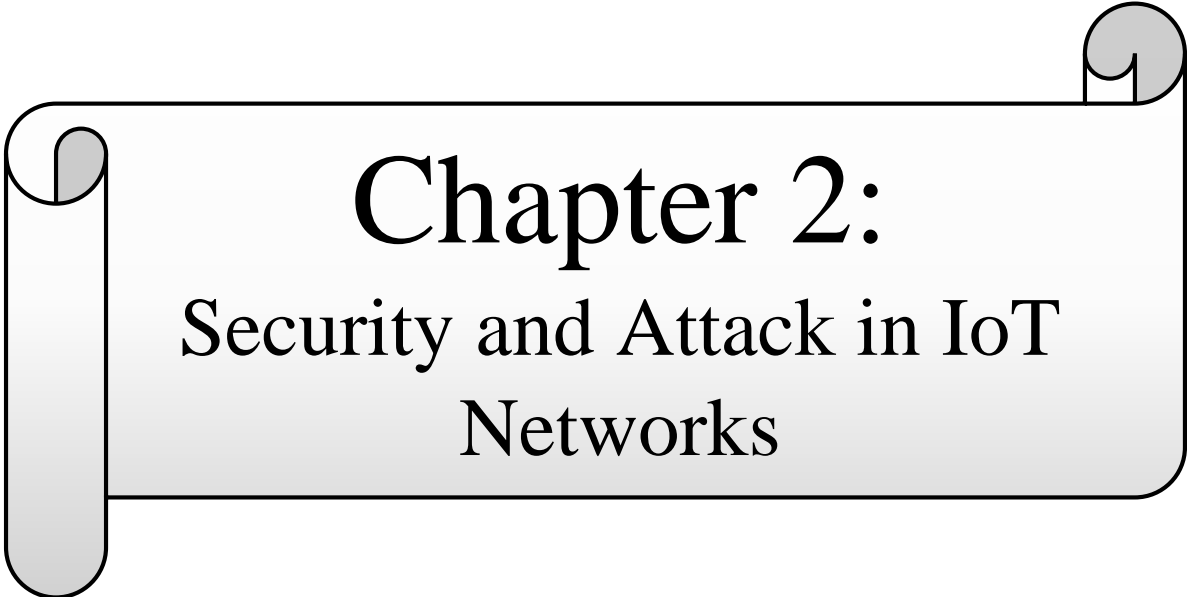
I.9.4   ZigBee

ZigBee technology, based on the IEEE 802.15.4 standard, facilitates low-speed, short-distance communication, drawing inspiration from bee colonies' communication methods. In agricultural settings, ZigBee networks emulate colonies, with nodes serving as data-collecting agents akin to bees gathering honey. These networks offer reliable transmission, low power consumption, and support various topologies such as star, tree, and mesh. Several studies have demonstrated ZigBee's utility in automated irrigation systems, water quality monitoring, and smart agriculture applications.

However, limitations include short communication distances and susceptibility to interference, which may restrict its use in large farmland or areas with complex environmental conditions. Despite these challenges, ZigBee technology enables real-time data transmission and remote system management, contributing to enhanced efficiency and resource conservation in agricultural operations.**[46]**

I.10 Conclusion:

Chapter 1 provides an extensive overview of the Internet of Things (IoT), covering its fundamental definition, architectural layers, essential protocols for network functionality, critical elements, and various types of IoT networks. It serves as a comprehensive introduction to the subject, offering insights into its complexities and practical applications. In the next chapter, we will discuss the security of the Internet of Things and present its most important security vulnerabilities and the attacks that it may face.

Chapter 2:
Security and Attack in IoT Networks

II Chapter 2: Security and Attack in IoT Network

II.1 Introduction:

The convergence of several devices connected by the digital fabric creates a double-edged sword in the rapidly developing Internet of Things scenario.
Although the Internet of Things (IoT) paradigm enhances the functionalities of networked devices by enabling smooth data transfer and task automation, it also increases the attack surface for possible cyber threats. Thus, the security of IoT systems becomes a critical issue that demands close examination and strong protective measures **[47] [48]**.
This chapter provides security mechanisms. And also presents the most important security vulnerabilities, attacks that you may face, and security mechanisms.

II.2 Security mechanism of IoT:

IoT deployment risks are reduced by security procedures, which also protect the availability, confidentiality, and integrity of IoT systems and data and communication channels against malevolent invasions, illegal access, and breaches of sensitive data, security methods are essential **[49].**
And these are some of the IoT security mechanisms:

II.2.1 Authentication Protocol:

These cryptographic protocols are intended to verify the identity of devices connected to the Internet of Things, guaranteeing that only authorized parties are able to connect to and use the system**[50].**

A. T2S-MAKEP Protocol :
As the object and the server are the only ones aware of the secret key obtained during the setup phase and saved on the trustworthy server, mutual authentication is achieved.
In order to protect itself against attacks, the server only keeps one pair of CRPs.
Our protocol's most important feature is that it prevents physical attacks by not storing any private or public information on the device**[51].**

II.2.2 Encryption Algorithms:

play a crucial part in IT by guaranteeing data integrity and confidentiality.
The choice of encryption technique is crucial in the context of the Internet of Things since devices frequently have limited computational capabilities **[52].**
An overview of IoT security encryption methods is provided here:

A. Symmetric Encryption Algorithms :
These algorithms encrypt and decrypt data using the same key**[53].**

B. Asymmetric Encryption Algorithms :
These require two keys: a private key for decryption and a public key for encryption.
Because it can offer robust security with reduced key sizes, Elliptical Curve Cryptography (ECC) is preferred in the Internet of Things (IoT) for devices with limited resources**[54]**

C. **Lightweight Cryptography:**

Lightweight cryptography has been created in response to the drawbacks of conventional encryption methods on Internet of Things devices.

For its lightweight cryptography standard, the National Institute of Standards and Technology (NIST) has chosen a set of cryptographic algorithms known as Ascon. Because Ascon is made to be as efficient as possible in terms of size, speed, and energy consumption, it may be used on small devices with low processing power[55].

II.2.3 **Intrusion Detection System (IDS):**

IDS are used to keep an eye on network traffic for any unusual activity that might point to a security breach.
This allows for the quick identification and mitigation of possible threats[56].

II.2.4 **Public Key Infrastructure (PKI):**

Public-key infrastructure, or PKI, is a framework for public-key cryptography and digital certificates that makes encrypted communications and secure device authentication possible[57].

II.2.5 **Blockchain:**

Blockchain technology is being leveraged in the IoT to bolster security through several key functions:

A. **Decentralization:**

IoT networks are more resistant to assaults and system failures thanks to the blockchain decentralized structure, which removes single points of failure[58].

B. **Immutability:**

Data integrity and permanence are ensured by the fact that once it is recorded on the blockchain, it cannot be changed without network consensus[59].

C. **Transparency and Auditability:**

Because every transaction on the blockchain is public and auditable, data and transactions within the IoT ecosystem can be tracked and verified[60].

D. **Smart Contracts:**

The terms are hardcoded into the contract, making it self-executing.
Through the Internet of Things, they may streamline workflows, implement security guidelines, and enable automated transactions between machines without the need for human involvement[58].

E. Enhanced Security:

Blockchain offers an IoT device security framework that prevents data manipulation and illegal access by utilizing cryptographic algorithms**[61].**

F. Trust and Accountability:

Blockchain provides a tamper-resistant ledger for documenting transactions, which is essential for accountability and dispute resolution, enabling confidence amongst parties in an IoT network**[60].**

G. Data Privacy:

By using blockchain technology, users may better control who can access their data and enhance their privacy by encrypting and anonymizing Internet of Things data**[59].**

II.3 Security vulnerabilities in IoT:

Significant vulnerabilities exist in IoT systems' software, hardware, networks, and chips. Adversaries can gain control through software weaknesses, including weak authentication and vulnerable firmware. Man-in-the-middle attacks on sensors and Advanced Metering. Infrastructure (AMI) are two examples of hardware vulnerabilities that can result in data theft and grid disruption.

Inadequate security measures cause network vulnerabilities, as demonstrated by breaches in devices such as Amazon's Ring owing to unencrypted protocols. Chip vulnerabilities include Hardware Trojans (HTs) and side-channel attacks, which allow adversaries to obtain cryptographic keys and sensitive data, posing serious security risks**.[62]**

Here are some common vulnerabilities:

A. **Password-Based Authentication**: Many IoT devices use default or weak passwords, making them vulnerable to brute-force attacks**[63].**

B. **Inadequate Firmware Updates:** The absence of robust firmware update procedures in IoT systems exacerbates security vulnerabilities, leaving devices susceptible to exploitation and undermining the integrity of the entire network **[64].**

C. **Privacy Concerns:** Sensitive data is collected and processed by IoT devices, giving rise to privacy issues with data collecting, storage, and sharing procedures. Insufficient safeguards against data loss could leave private or sensitive data vulnerable to illegal access or disclosure**[65].**

D. **Network Reconnaissance:** To obtain strategic intelligence, attackers make use of their comprehension of the network topology. They can locate vital infrastructure components, identify possible targets, and create complex attack methods by examining the network configuration. With this knowledge, they may optimize the impact of their activities and successfully exploit weaknesses**[66].**

II.4 RPL Protocol :

In order to arrange nodes into a hierarchical structure with a single root, children, and additional descendants, RPL creates loop-free topologies known as Destination Oriented Directed Acyclic Graphs (DODAG).

