SEBHA UNIVERSITY CONFERENCE PROCEEDINGS, VOL.04 NO. 1 2025
DOI: 10.51984/SUCP.V4I1.3920

المؤتمر العلمي الأول للتطبيقات الهندسية (ICEA'2024)

The First Scientific Conference on Engineering Applications (ICEA'2024)

Conference homepage: www.icea.ly

Analyzing the Networking Infrastructure and Security Issues In Agriculture Smart Systems Based on Internet of Things Technology

*Nahed Fathi Farah[a], Azeddien M. Sllame[b], Osama Milud Sleik[c]

[a]Department of Mobile Computing, University of Tripoli, Tripoli, Libya
[b]Department of Networking, University of Tripoli, Tripoli, Libya
[c]Department of Crop Agricultural Research Center Tripoli, Libya

Keywords:

Internet of Things (IoT)
Smart Agriculture
Smart farming
Cloud computing
Fog computing
ZigBee
Security

ABSTRACT

This paper describes the impact of two main issues while designing Internet of Things (IoT)-based systems for agriculture and smart farms. The first issue is the network infrastructure, which needs careful evaluation in order to meet performance and data transfer requirements. The second issue is protection from cyber security attacks. However, the paper analyzed the ZigBee based on the IEEE 802.15.4 protocol, which showed promising throughput results. The distributed denial of service attacks were modeled and simulated, but the results showed that more protection techniques need to be researched and applied for designing novel IoT-based systems while enhance reliability, embed security and improve availability in the technology applied on agriculture smart farming fields.

تحليل بنية الشبكات وحوادث الأمن السيبر انى في أنظمة الزراعة الذكية القائمة على تكنولوجيا إنترنت الأشياء

*ناهد فرح[a] و عزالدين السلامي[b] و أسامة سليك[c]

[a] قسم الحوسبة المتنقلة، جامعة طرابلس، طرابلس، ليبيا
[b] قسم الشبكات، جامعة طرابلس، طرابلس، ليبيا
[c] مركز البحوث الزراعية - وزارة الزراعة، طرابلس، ليبيا

الكلمات المفتاحية:

إنترنت الأشياء
الأمان
الحوسبة السحابية
الحوسبة الضبابية
الزراعة الذكية
الأمان

الملخص

تناقش هذه الورقة تأثير مشكلتين رئيسيتين أثناء تصميم أنظمة تعتمد على إنترنت الأشياء (IoT) للزراعة والمزارع الذكية. المشكلة الأولى هي بنية الشبكة التحتية، التي تحتاج إلى تقييم دقيق لتلبية متطلبات الأداء ونقل البيانات. المشكلة الثانية هي الحماية من هجمات (الأمن السيبراني). تم في هذه الورقة تحليل ZigBee بناءً على بروتوكولIEEE 802.15.4 ، الذي أظهر نتائج واعدة في معدل النقل. كما تمت نمذجة ومحاكاة هجمات الحرمان الموزع للخدمة، وأظهرت النتائج أن هناك حاجة إلى البحث وتطبيق تقنيات حماية إضافية لتصميم أنظمة جديدة تعتمد على إنترنت الأشياء، مع تعزيز الموثوقية، وتضمين الأمان، وتحسين التوافر في التكنولوجيا المستخدمة في مجالات الزراعة الذكية.

1. Introduction

A number of strategies have been put in place to increase agricultural productivity since agriculture is essential to human life. On the other hand, difficulties like inclement weather and recurrent insect infestations can result in large agricultural losses. Agricultural production might be increased and financial losses could be decreased with the incorporation of cutting edge technology, especially Internet of Things (IoT) and smart sensors. With the help of smart sensors and communication technologies, the IoT is connecting disparate agricultural elements as well as helping continuous monitoring and control of critical issues. This empowers farmers to come to well-informed decisions, maximize resource efficiency, or increase the productivity of crops. Smart irrigation, precision farming, with computerized insect identification are some of the key uses. Although it involves enormous data transfers and quick reaction times, cloud computing enables worldwide applications. Fog computing reduces time prerequisites, optimizes usage of resources, plus improves data transport to meet these challenges. Mass adoption is hampered by issues including elevated expenses for implementation, worries about data security, and low levels of knowledge about technology between farmers. To optimize IoT in agriculture, supportive legislation and instructional programs are essential [1].