RPL uses objective functions to optimize the topology by predetermined objectives, such as energy consumption, hop count, or link quality. A network can contain several RPL instances, each with its DODAGs and an execution of RPL with a particular objective function.

A node may be a part of more than one instance, but it can only ever join one DODAG within an instance **[67].**

The following control messages are used to construct and manage an RPL DODAG:

II.4.1 DODAG Information Solicitation (DIS):

Upon first powering on, nodes throughout the network send out DIS control messages as their first multicast ICMP message. Nodes utilize these messages to ask for pertinent parameters that allow them to join an already-existing DODAG or start a new one.

The fact that DIS messages are still transmitted to keep the network running even after DODAG was created is significant **[68].**

II.4.2 DODAG Information Object (DIO):

In response to the DIS messages, the sink is the first to broadcast the DIO control message, which is followed by other nodes in the sensor network, and in the multicast mode, it provides a DODAG path for DIO messages to create a new DODAG so that any node can use the network information in the DIO message to find an RPL instance, identify a set of parents, understand the configuration, and finally create a DODAG **[67].**

II.4.3 Destination Advertisement Object (DAO):

Nodes confirm receipt of DIO messages sent by the Sink and other nodes that may have updated DIOs by sending a unicast DAO Control Message to the Sink and other nodes.
In the DODAG network, DAO is used to create and maintain the upward path connecting nodes to the Sink **[68].**

There are two available modes of operation:

• The non-storing mode: all routing data can only be stored on the root node**[69].**
• The storing mode: the routing data must be stored on all parent nodes in the topology **[70].**

II.4.4 Destination Advertisement Object with Acknowledgment (DAO-ACK):

an indicate of the DAO message is successful reception that is sent by the parent node to the child nodes. In order to uphold and modify a specific topology **[71]**
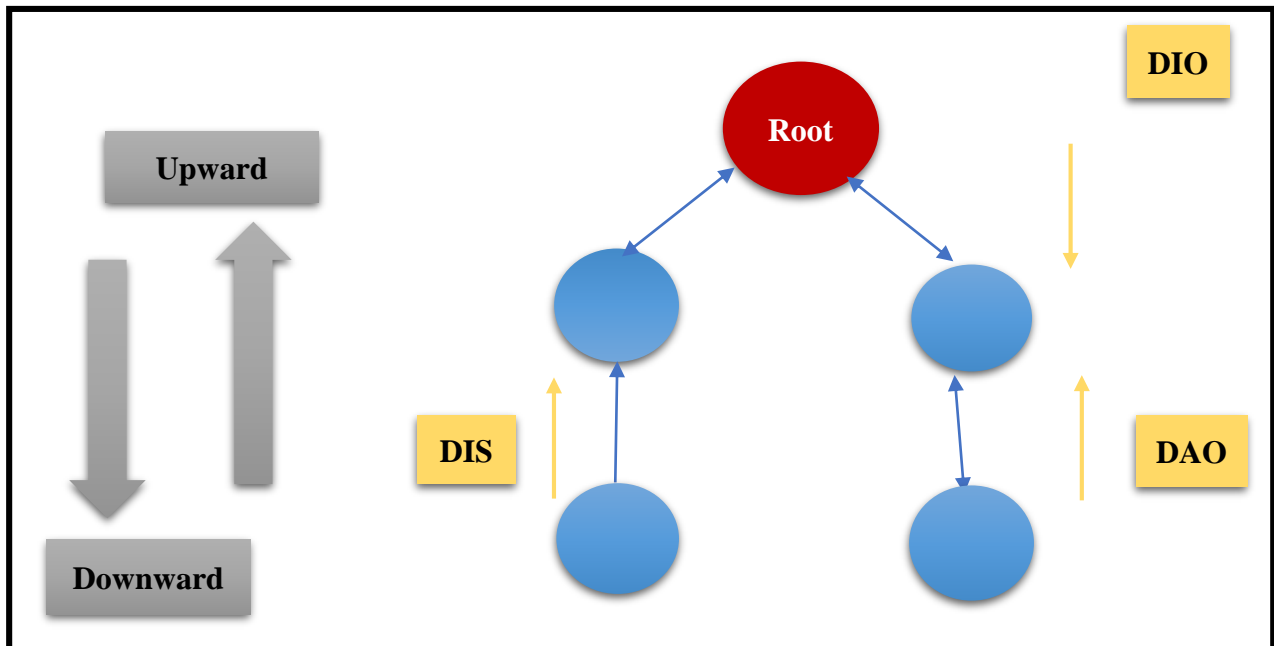
FIGURE 4: RPL CONTROL MESSAGES

II.5 Trickle timer:

The Trickle algorithm controls the emission of DIOs. Trickle was first created for polite gossiping in wireless networks. It minimizes redundant messages and dynamically adjusts the transmission rate to lower the nodes' power consumption. Specifically, the stability of routing information is used to adjust the emission rate of DIOs. The emission rate is decreased if the data in the DIOs from the neighbors matches the internal routing information. Otherwise, the emission rate is raised in the event that inconsistent DIOs are received. RPL outlines the requirements for figuring out whether audio is consistent.
A DIO must be deemed consistent, for instance, if it has no effect on the parent set, the preferred parent, or the distance to the root **[72].**

The Trickle algorithm splits time in periods of variable length. In the second half of each period, the node plans to transmit a DIO message at a random time t. The node monitors the consistent DIOs and listens for messages till *t*. Only if the number of consistent DIOs received during the current period is less than a specified suppression threshold (*k*) will the scheduled DIO message be broadcast at time *t*. If not, the DIO's transmission is muted, as seen in the example of Figure 5 during the fourth phase. By the end of the time frame, if only reliable
The current period is interrupted and the algorithm restarts at a period of minimum length Imin if an inconsistent DIO is received at any point. The Trickle algorithm relies heavily on the DIO suppression mechanism, which causes DIO traffic to scale logarithmically with the number of nodes. It is not advised to disable this technique since it may cause congestion in networks with a lot of use **[72].**
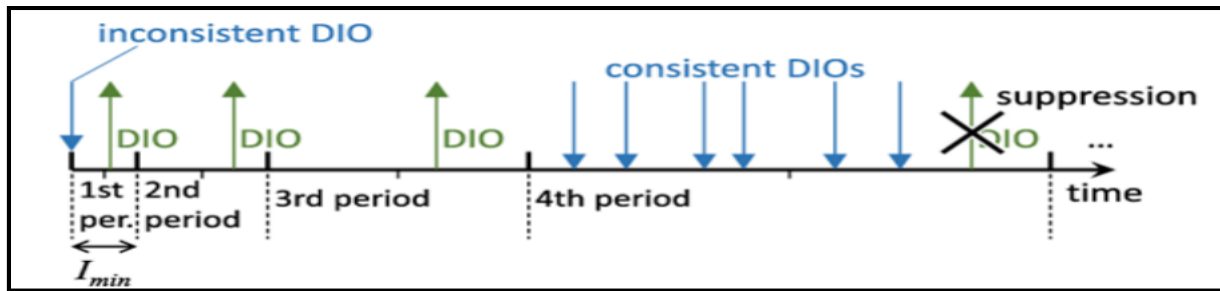
FIGURE 5: EXAMPLE OF TRICKLE ALGORITHM WITH K = 6

[72]

II.6 Attacks Based in RPL Protocol:

The Internet of things is susceptible to numerous security flaw-focused attacks, which can take many different forms and include the following:
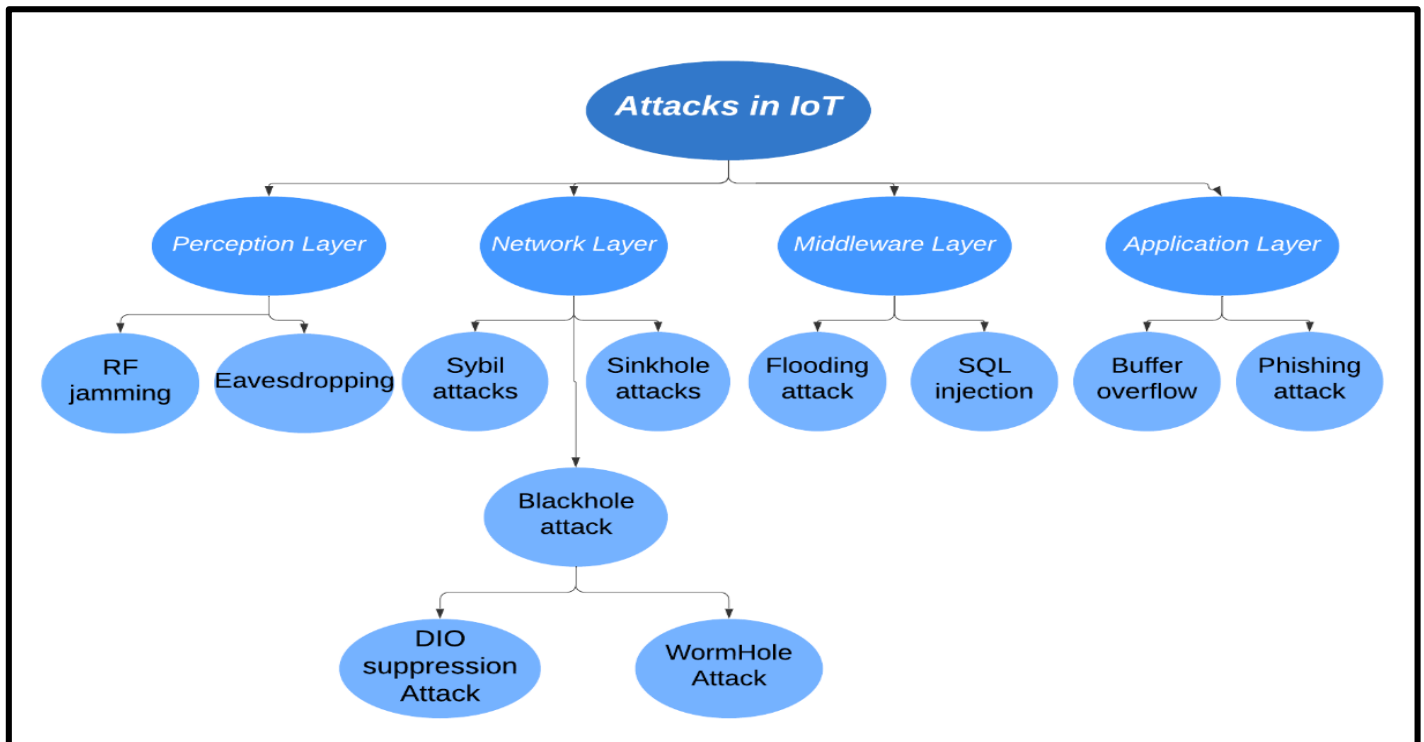
FIGURE 6: ATTACKS BASED ON RPL PROTOCOL

II.6.1 DIO suppression Attack:

Disrupting or slowing down the network's DIO message transmission is the aim of the DIO suppression attack. Trickles DIO suppression approach is employed for this purpose.
A persistent DIO message that the recipient nodes interpret as consistent is sent by the adversary during this attack.

20

Assume that there are enough consistent DIOs for the nodes. Then, they stop transmitting data across their own DIO, which lowers the overall quality of the routes or, in the worst situation, causes a network failure **[73].**

II.6.2 RF jamming Attack:

The purpose of this attack is to interfere with the tags and readers' ability to communicate by sending RF waves to the network.
Attackers may use radio frequency jamming (RF jamming) to stop readers from communicating with all tags by disrupting all signals within their range**[74].**

II.6.3   Wormhole Attack:

An assault known as a Wormhole occurs when two or more attackers work together to create a virtual tunnel that allows traffic to transit through it either completely or partially instead of via the original path. Thus, an assault of this kind throws off the topology of the network, depletes its resources, and gives the attackers access to private data **[75].**

II.6.4 Blackhole attack:

This type of attack directs network traffic to a particular node that is not even there in the network. As a result, packets are dropped, which causes a large loss of data. WSNs are then equipped with a Security Aware Routing (SAR) protocol to thwart the blackhole attack **[76].**

II.6.5 Replay Attack:

Attackers may utilize the answers of tags to fictitious reader challenges in this kind of assault. Replay attacks cause the tag is accessibility to be falsified by recording, storing, and replaying the signal that was sent between the tag and the reader at a later date to the receiving device **[77].**

II.6.6 Eavesdropping:

Anytime along a communication channel—wireline or wireless—an adversary can listen in and steal data. IoT edge devices must utilize lightweight encryption techniques to prevent data eavesdropping.
By producing noise and warping the data while it is being transmitted, adversaries can also cause disruption and launch denial-of-service attacks **[78].**

II.6.7 Sinkhole Attack:

The attacker advertises itself as the shortest path to the sink node (e.g., gateway or base station). Legitimate nodes, unaware of the deception, route their traffic through the sinkhole. The malicious node then drops or modifies the received packets, disrupting communications **[79].**

II.6.8 Sybil attack:

Pseudonymous identities are created by the attacker to give the impression that there are multiple separate nodes when, in fact, they are all part of the same malevolent entity **[80].**

II.6.9 Routing Information Attack:

With this attack, the attacker can send, alter, or fake routing information to add complexity to the network.
As a result, the network may get divided, incorrect data may be forwarded, or packets may be allowed or dropped **[81].**

II.6.10 Man in the Middle Attack:

An MITM attack could occur on an RFID system while data is being sent between the tags and the reader.
In this scenario, the communication route between the RFID system is component parts could be intercepted and altered by an attacker. Since it displays and modifies the information before the legitimate entity receives it, this kind of attack is regarded as real-time **[77].**

II.6.11 DDOS attack:

There are weaknesses in the IoT infrastructure. An adversary obtains access to the node and/or gateways by capturing the credentials. Gateways in their local databases typically store information about things (IoT). An enemy can use this intelligence to compromise the other devices.
Lastly, it can initiate a denial-of-service attack by delivering bogus packets and interfering with IoT network connections **[69].**

II.7 Countermeasures of attacks:

This section discusses countermeasures for the attacks mentioned above.

TABLE 2:COUNTERMEASURES OF IOT ATTACKS

Layers	Attacks	Countermeasures
Perception	- RF jamming - Eavesdropping	- Hashed-based encryption - Device authentication - Secure booting - RF Shielding
Network	- Sybil Attack - Sinkhole Attack - Blackhole Attack - DIO suppression Attack - Wormhole Attack	- Secure Routing - Ad hoc routing - Data privacy
Processing	- Flooding Attack - SQL Injection	- Web application scanners - Fragmentation redundancy scattering (FRS) - Hyper Safe
Application	- Buffer overflow - Phishing Attack	- Access Control Lists (ACLs) - Intrusion Detection - Firewalls

A. Hashed-based encryption:

With the help of hash-based encryption security, communication can be encrypted and transformed into cipher text, an anonymous form.
When a message is transmitted, it is transformed using a key that only authorized users can decipher when it is sent from the sender.
Based on the message length, a key is generated.
Its key is usually twice as long as the message.
As a result, breaking a key is a difficult task.
Additionally, the receiver receives the key.
By utilizing the key, the recipient can change the cipher text into the original message**[82].**

B. Device authentication:

Before sending or receiving data, a new physical device connecting to the Internet of Things needs to verify itself.
Once the device has been correctly detected, the system ensures that hostile devices are never allowed to enter the network**[83].**

C. Secure Booting:

The software's originality and authenticity can be verified through the use of a cryptographic hash technique.
Using a digital signature, this technique validates the software installed on the devices.
Too few devices have the computing power to implement a large number of cryptographic hash methods.
Certain cryptographic hash algorithms **[84],** such as the NH and WH algorithms are appropriate for devices with minimal power consumption.

D. RF Shielding:

employ physical barriers or shielding materials to prevent eavesdropping on wireless signals **[85].**

II.7.1 IoT Network Layer Security:

A. secure routing:

Secure routing is crucial for the sensor network in many applications.
Several routing algorithms are used in IoT systems to guarantee the secrecy of data being. Transferred to multiple sensor nodes as a result of insecure routing protocols.
Multiple pathways, on the other hand, offer secure routing that corrects network problems and boosts system performance.
Source routing is a technique used for routing purposes in which data that is transmitted is kept in packets and then processed after analysis.
Where it can prevent attacks such as sinkholes and wormholes **[86].**

B. Security aware ad hoc routing:

The security-aware ad hoc routing (SAR) protocol guards against insider assaults on the Internet of Things network.
Following the examination of the received data, the adversary is removed from the network and certain security measures are appended to the packets**[87].**

C. Data privacy:

Safety control procedures are designed to prevent errors of any kind in the network.
As a result, data integrity has been implemented to ensure that the data that users receive is identical to what was originally encrypted, for example.
To prevent unauthorized access to data on sensor nodes, authentication mechanisms are used[88].

II.7.2 IoT Processing Layer Security:

A. Web application scanners:

This program is used to identify various dangers that exist on the website's front end.
Additional web firewall programs are also monitoring any attacker attacks[89].

B. Fragmentation redundancy scattering (FRS):

The crucial data for FRS is divided and distributed among different server storage components.
Since the fragment contains no valuable information about the data, there is little chance of data theft in this case[90].

C. Hyper Safe:

Hyper-safe prevents memory pages from being changed and permits pointing index restrictions that transfer tracked data to pointer indexes[83].

II.7.3 IoT Application Layer Security:

A. Access Control Lists (ACLs):

Establishing rules and permissions for who can access and manage the Internet of Things (IoT) system is essential for protecting both the system's security and the privacy of the data.
ACLs have the ability to grant or deny access to requests made by various users within or outside of the network, as well as to block or allow incoming or outgoing traffic[91].