*Corresponding author:
E-mail addresses: N.Farah@uot.edu.ly ,(A. M. Sllame) a.sllame@uot.edu.ly ,(O. M. Sleik) sleik@uot.edu.ly

Article History : Received 25 March 2024 - Received in revised form 20 September 2024 - Accepted 15 October 2024

Climate change, population increase, with growing wealth have made ensuring global food security a serious concern. According to the Food and Agriculture Organization (FAO) of the United Nations, in order to feed 10 billion people by 2050, there would need to be a 70% increase in world production of food. IoT technologies are being used to build new agricultural practices, such as Smart Farming (SF), Precision Agriculture (PA), and Smart Agriculture (SA), in order to fulfill this need. IoT and other contemporary technologies are used in SF, SA, and PA. Drones, robots, and artificial intelligence are also employed to decrease input, labor, overall site needs thus increasing yield and production. Intelligent IoT devices, such actuators and sensors, are typically connected to the internet and one another using a multiple-layer SF framework. An SF platform gathers information from Internet of Things devices and analyses it to offer consumers different apps and degrees of accessibility.

"**Smart farming**" or intelligent agriculture, is the supervision of farms employing contemporary ICTs (Internet of Things, cloud computing, artificial intelligence (AI), big data analytics, robotics, and others to enhance the productivity, sustainability, and efficiency of agricultural processes by using sensors to monitor climate forecasts, irrigation, fertilizer, harvesting data, and other variables. Farmer organization is going to improve as a result of this. decisions by making the best use of available resources, resulting in higher production and profitability. "**IoT and Agriculture**" Real-time data collection and interpretation to track crop quality yield, and amount of water, with health of the soil at a specific location may be greatly enhanced by IoT, smart sensors, and artificial intelligence. Smart farming, which is characterized by increased productivity, is taking the place of conventional agricultural methods thanks to the Internet of Things and smart sensors. As shown in Figure (1), IoT-enabled technical procedures in agriculture also help with the analysis of soil health, soil erosion, fertilizer demands, soil fertility status, and crop quality.

The multi-layer smart agricultural architecture shown in Figure (1) is a typical example. This design is the reference architecture for a number of research initiatives. The architecture portrays the "Cloud", "Network Communication", "Edge", and "Physical" layers that link different smart IoT devices, including actuators and sensors, and heterogeneous Cyber-Physical Systems (CPSs) to the internet and each other. The framework of an SF platform, which shapes, operations, and maintains data in order to offer users a range of applications and access levels, is shown in the figure. The platform receives data from IoT devices. Therefore, cloud computing offers global services through virtualization over high-standard data centers, enabling the spread of IoT-based computing. Nevertheless, it requires large data transfer and minimal response time. To address these issues, fog computing is needed. In addition, Fog computing enhances data transfer, improves resource utilization, and reduces timing requirements for IoT devices and applications. It places computing power, resource management, efficient networking services, and network capacity at the edge between cloud data centres and users. Fog computing must consider applications, software, storage, communication infrastructure, and network design principles [1-5].