B. Firewalls:

This additional layer of protection will assist in thwarting attacks that authentication, encryption, and ACLs would not be able to stop.
Passwords used for encryption and authentication can be compromised if they are weak. A firewall has the ability to filter packets as they come in, stopping DOS attacks, unwanted packets, and obnoxious login attempts before the authentication process even starts[92].
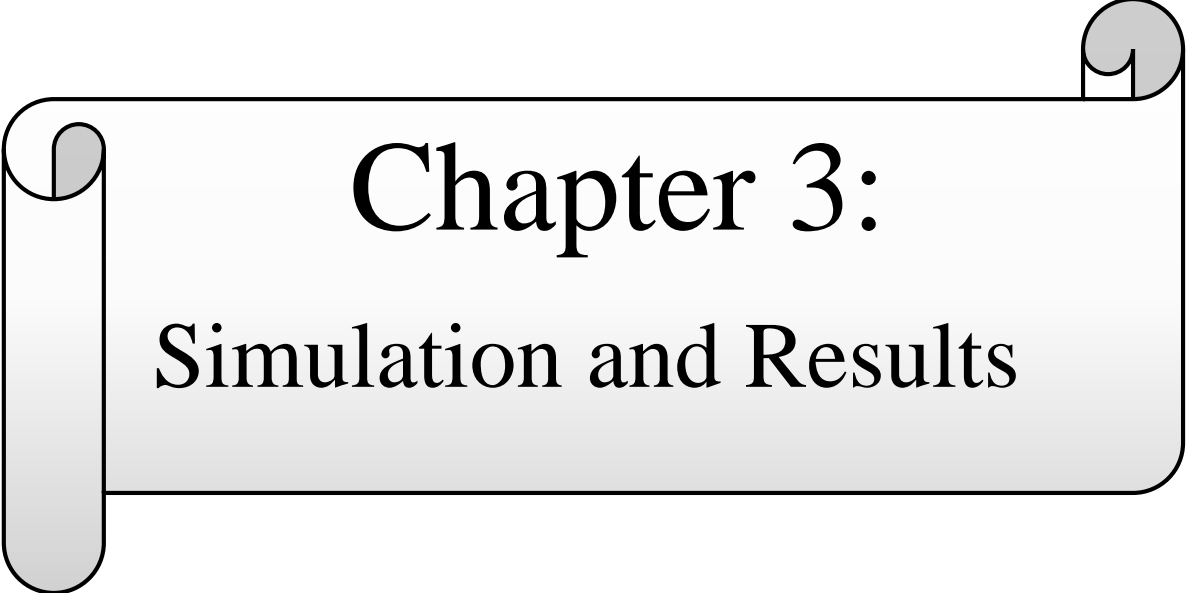
C. Intrusion Detection:

Because the intrusion detection method continuously monitors a log of the intruder's activities, it offers security solutions to several dangers by raising an alarm whenever an unauthorized action is carried out in the system.
Numerous detection methods, including anomaly detection in data mining, can be used to detect intrusions[93].

II.8 Conclusion:

This chapter is dedicated to the security of the IoT network, where we talked about the security vulnerabilities that permeate it, its mechanisms, and the attacks carried out by attackers in the IoT network, with mentioning countermeasures for attack and also talked a little about RPL protocol and his control messages and also about Trickle Timer.

In the next chapter, we will study the DIO suppression attack in a new method, where we will simulate it and compare the results obtained from this simulation .

Chapter 3:

Simulation and Results

III **Chapter 3: Simulation and Results**

III.1 Introduction:

Due to the vulnerabilities in the security framework of the Internet of Things (IoT), it is susceptible to numerous attacks that can disrupt the network. One of the most serious attacks is the DIO suppression attack, which aims to disrupt and slow down the transmission of DIO messages. This can lead to a decrease in the overall quality of the network paths and, in the worst case, result in the fragmentation of the entire network.

In this chapter, we will conduct simulations without and with the DIO suppression attack, and then compare the outcomes.

III.2 Implementation:

This part contains the steps we took to prepare the platform used for this simulation

III.2.1 Contiki OS:

Contiki is a lightweight IoT operating system specifically aimed at small IoT devices with limited memory, power, bandwidth, and processing power, developed at the Swedish Institute of Computer Science by Adam Dunkels and written in the C programming language. The Contiki operating system requires 30 kb (random access memory).

Contiki is an Ubuntu Linux virtual machine that can run on Windows or Linux pre-installed with a Vmware Pro running a Linux Virtual Machine.

Contiki is distinguished by his work on the concept that lies Between Multi-threading and event-driven programming, which leads to the exchange of the same execution context, and this improves the use of memory and energy, and this is the so-called Protothreads.

Contiki supports IPv6 and IPv4 stack implementations and less advanced wireless standards such as 6LoWPAN, and RPL.

III.2.2 Cooja Simulator:

Cooja is the network simulator for Contiki OS, allowing developers to test wireless sensor network applications and IoT simulations. It's a Java-based tool that can simulate networks from the physical layer to the application layer, including hardware emulation of sensor nodes.

As shown in Figure 6, the Cooja simulation interface consists of five windows and is as follows:

27

- ➢ The network window.
- ➢ You can check and see the status of every network node in this area (ID, address, position, etc.) This area is vacant when the simulation starts and nodes must be added.
- ➢ The simulation control window:

  To launch, resume, or go to the simulation, utilize this section. Not only is the speed given there, but we also get the execution time.
- ➢ The notes window:

  You can take notes about the current simulation in this area.
- ➢ The motes output window:

  This is the area where the output from the various node interfaces is shown, allowing us to observe all communication between network nodes and the messages they exchange.
- ➢ The timeline window:

  It displays the radio communications (transmission, reception, collision) and the sensor nodes' states of wakefulness and sleep over time.
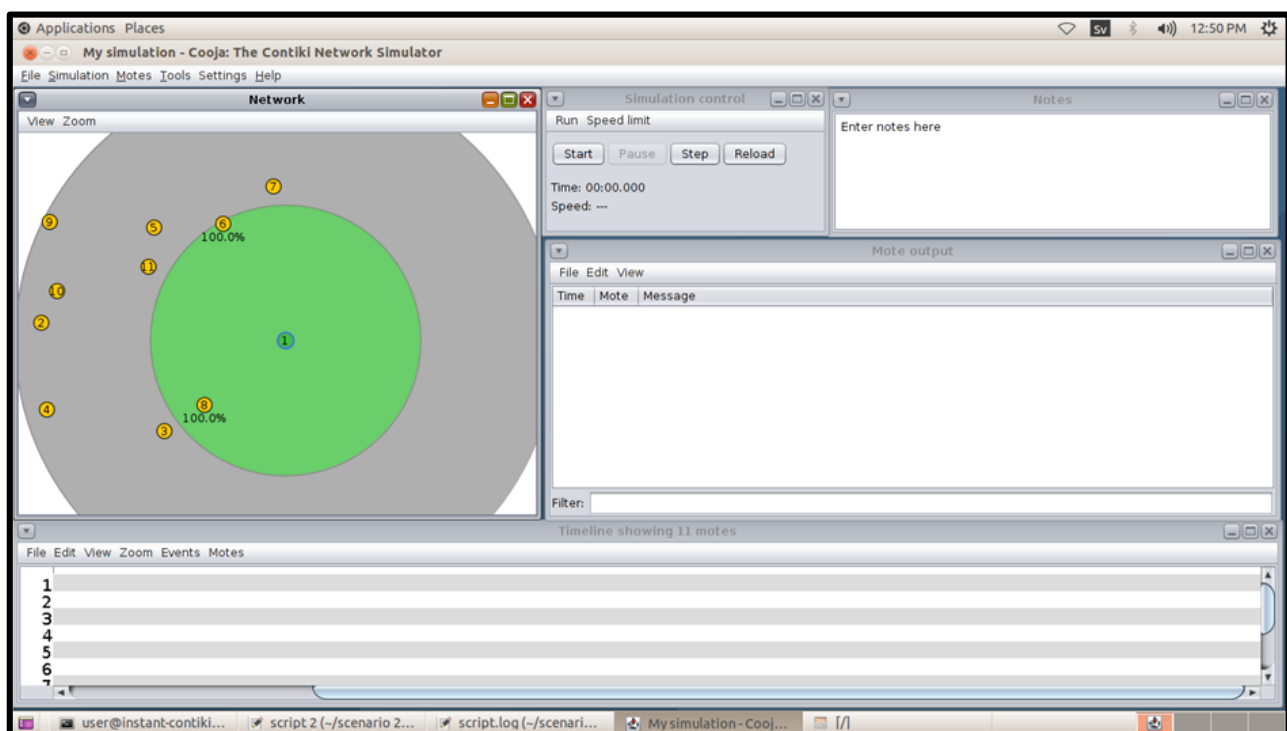
FIGURE 6: COOJA SIMULATOR INTERFACE

III.2.3 Installing Contiki 3.0 on VMware:

1. We downloaded and installed the VMware software on our computer.
2. We downloaded the latest Contiki version 3.0 VM image from the Contiki website. A VM image is a pre-configured virtual machine with Contiki-3.0 already installed.
3. We imported the Contiki-3.0 VM image into VMware. To do this, we opened VMware, went to File > Open, and selected the Contiki-3.0 VM image file.
4. This created a new virtual machine in VMware with Contiki 3.0 pre-installed.
5. We started the Contiki-3.0 VM in VMware. We selected the Contiki-3.0 VM in the VMware interface and clicked the "Start" button. This started the virtual machine and launched Contiki-3.0.
6. Finally, Contiki-3.0 is launched.
7. After Contiki started working, we started activating Cooja, where we first downloaded a file called mspsim to our computer and copied it into Contiki and exactly in tools.
8. Then we went to the terminal to run Cooja and wrote the following

➢ Cd contiki-3.0/tools/cooja

➢ Ant run_bigmem

Cooja was turned on.

III.2.4 The simulation environment:

In this section, table 3 shows the simulation parameters that were taken into account in the experiments in order to simulate three scenarios without a DIO suppression attack where the duration of the simulation is 15 minutes.

TABLE 3: EVALUATION PARAMETERS

Parameter	Scenario 1	Scenario 2	Scenario 3
Number of nodes	1 server, 15 clients, 1 Attack	1 server, 20 clients, 1 Attack	1 server, 25 clients, 1 Attack
Deployment area	100 × 100 m	100 × 100 m	100 × 100 m
Simulation runtime	15 minutes	15 minutes	15 minutes

III.3 Results of simulation with and without attack:

We have created a new method of DIO suppression attack that occurs in the network and not outside it, where the attacker sends inconsistent DIO messages and the number of their packets is determined by a trickle algorithm and exactly at redundancies k, since in redundancies k we determine how many times the DIO messages are repeated

We conducted three scenarios over a 15-minute period, with each scenario incorporating both a case employing the new method we devised for the Duo suppression attack and a case without it. These experiments produced the following results, which will be discussed in detail:

III.3.1 Packet Delivery Ratio:

In the first results, we discuss the Packet Delivery Ratio:

It is the ratio of all the data packets delivered by the sensor nodes, including those that were retransmitted, to all the data packets received by the gateway node within the specific time interval T.

$$PDR = \frac{Number\ of\ packets\ received}{Total\ number\ of\ packets\ sent}$$

In the PDR result shown above, in the absence of a DIO suppression attack, we observe that the PDR percentage is relatively constant and high, ranging between **95%** and **99%**. This percentage is considered normal. However, this changes significantly during a DIO suppression attack, as it gradually decreases, with percentage ranging between **55%** and **86%**. This is because the attack directly impacts the network topology. In RPL, nodes use DIO messages to construct and maintain the DODAG. When an attacker suppresses the transmission of DIO

messages, it leads to the dissemination of incomplete or inaccurate routing information throughout the network, causing not all packets to reach their destination .
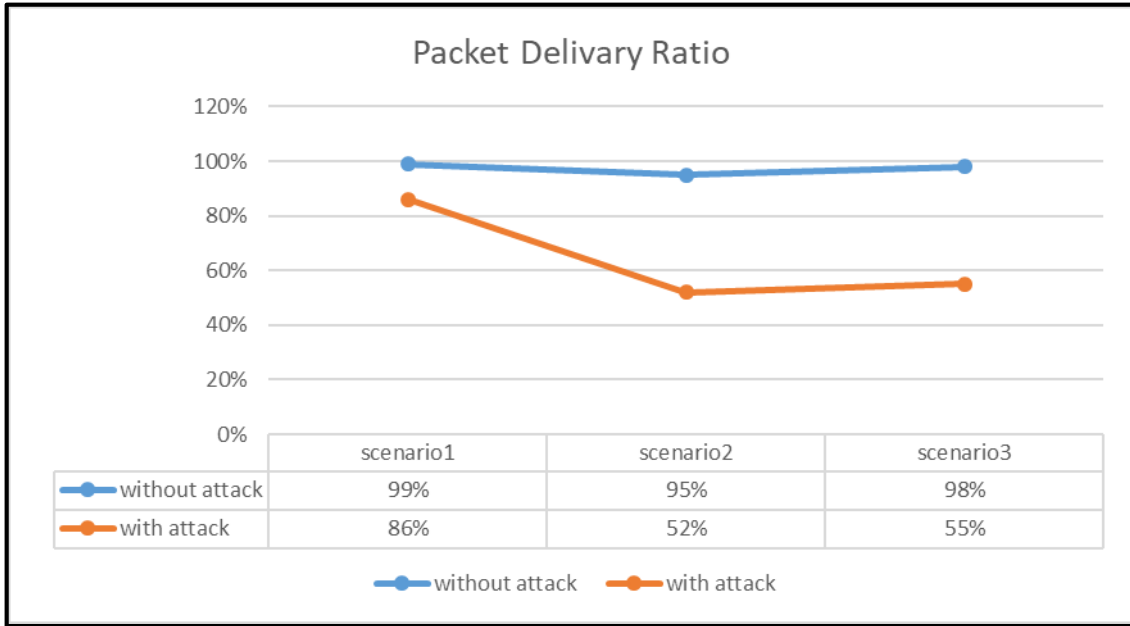
FIGURE 7: RESULT OF PACKET DELIVERY RATIO

III.3.2 Average End-to-End Delay:

In the second result, we discuss the Average End-to-End Delay:

AE2ED is the average time it takes for all data packets sent from each sensor node to reach the gateway node.

$$AE2ED = \sum_{i=1}^{n} \frac{Treceived,i - Tsent,i}{n}$$

- $T_{received}$, i = time when the packet is received.
- T_{sent}, i = time when the packet is sent.
- n = is the total number of packets considered in the calculation .

The graphical curve for AE2ED indicates that in normal conditions without any attack, its values range from **0.22** to **0.37**. However, in the event of a DIO suppression attack, the values of AE2ED increase significantly, ranging between **0.76** and **0.97**. This change is attributed to the attack preventing the transmission of DIO messages, causing the affected nodes to lack the necessary updates to maintain routing tables. Consequently, they possess incomplete or

31

outdated routing information, resulting in inefficient routing paths and longer delays in packet delivery.
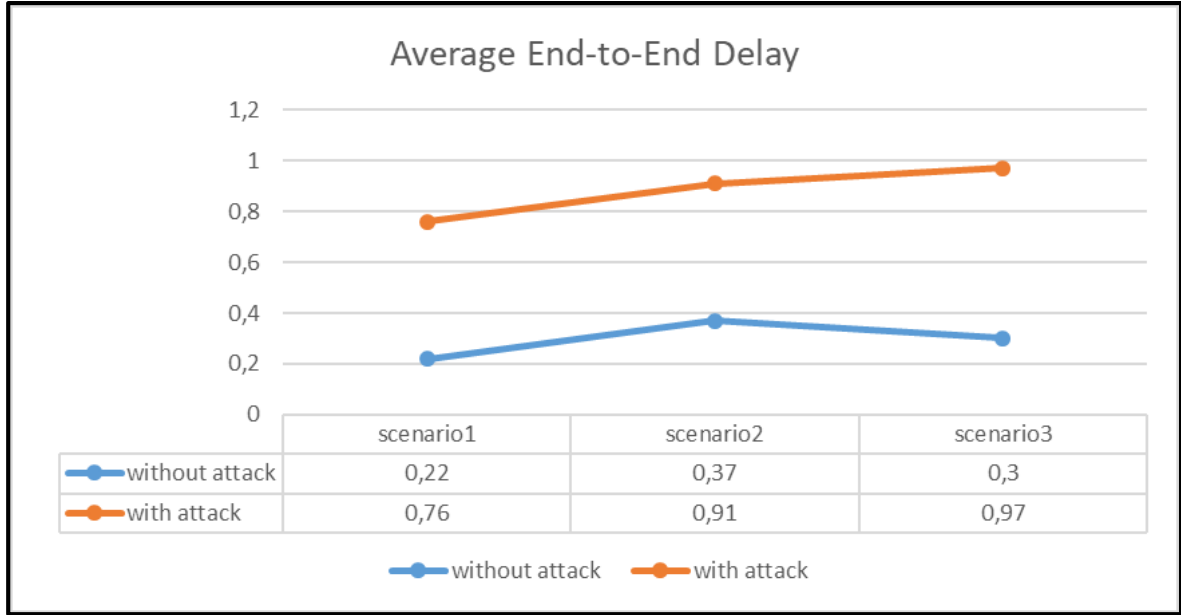
FIGURE 7: RESULT OF AVERAGE END-TO-END DELAY

III.3.3 Power Consumption:

In the third result, we discuss the Power Consumption:

This measure evaluates how much power each network node uses overall when it is in use.

$$APC = \sum_{i=1}^{n} \frac{(Etransmit, i \ + \ Ereceive, i \ + \ Eprocess, i \ + \ Eidle, i)}{n}$$

-   $E_{transmit}, i$ = the energy consumed by node i for transmission
-   $E_{receive}, i$ = the energy consumed by node i for receiving data
-   $E_{process}, i$ = the energy consumed by node i for processing data
-   E_{idle}, i = the energy consumed by node i while in idle state
-   n = total number of nodes in the network

In normal conditions, power consumption results for ON, TX, and RX components are relatively small and typical, ranging as follows: ON: **6.36-8.57**, TX: **1.07-1.49,** RX: **0.26-0.46**. However, during a DIO suppression attack, notable differences emerge. ON values range between **10.13-11.25**, TX between **3.09-3.99**, and RX between **0.74-0.89**. This discrepancy arises because the attack delays and causes retransmissions of DIO messages, leading to increased power consumption.