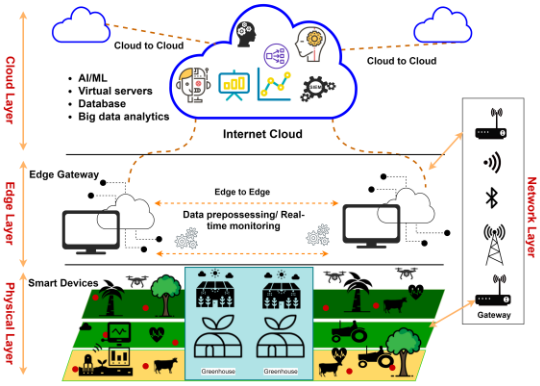


Figure 1: A typical illustration of smart agriculture architecture based on IoT

2. Literature Review

There are many research papers discussing many topics in IoT and smart applications. However, authors of reference [8] investigated precision agriculture in underdeveloped countries through the use of edge computer technologies and smart sensing. It emphasizes how easily edge computing may be integrated and how applicable different sensor technologies are. The construction of models for certain agricultural areas is also covered in the study, and the difficulties in interpreting the differences among distinct sensing equipment and edge computing algorithms are acknowledged. It also highlights the necessity of edge servers with high-performance computing capabilities that are affordable in order to provide seamless data flow operations for precision agriculture [8]. By providing taxonomy of cyber threats to SF and PA, with an emphasis on Advanced Persistent Threats (APTs), and researching associated risk mitigation techniques and safeguards, the authors of [9] examined the protective components of SF and PA. The primary contributions are taxonomy and a classification of security concerns inside SF/PA sectors. for SF environments to detect APT attacks and other security threats [9]. The authors of [10] highlighted the importance of IoT technology in transforming traditional agricultural practices into modern, intelligent systems. It highlights its potential for enhancing automation and intelligence, leading to improved product quality and efficiency. It also emphasizes the sustainable development of IoT, ensuring long-term viability and productivity. However, the authors call for overcoming challenges like infrastructure. They also suggest tailoring intelligent agriculture to local conditions for effective implementation [11]. In addition, authors in [12] discussed existing challenges in agricultural IoT, such as the need for improved data transmission in remote areas and the lack of comprehensive application systems. It forecasts future developments, including the establishment of standardized information perception, the use of advanced communication technologies like 5G, and the creation of integrated systems that enhance decision-making and traceability in agricultural processes [12]. The study in [13] examines the applications, challenges, and security measures of integrating IoT technologies in agriculture. It highlights the benefits of IoT in enhancing productivity and efficiency, but also identifies security challenges such as cyberattacks, data privacy issues, and insufficient authentication protocols. The paper reviews existing security protocols and proposes a layered architecture for smart agriculture, in which every layer identified with specific security requirements. It also examines existing testbeds and research contributions, emphasizing the need for further research in security protocols. The study concludes by calling for the development of robust authentication protocols to secure communication in smart farming environments [13].

In [18] the authors described implementing Machine Learning with IoT in smart farming to improve productivity as well as sustainability. It introduced the "*Remote Sensing Aided Framework for Smart Sustainable Agriculture*" (RSAF-SSA), a methodology optimizing production efficiency and resource utilization. The system shows high efficiency in irrigation techniques and productivity, highlighting the importance of leveraging advanced technologies for a sustainable future [18]. The study conducted by Kumar Shwetabh and Asha Ambhaikar in [19] explored the difficulties associated with applying intelligent monitoring systems for Agricultural Machinery (AM), primarily due to complexity with expense of IoT sensor technologies. It discusses challenges such as dependence on cloud and fog computing, while discussing necessity for robust network infrastructure, and the expertise needed, especially in rural areas with limited connectivity. The authors suggest utilizing edge devices like smartphones, which possess substantial computational power, as a practical solution. However, [19] describes the SHMAM-DLO (Smart Health Monitoring System for Agricultural Machines with Deep Learning-based Optimization), that utilizes an artificial neural network (ANN) with the Fusion Genetic Algorithm (FGA) for optimization. This approach efficiently addresses the growing agricultural needs in a sustainable manner by using smartphone microphones in place of expensive IoT sensors to offer cost-effective monitoring [19]. Additionally, the authors of [20] looked at how smart sensors and the Internet of Things have revolutionized agricultural techniques. It draws attention to how these technologies might improve agricultural productivity by precisely monitoring environmental variables including moisture content, soil quality, and insect detection. Ultimately, better decision-making and resource management can result from the incorporation of IoT, which will support agricultural sustainability.