Power Consumption

	scenario1	scenario2	scenario3
ON without attack	8,75%	7,95%	6,36%
ON with attack	11,26%	11,80%	10,13%
TX without attack	1,07%	1,49%	1,08%
TX with attack	3,09%	3,99%	3,38%
RX without attack	0,26%	0,40%	0,46%
RX witht attack	0,74%	0,78%	0,89%
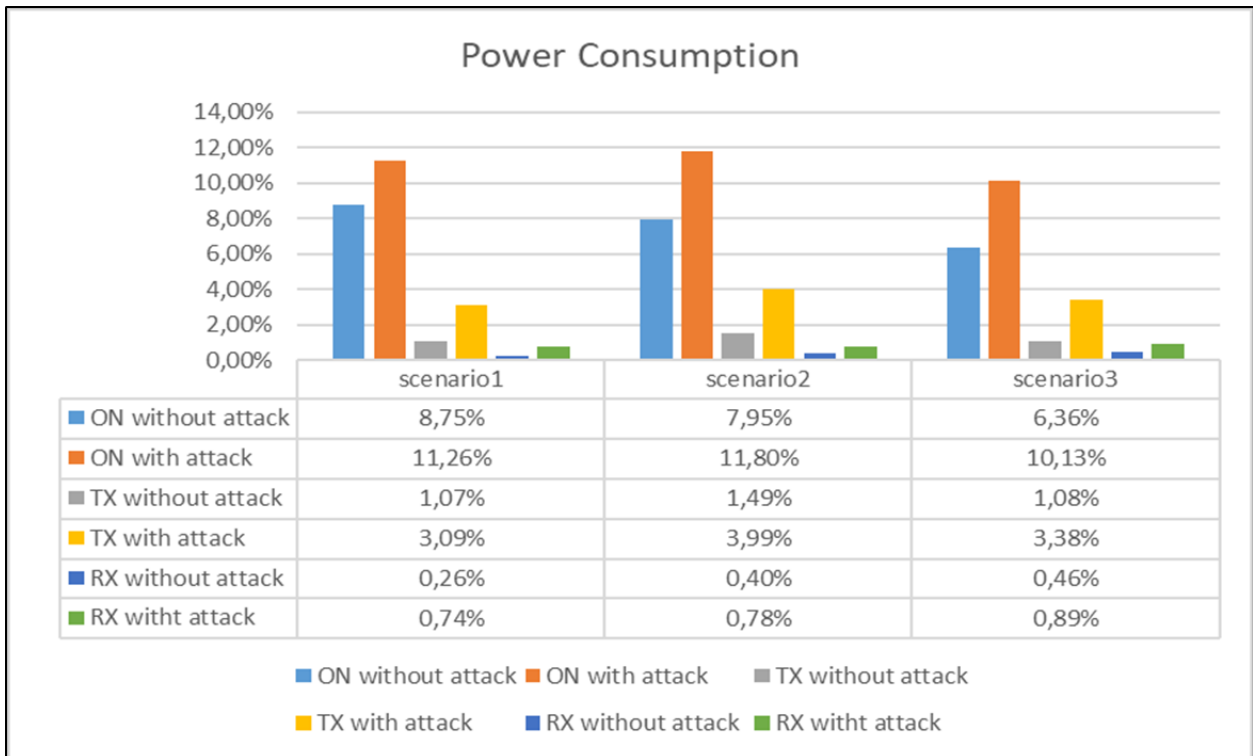
FIGURE 9: RESULT OF POWER CONSUMPTION

III.4 Conclusion

finally, we have successfully completed our project. Throughout our study, we extensively discussed our working environment, explained the structure of our proposed project, and provided a detailed overview of the stages we went through to obtain the simulation results of our topologies.

GENERAL CONCLUSION

The rapid advancement of the Internet of Things (IoT) is revolutionizing how we interact with the world around us, connecting billions of devices to create smarter, more efficient systems. This research has delved into the intricate layers of IoT, its architecture, and the crucial role of communication protocols in enabling seamless data exchange.

Our exploration revealed that while IoT offers unprecedented opportunities for innovation across various sectors, it also introduces significant security challenges. The vulnerabilities inherent in IoT networks, particularly within the RPL protocol, present substantial risks that can compromise the integrity and performance of these systems. Through our detailed examination of security mechanisms and the implementation of the DIO suppression attack, we highlighted the critical impact of such threats on network performance metrics like Packet Delivery Ratio (PDR), Average End-to-End Delay (AE2ED), and Average Power Consumption.

The simulation results underscore the necessity for robust security frameworks to protect IoT networks from malicious activities. This study emphasizes that addressing these vulnerabilities is not just about enhancing security protocols but also about ensuring the overall reliability and efficiency of IoT deployments.

 the findings of this research advocate for a proactive approach to IoT security. As the adoption of IoT continues to expand, so too must our efforts to fortify these networks against emerging threats. Future research should focus on developing innovative security solutions tailored to the dynamic nature of IoT environments. By doing so, we can safeguard the immense potential of IoT, enabling it to drive progress and improve quality of life across the globe.

Reference

[1]   T. UNLU, F. BASCIFTCI, and N. KARASEKRETER, "Wireless Sensor Networks Technology", Accessed: Mar. 13, 2024. [Online]. Available: https://www.isres.org/books/chapters/CSBET2021_3_03-01-2022.pdf

[2]   M. Lombardi, F. Pascale, and D. Santaniello, "Internet of Things: A General Overview between Architectures, Protocols and Applications," *Information*, vol. 12, no. 2, p. 87, Feb. 2021, doi: 10.3390/info12020087.

[3]   "What Is the Internet of Things (IoT)? With Examples," Coursera. Accessed: Mar. 14, 2024. [Online]. Available: https://www.coursera.org/articles/internet-of-things

[4]   G. Alqarawi, B. Alkhalifah, N. Alharbi, and S. El Khediri, "Internet-of-Things Security and Vulnerabilities: Case Study," *J. Appl. Secur. Res.*, vol. 18, no. 3, pp. 559–575, Jul. 2023, doi: 10.1080/19361610.2022.2031841.

[5]   K. S. Mohamed, "An Introduction to IoT," in *Bluetooth 5.0 Modem Design for IoT Devices*, Cham: Springer International Publishing, 2022, pp. 33–43. doi: 10.1007/978-3-030-88626-4_2.

[6]   admin, "The Internet of Things Training (IoT) Overview Course," Wireless Technologies Training. Accessed: Jun. 12, 2024. [Online]. Available: https://www.enowireless.com/training-tutorials-courses/internet-of-things-iot-training-overview/

[7]   E. Irmak and M. Bozdal, "Internet of Things (IoT): The Most Up-To-Date Challenges, Architectures, Emerging Trends and Potential Opportunities," *Int. J. Comput. Appl.*, vol. 179, no. 40, pp. 20–27, May 2018, doi: 10.5120/ijca2018916946.

[8]   "Dr. Ning Wang." Accessed: Mar. 23, 2024. [Online]. Available: https://www.dsi.uzh.ch/en/people/researchers/dsi-researchers/nwang.html

[9]   "Ning Wang | University of Zurich, Switzerland - Academia.edu." Accessed: Mar. 23, 2024. [Online]. Available: https://uzh.academia.edu/NingWang

[10]   H. Ning and Z. Wang, "Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework?".

[11]   H. Ning and S. Hu, "Technology classification, industry, and education for Future Internet of Things," *Int. J. Commun. Syst.*, vol. 25, no. 9, pp. 1230–1241, Sep. 2012, doi: 10.1002/dac.2373.

[12]   M. Yildirim, U. DemiRoğlu, and B. Şenol, "An in-depth exam of IoT, IoT Core Components, IoT Layers, and Attack Types," *Eur. J. Sci. Technol.*, Oct. 2021, doi: 10.31590/ejosat.1010023.

[13]   E. Irmak and M. Bozdal, "Internet of Things (IoT): The Most Up-To-Date Challenges, Architectures, Emerging Trends and Potential Opportunities," *Int. J. Comput. Appl.*, vol. 179, no. 40, pp. 20–27, May 2018, doi: 10.5120/ijca2018916946.

[14]   T. Aziz and E. Haq, "Security Challenges Facing IoT Layers and its Protective Measures," *Int. J. Comput. Appl.*, vol. 179, no. 27, pp. 31–35, Mar. 2018, doi: 10.5120/ijca2018916607.

[15]   M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey," *Sensors*, vol. 18, no. 9, Art. no. 9, Sep. 2018, doi: 10.3390/s18092796.

[16]   M. R. Islam and K. M. Aktheruzzaman, "An analysis of cybersecurity attacks against internet of things and security solutions," *J. Comput. Commun.*, vol. 8, no. 4, pp. 11–25, 2020.

[17]   F. K. Örs and A. Levi, "Data driven intrusion detection for 6LoWPAN based IoT systems," *Ad Hoc Netw.*, vol. 143, p. 103120, Apr. 2023, doi: 10.1016/j.adhoc.2023.103120.

[18]   "Survey on the authentication and key agreement of 6LoWPAN: Open issues and future direction - ScienceDirect." Accessed: May 23, 2024. [Online]. Available: https://www-sciencedirect-com.sndl1.arn.dz/science/article/pii/S1084804523001789

[19]   A. Zakari, M. Musa, G. Bekaroo, S. A. Bala, I. A. T. Hashem, and S. Hakak, "IPv4 and IPv6 Protocols: A Comparative Performance Study," in *2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC)*, Aug. 2019, pp. 1–4. doi: 10.1109/ICSGRC.2019.8837050.