3. Networking Infrastructure for IoT Smart Systems

Cloud computing offers reliably efficient services to different users and applications anytime and everywhere by employing concepts of virtualization over its high-standard data centers. Therefore, with cloud computing, users can hire different available resources from cloud service providers (e.g., Amazon, Google) either in hardware or software for their platforms or infrastructures to perform their work and provide other services to other users [1]. However, cloud computing providers own many geographically distributed data centers to provide a wide range of computing services to users independently of locations, which makes the cloud computing components performing an important function that facilitates the spread of IoT based computing[1]. Different applications of IoTs need huge data transfer and minimum response time. However, to solve many networking bottlenecks, distribution of intensive data transfer between users or IoT devices, and accessibility of mobile service providers everywhere in the world, make fog computing layer must exist, as seen in Figure (2) [3].

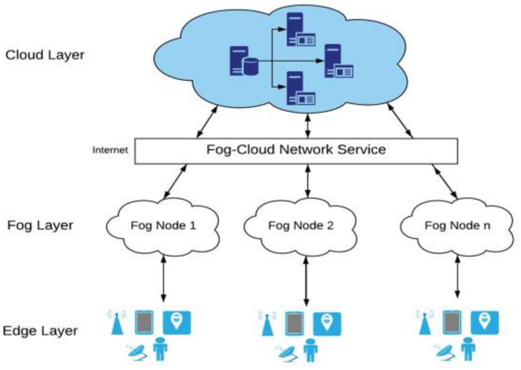


Figure 2: Hierarchical architecture: Cloud, Fog computing, and IoT

Fog computing has been introduced to fulfill gab, enhance data transfer, improve resource utilization, and reduce timing requirements by different IoT devices and applications between the users and cloud computing. Thus, for such purposes the fog computing is used to place computing power, resource management, efficient networking services and programming, and sufficient network capacity at the edge between cloud data centers and users to smoothness the data transfer between data centers of clouds, users, and IoTs devices. Consequently, to make fog computing do the intended role, it needs to care about applications, software, storage, communication infrastructure, and appropriate network design principles such as availability security, scalability, reliability, resiliency, fault tolerance, resource management, and efficiency. On another hand, information security is defined as the act of protecting data and information from unauthorized access, change, disruption, leakage, insertion, and deletion, while information systems security deals with protecting those systems used to process, transfer, and store such data and information. Usually, threats are applied against data, software, or hardware of target systems or networks to compromise the confidentiality, integrity, and availability (CIA) of those systems or networks. The threats may be made by nature, accidental, human's errors, or intentional "attacker" [1-5]. Fog computing architecture is a decentralized structure placed adjacent to IoT devices to provide on-demand services and applications with sufficient storage, efficient management, and reliable networking to meet timing and speed requirements. However, Fog is not substituting the cloud it works as a transitional layer in the IoT-Cloud infrastructure. One of the fog computing architecture point of view divides fog computing into five layers starting from bottom up: end devices layer, network layer, resources and cloud services layer, software defined layer, and cloud layer. Fog node is considered as the main service node in fog computing, which could be a router, gateway, a server. However, in the fog service layer, the fog nodes have the following features: (a) usually fog nodes are geographically distributed over a large area; (b) fog nodes have limited resource, computing power, and storage; (c) fog nodes operate with heterogeneous data from different applications; (d) fog nodes needs interoperability, and compatibility [3][4]. Therefore, such functions and architecture characteristics of fog nodes make them targeted by many security attacks such as DDoS attacks. However, these attacks target to disable the work of fog nodes by consuming their little computing resources and to overwhelm the networking systems between mobile fog nodes and the cloud.