[20]   L. Wallgren, S. Raza, and T. Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things," *Int. J. Distrib. Sens. Netw.*, vol. 9, no. 8, p. 794326, Aug. 2013, doi: 10.1155/2013/794326.

[21]   J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.

[22]   "Ubiquitous ID: Standards for Ubiquitous Computing and the Internet of Things | IEEE Journals & Magazine | IEEE Xplore." Accessed: May 28, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/5586696

[23]   T. K. Gannavaram V, U. M. Kandhikonda, R. Bejgam, S. B. Keshipeddi, and S. Sunkari, "A Brief Review on Internet of Things (IoT)," in *2021 International Conference on Computer Communication and Informatics (ICCCI)*, Jan. 2021, pp. 1–6. doi: 10.1109/ICCCI50826.2021.9451163.

[24]   A. Shivakrishna and K. M. Lakshman Rao, "v/c ratio based on road geometrical elements using IoT sensors based on artificial neural network modeling," *Meas. Sens.*, vol. 33, p. 101109, Jun. 2024, doi: 10.1016/j.measen.2024.101109.

[25]   "Enhancing water management in smart agriculture: A cloud and IoT-Based smart irrigation system," *Results Eng.*, vol. 22, p. 102283, Jun. 2024, doi: 10.1016/j.rineng.2024.102283.

[26]   A. F. da Silva, R. L. Ohta, M. N. dos Santos, and A. P. D. Binotto, "A Cloud-based Architecture for the Internet of Things targeting Industrial Devices Remote Monitoring and Control," *IFAC-Pap.*, vol. 49, no. 30, pp. 108–113, Jan. 2016, doi: 10.1016/j.ifacol.2016.11.137.

[27]   M. Gigli and S. Koo, "Internet of Things: Services and Applications Categorization Abstract," *Adv Internet Things*, vol. 1, pp. 27–31, Jan. 2011, doi: 10.4236/ait.2011.12004.

[28]   M. Elkhodr, S. Khan, and E. Gide, "A Novel Semantic IoT Middleware for Secure Data Management: Blockchain and AI-Driven Context Awareness," *Future Internet*, vol. 16, no. 1, Art. no. 1, Jan. 2024, doi: 10.3390/fi16010022.

[29]   K. Kritsis, G. Z. Papadopoulos, A. Gallais, P. Chatzimisios, and F. Théoleyre, "A Tutorial on Performance Evaluation and Validation Methodology for Low-Power and Lossy Networks," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 3, pp. 1799–1825, 2018, doi: 10.1109/COMST.2018.2820810.

[30]   R. Sahay, A. Nayyar, R. K. Shrivastava, M. Bilal, S. P. Singh, and S. Pack, "Routing attack induced anomaly detection in IoT network using RBM-LSTM," *ICT Express*, May 2024, doi: 10.1016/j.icte.2024.04.012.

[31]   J. V. V. Sobral, J. J. P. C. Rodrigues, R. A. L. Rabêlo, J. Al-Muhtadi, and V. Korotaev, "Routing Protocols for Low Power and Lossy Networks in Internet of Things Applications," *Sensors*, vol. 19, no. 9, Art. no. 9, Jan. 2019, doi: 10.3390/s19092144.

[32]   A. Belghith and M. S. Obaidat, "Chapter 2 - Wireless sensor networks applications to smart homes and cities," in *Smart Cities and Homes*, M. S. Obaidat and P. Nicopolitidis, Eds., Boston: Morgan Kaufmann, 2016, pp. 17–40. doi: 10.1016/B978-0-12-803454-5.00002-X.

[33]   M. Neema, E. S. Gopi, and P. S. Reddy, "Optimizing Broadband Access and Network Design in Wireless Mesh Networks using Multi-Objective Particle Swarm Optimization," *Procedia Comput. Sci.*, vol. 230, pp. 275–286, Jan. 2023, doi: 10.1016/j.procs.2023.12.083.

[34]   J. Jun and M. L. Sichitiu, "MRP: Wireless mesh networks routing protocol," *Comput. Commun.*, vol. 31, no. 7, pp. 1413–1435, May 2008, doi: 10.1016/j.comcom.2008.01.038.

[35]   L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020, doi: 10.1109/JIOT.2019.2948888.

[36]   U. Elordi, A. Bertelsen, L. Unzueta, N. Aranjuelo, J. Goenetxea, and I. Arganda-Carreras, "Optimal deployment of face recognition solutions in a heterogeneous IoT platform for secure elderly care applications," *Procedia Comput. Sci.*, vol. 192, pp. 3204–3213, Jan. 2021, doi: 10.1016/j.procs.2021.09.093.

[37]   R. Want, "An introduction to RFID technology," *IEEE Pervasive Comput.*, vol. 5, no. 1, pp. 25–33, Jan. 2006, doi: 10.1109/MPRV.2006.2.

[38]   B. Li and J. Yu, "Research and Application on the Smart Home Based on Component Technologies and Internet of Things," *Procedia Eng.*, vol. 15, pp. 2087–2092, Jan. 2011, doi: 10.1016/j.proeng.2011.08.390.

[39]   H. Nguyen, D. Nawara, and R. Kashef, "Connecting the indispensable roles of IoT and artificial intelligence in smart cities: A survey," *J. Inf. Intell.*, Jan. 2024, doi: 10.1016/j.jiixd.2024.01.003.

[40]   H. Ziwei *et al.*, "The applications of internet of things in smart healthcare sectors: a bibliometric and deep study," *Heliyon*, vol. 10, no. 3, p. e25392, Feb. 2024, doi: 10.1016/j.heliyon.2024.e25392.

[41]   "HC3 TLP White Analyst Note: Internet of Things (IoT) Security - August 04, 2022 | AHA." Accessed: May 27, 2024. [Online]. Available: https://www.aha.org/cybersecurity-government-intelligence-reports/2022-08-04-hc3-tlp-white-analyst-note-internet-things

[42]   S. H. Shah and I. Yaqoob, "A survey: Internet of Things (IOT) technologies, applications and challenges," in *2016 IEEE Smart Energy Grid Engineering (SEGE)*, Oshawa, ON, Canada: IEEE, Aug. 2016, pp. 381–385. doi: 10.1109/SEGE.2016.7589556.

[43]   P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *J. Electr. Comput. Eng.*, vol. 2017, p. e9324035, Jan. 2017, doi: 10.1155/2017/9324035.

[44]   D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in IoMT Communications: A Survey," *Sensors*, vol. 20, no. 17, Art. no. 17, Jan. 2020, doi: 10.3390/s20174828.

[45]   B. Pradhan, S. Bhattacharyya, and K. Pal, "IoT-Based Applications in Healthcare Devices," *J. Healthc. Eng.*, vol. 2021, p. e6632599, Mar. 2021, doi: 10.1155/2021/6632599.

[46]   P. Tang, Q. Liang, H. Li, and Y. Pang, "Application of Internet-of-Things Wireless Communication Technology in Agricultural Irrigation Management: A Review," *Sustainability*, vol. 16, no. 9, Art. no. 9, Jan. 2024, doi: 10.3390/su16093575.

[47]   J. Zhang, H. Chen, L. Gong, J. Cao, and Z. Gu, "The Current Research of IoT Security," in *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)*, Hangzhou, China: IEEE, Jun. 2019, pp. 346–353. doi: 10.1109/DSC.2019.00059.

[48]   A. D. Jurcut, P. Ranaweera, and L. Xu, "Introduction to IoT Security," in *IoT Security*, 1st ed., M. Liyanage, A. Braeken, P. Kumar, and M. Ylianttila, Eds., Wiley, 2020, pp. 27–64. doi: 10.1002/9781119527978.ch2.

[49]   "A Blockchain-Based Authentication and Security Mechanism for IoT | IEEE Conference Publication | IEEE Xplore." Accessed: May 06, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8487449

[50]   S. Li, Y. Huang, and B. Yu, "A practical and flexible PUF-based end-to-end anonymous authentication protocol for IoT," *Comput. Netw.*, vol. 247, p. 110426, Jun. 2024, doi: 10.1016/j.comnet.2024.110426.

[51]   "S2542660523002767.htm."

[52]   A. Ghaz, A. Seddiki, and N. Nouioua, "Comparative Study of Encryption Algorithms Applied to the IOT," *Eurasia Proc. Sci. Technol. Eng. Math.*, vol. 21, pp. 469–476, Dec. 2022, doi: 10.55549/epstem.1226679.

[53]   D. A. F. Saraiva, V. R. Q. Leithardt, D. De Paula, A. Sales Mendes, G. V. González, and P. Crocker, "PRISEC: Comparison of Symmetric Key Algorithms for IoT Devices," *Sensors*, vol. 19, no. 19, p. 4312, Oct. 2019, doi: 10.3390/s19194312.

[54]   N. H. Shah, D. T. Khan, A. A. Banu, and L. H. Shah, "Symmetric and Asymmetric Encryption Schemes for Internet of Things: A Survey," *Int. J. Intell. Syst. Appl. Eng.*.

[55]   M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 1, 2017, doi: 10.14569/IJACSA.2017.080151.

[56]   S. K. S. Jose Costa Sapalo Sicato Shailendra Rathore, and Jong Hyuk Park, "A Comprehensive Analyses of Intrusion Detection System for IoT Environment," *J. Inf. Process. Syst.*, vol. 16, no. 4, pp. 975–990, Aug. 2020, doi: 10.3745/JIPS.03.0144.

[57]   J. Won, A. Singla, E. Bertino, and G. Bollella, "Decentralized Public Key Infrastructure for Internet-of-Things," in *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, Los Angeles, CA: IEEE, Oct. 2018, pp. 907–913. doi: 10.1109/MILCOM.2018.8599710.

[58]   S. Roy, Md. Ashaduzzaman, M. Hassan, and A. R. Chowdhury, "BlockChain for IoT Security and Management: Current Prospects, Challenges and Future Directions," in *2018 5th International Conference on Networking, Systems and Security (NSysS)*, Dhaka, Bangladesh: IEEE, Dec. 2018, pp. 1–9. doi: 10.1109/NSysS.2018.8631365.

[59]   A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an Optimized BlockChain for IoT," in *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, Pittsburgh PA USA: ACM, Apr. 2017, pp. 173–178. doi: 10.1145/3054977.3055003.

[60]   M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.

[61]   E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, "A Survey of IoT and Blockchain Integration: Security Perspective," *IEEE Access*, vol. 9, pp. 156114–156150, 2021, doi: 10.1109/ACCESS.2021.3129697.

[62]   R. Ramadan, "Internet of Things (IoT) Security Vulnerabilities: A Review," *PLOMS AI*, vol. 2, no. 1, 2022, Accessed: May 24, 2024. [Online]. Available: https://plomscience.com/journals/index.php/PLOMSAI/article/view/14

[63]   P. Singh and S. Sachdeva, "A Landscape of XML Data from Analytics Perspective," *Procedia Comput. Sci.*, vol. 173, pp. 392–402, Jan. 2020, doi: 10.1016/j.procs.2020.06.046.

[64]   I. Nadir, H. Mahmood, and G. Asadullah, "A taxonomy of IoT firmware security and principal firmware analysis techniques," *Int. J. Crit. Infrastruct. Prot.*, vol. 38, p. 100552, Sep. 2022, doi: 10.1016/j.ijcip.2022.100552.

[65]   A. Bhardwaj, S. Bharany, A. W. Abulfaraj, A. Osman Ibrahim, and W. Nagmeldin, "Fortifying home IoT security: A framework for comprehensive examination of vulnerabilities and intrusion detection strategies for smart cities," *Egypt. Inform. J.*, vol. 25, p. 100443, Mar. 2024, doi: 10.1016/j.eij.2024.100443.

[66] S. A. Shaikh, H. Chivers, P. Nobles, J. A. Clark, and H. Chen, "Network reconnaissance," *Netw. Secur.*, vol. 2008, no. 11, pp. 12–16, Nov. 2008, doi: 10.1016/S1353-4858(08)70129-6.

[67] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "A Study of RPL DODAG Version Attacks," in *Monitoring and Securing Virtualized Networks and Services*, vol. 8508, A. Sperotto, G. Doyen, S. Latré, M. Charalambides, and B. Stiller, Eds., in Lecture Notes in Computer Science, vol. 8508. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 92–104. doi: 10.1007/978-3-662-43862-6_12.

[68] I. U. Onwuegbuzie, S. A. Razak, and I. F. Isnin, "Control Messages Overhead Impact on Destination Oriented Directed Acyclic Graph—A Wireless Sensor Networks Objective Functions Performance Comparison," *J. Comput. Theor. Nanosci.*, vol. 17, no. 2, pp. 1227–1235, Feb. 2020, doi: 10.1166/jctn.2020.8794.

[69] V. Varadharajan, D. U. Tupakula, and K. Karmakar, "Study of Security Attacks against IoT Infrastructures".

[70] M. A. Boudouaia, A. Ali-Pacha, A. Abouaissa, and P. Lorenz, "Security Against Rank Attack in RPL Protocol," *IEEE Netw.*, vol. 34, no. 4, pp. 133–139, Jul. 2020, doi: 10.1109/MNET.011.1900651.

[71] A. H. Farea and K. Küçük, "Detections of IoT Attacks via Machine Learning-Based Approaches with Cooja," *EAI Endorsed Trans. Internet Things*, vol. 7, no. 28, pp. 1–12, Apr. 2022, doi: 10.4108/eetiot.v7i28.324.

[72] P. Perazzo, C. Vallati, G. Anastasi, and G. Dini, "DIO Suppression Attack Against Routing in the Internet of Things," *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2524–2527, Nov. 2017, doi: 10.1109/LCOMM.2017.2738629.

[73] V. Sindhu, "Performance of DIO Suppression attack in RPL based IoT networks," *Univers. Res. Rep.*, vol. 10, no. 1, 2023, doi: 10.36676/urr.2023-v10i1-032.

[74] D. Karagiannis and A. Argyriou, "Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning," *Veh. Commun.*, vol. 13, pp. 56–63, Jul. 2018, doi: 10.1016/j.vehcom.2018.05.001.

[75] P. Pongle and G. Chavan, "Real Time Intrusion and Wormhole Attack Detection in Internet of Things," *Int. J. Comput. Appl.*, vol. 121, no. 9, pp. 1–9, Jul. 2015, doi: 10.5120/21565-4589.

[76] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 1, pp. 616–644, 2020, doi: 10.1109/COMST.2019.2953364.

[77] H. Damghani, L. Damghani, H. Hosseinian, and R. Sharifi, "Classification of Attacks on IoT".

[78] S. K. K, S. Sahoo, A. Mahapatra, A. K. Swain, and K. K. Mahapatra, "Security Enhancements to System on Chip Devices for IoT Perception Layer," in *2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, Bhopal: IEEE, Dec. 2017, pp. 151–156. doi: 10.1109/iNIS.2017.39.

[79] G. H. An and T. H. Cho, "Improving Sinkhole Attack Detection Rate through Knowledge-Based Specification Rule for a Sinkhole Attack Intrusion Detection Technique of IoT," *Int. J. Comput. Netw. Appl.*, vol. 9, no. 2, p. 169, Apr. 2022, doi: 10.22247/ijcna/2022/212333.

[80] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *2015 IEEE Symposium on Computers and Communication (ISCC)*, Larnaca: IEEE, Jul. 2015, pp. 180–187. doi: 10.1109/ISCC.2015.7405513.

[81] J. Deogirikar and A. Vidhate, "Security Attacks inIoT: A Survey," 2017.

[82] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in *2017 IEEE*

International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bhubaneswar: IEEE, Dec. 2017, pp. 1–6. doi: 10.1109/ANTS.2017.8384164.

[83]   A. Wahab, O. Ahmad, M. Muhammad, and M. Ali, "A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 7, 2017, doi: 10.14569/IJACSA.2017.080768.

[84]   Z. Ling *et al.*, "Secure boot, trusted boot and remote attestation for ARM TrustZone-based IoT Nodes," *J. Syst. Archit.*, vol. 119, p. 102240, Oct. 2021, doi: 10.1016/j.sysarc.2021.102240.

[85]   A. Boteanu, F. Rastoceanu, I. Radoi, and C. Rusea, "Modeling and simulation of electromagnetic shielding for IoT sensor nodes case," in *2019 International Conference on Speech Technology and Human-Computer Dialogue (SpeD)*, Timisoara, Romania: IEEE, Oct. 2019, pp. 1–6. doi: 10.1109/SPED.2019.8906621.

[86]   D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," *J. Netw. Comput. Appl.*, vol. 66, pp. 198–213, May 2016, doi: 10.1016/j.jnca.2016.03.006.

[87]   S. Yi, P. Naldurg, and R. Kravets, "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks".

[88]   E. Bertino, "Data privacy for IoT systems: Concepts, approaches, and research directions," in *2016 IEEE International Conference on Big Data (Big Data)*, Washington DC,USA: IEEE, Dec. 2016, pp. 3645–3647. doi: 10.1109/BigData.2016.7841030.

[89]   R. Antrobus, B. Green, S. Frey, and A. Rashid, "The Forgotten I in IIoT: a vulnerability scanner for industrial internet of things," in *Living in the Internet of Things (IoT 2019)*, London, UK: Institution of Engineering and Technology, 2019, p. 1 (8 pp.)-1 (8 pp.). doi: 10.1049/cp.2019.0126.

[90]   J.-C. Fabre, Y. Deswarte, and B. Randell, "Designing Secure and Reliable Applications using Fragmentation-Redundancy-Scattering: an Object-Oriented Approach," in *Predictably Dependable Computing Systems*, B. Randell, J.-C. Laprie, H. Kopetz, and B. Littlewood, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, pp. 173–188. doi: 10.1007/978-3-642-79789-7_11.

[91]   J. Qian, S. Hinrichs, and K. Nahrstedt, "ACLA: A Framework for Access Control List (ACL) Analysis and Optimization".

[92]   N. Gupta, V. Naik, and S. Sengupta, "A firewall for Internet of Things," in *2017 9th International Conference on Communication Systems and Networks (COMSNETS)*, Bengaluru, India: IEEE, Jan. 2017, pp. 411–412. doi: 10.1109/COMSNETS.2017.7945418.

[93]   B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. De Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, Apr. 2017, doi: 10.1016/j.jnca.2017.02.009.