4. Cyber Challenges of Applying IoT in Agriculture:

The adoption of IoT in agriculture confronts hurdles such as high implementation costs, data security concerns, and digital literacy issues, particularly in rural regions where farmers may lack the necessary skills to use these technologies efficiently. Despite the benefits of using IoT, AI, and big data in smart agriculture, it has significant security concerns. [3-6].

4.1 The following are the most important weaknesses [3-6].

1) **IoT Device Vulnerabilities in Smart Agriculture:** Their lack of strong security mechanisms renders them open to threats. There is also the potential that the firmware is out of date or unpatched.
2) **Data Security**: Sensitive data can be intercepted during transmission, and weak authentication mechanisms might result in illegal access.
3) **Network Security**: Weak encryption can lead to data interception and manipulation, while Distributed Denial of Service (DDoS) attacks can stop smart agricultural systems from operating steadily.

4.2 Cyber-Attacks on Smart Agriculture [1-11]

Numerous threats might target smart agriculture, taking advantage of these settings and associated smart information systems, or causing damage, disruption, illegal alteration, or even destruction. This section categorizes smart agricultural attacks according to the components they aim to target [3-6].

- **Hardware Attacks:** Skilled hackers take use of radio frequency (RF) jamming and side channel attacks, among other weaknesses, in cyberphysical and Internet of Things devices. While RF jamming threats cause communication disruptions and system unavailability, they also collect unauthorized information on system implementation details, which can seriously compromise the security and functionality of precision agriculture and smart farming systems.
- **Software attacks:** Indirect Attacks (SQL Injection), malware injection, buffer overflow, and software update incidents fall under this category. Applications are put at serious danger by these threats, which can deceive database servers into executing malicious SQL instructions, compromise system integrity, corrupt nodes; and devices, take advantage of code mistakes, and erode confidence in smart farming and precision farming systems.
- **Attacks on Networks and Related Equipment:** There are four types of network attacks: botnets, cloud computing, man-in-the-middle (MITM), and denial of service (DoS). DoS attacks block access to resources by authorized users; MIM attacks intercept and modify data; botnets employ devices connected to the internet for malicious purposes; and cloud computing attacks take use of functions like auto-scaling, self-provisioning, and on-demand services. These attacks go against the system's confidence, integrity, non-repudiation, and secrecy.

- **Data attacks:** Data leakage, ransomware, cloud data leakage, fake data injection, and misconfiguration are some of the subcategories of data attacks, which are threats that target data during storage, transport, or processing. Unauthorized data transmission occurs when files or storage devices are encrypted by ransomware; cloud data leakage exposes user-related data or services; fake data injection aims to compromise data integrity; and misconfiguration causes incorrect information to be distributed, breaching integrity.
- **Misuse Attacks:** These attacks target other organizations (individuals or institutes) by taking advantage of Smart Agriculture's physical resources. These can be further divided into compliance, invalidation, and cyberterrorism. IoT systems and cyber-physical devices may be used by cyberterrorism as a means of remote assault. On the other hand, the introduction of fake data through invalidation and compliance taints the certification process and makes it challenging to confirm the legitimacy of the data being certified.

5. Experimental Results:

The experimental results section will present two case studies: the first one will refer to the evaluation of the performance of ZigBee as IoT employing IEEE 802.15.4; while second case study will describe some attacks against the infrastructure of the smart IoT.

(A) An assessment of the PHY layer and MAC sublayer of the IEEE 802.15.4 standard for ZigBee, which enable basic sensor-to-sensor communication, is conducted. In accordance with IEEE 802.15.4 standard standards, an accurate simulation model is presented in this study. But utilizing OPNET simulator, a top modeling and simulation environment, we study two distinct situations in which we investigate the topological characteristics and performance of the IEEE 802.15.4 standard. In order to facilitate the modeling and prototyping of distributed systems and communication networks, this simulation tool offers an extensive development environment. We made a comparison of the three potential topologies (Star, Mesh, and Tree).

(B) Security issue with IoT layer is analyzed focusing on DDoS attacks using modeling and simulation tools using virtual components with Kali Linux environment.

5.1 Case study A: details

ZigBee is used in this scenario model, with two ZigBee coordinators in the case study topology as seen in Figure (3). With a single PAN_0, the first ZigBee coordinator travels to the Tree topology; with two PANs (PAN_0 and PAN_1), the second ZigBee coordinator goes to the Tree topology. Six ZigBee routers and six ZigBee End devices make up the topology. While the others are stationary and dispersed across a 1000 m × 1000 m area, one router and one end device are mobile

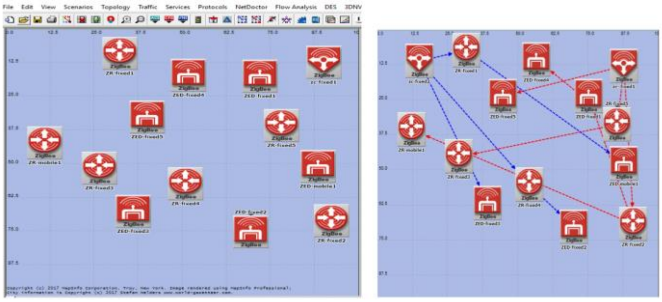
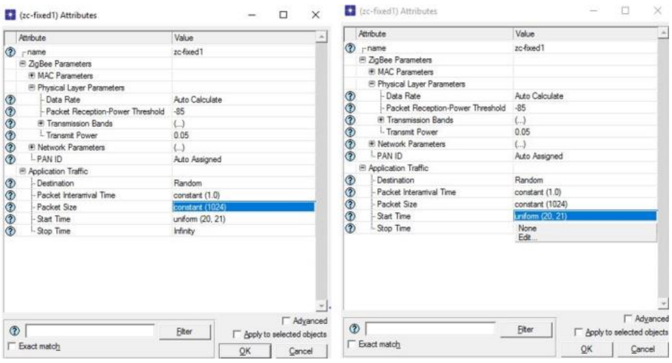


Figure 3: IoT infrastructure

However, IEEE 802.15.4 protocol describes 3 forms of modules:

1) PAN (Personal Area Network) coordinator: This supervisor connects with other nodes it recognizes its own PAN. Furthermore, it suggests providing global synchronization services to other network nodes by sending beacon frames with PAN identification and other pertinent data.
2) Coordinator: This function is equivalent to that of a PAN coordinator, with the exception it doesn't generate its own PAN. Coordinator is linked to the PAN coordinator and offers services for local node synchronization within its coverage area via major transfer beacon frames with the linked PAN's identifier.
3) A simple (secondary) node is one that lacks coordinated functionality. It is connected to the PAN Coordinator (or coordinator) as a secondary node so that it may synchronize with the other nodes in the network. Full Function Devices (FFDs) are the first two categories of nodes described in the IEEE 802.15.4 2003 standard; this indicates that they implement every feature of the IEEE 802.15.4 protocol.

Thus, Figure (4) displays the setting of the ZigBee coordinator, end-to-end latency (sec), number of hops, throughput (bit/sec), and load (bit/sec) are the performance metrics that are compared between the outcomes of the "Star, Tree, and Mesh topologies scenarios to analyze the implementation of ZigBee based WSN." Packets represent the traffic that is sent and received.



(zc-fixed1) Attributes

Attribute	Value
name	zc-fixed1
ZigBee Parameters	
MAC Parameters	
Physical Layer Parameters	
Data Rate	Auto Calculate
Packet Reception-Power Threshold	-85
Transmission Bands	(...)
Transmit Power	0.05
Network Parameters	(...)
PAN ID	Auto Assigned
Application Traffic	
Destination	Random
Packet Interarrival Time	constant (1.0)
Packet Size	constant (1024)
Start Time	uniform (20, 21)
Stop Time	Infinity

(zc-fixed1) Attributes

Attribute	Value
name	zc-fixed1
ZigBee Parameters	
MAC Parameters	
Physical Layer Parameters	
Data Rate	Auto Calculate
Packet Reception-Power Threshold	-85
Transmission Bands	(...)
Transmit Power	0.05
Network Parameters	(...)
PAN ID	Auto Assigned
Application Traffic	
Destination	Random
Packet Interarrival Time	constant (1.0)
Packet Size	constant (1024)
Start Time	uniform (20, 21)
Stop Time	None Edit...

Figure 4: ZigBee coordinator configuration

Packet End-to-End Delay: Figure (5) describes the end-to-end delay of the packets flown in the ZigBee network for the three topologies. The tree and Mesh topologies have similar end-to end delay (less than 0.05 sec) which is much less than the star topology delay (reaches 0.65 sec value). Therefore, the end-to-end delay of the star topology is worse where it is higher with more than 50% compared with other two topologies.

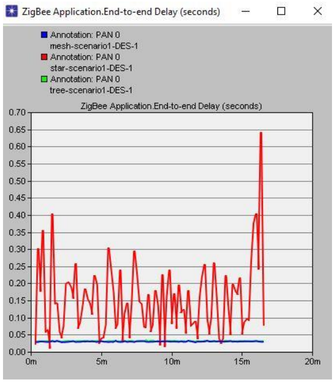


Figure 5: ZigBee Application end-to-end Delay (star, mesh, tree)

ZigBee 802.15.4 MAC Throughput (bits/sec): Figure (6) describes those measures of the highest Throughput accomplished in the all tested topologies. From the figure it is clear that the Tree topology has registered the highest value (about 43,000bps), while the Mesh topology has recorded the second highest Throughput (about 37,000 bps); but the Star topology has the lowest Throughput (around 10,000 bps).

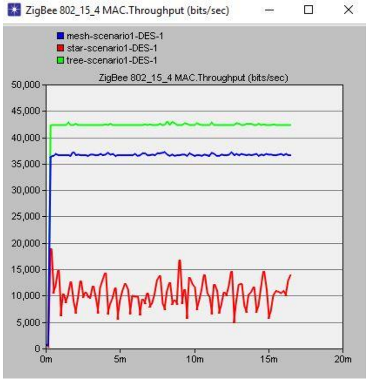


Figure 6: ZigBee 802.15.4MAC.Throughput (bits/ sec) with (star, mesh, tree)

ZigBee 802.15.4 MAC Load(bit/sec): Figure (7) shows that Star topology has the lowest (worst) ZigBee 802.15.4 the load of MAC layer (about 12,500 bps) value; while the Tree topology has got the highest ZigBee 802.15.4 MAC loads (about 41,000 bps) value compared to star topology and mesh topology. The Mesh topology has recorded (about 35,000 bps).

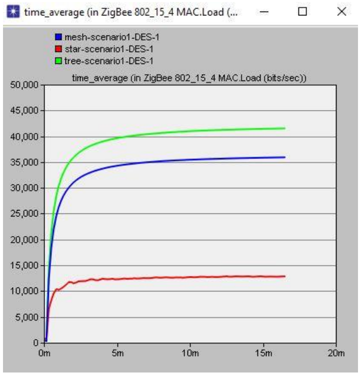


Figure 7: ZigBee 802.15.4MAC.Load (bits/sec) with (star, tree, mesh)

Case study B in this scenario we discuss the cyber security attacks against the IoT: This part is done by applying DDoS attacks on IoT to study the risk of such attacks on the field. The case study diagram is made on virtual machine environment using Kali Linux and its associated tools as seen in Figure (8). However, the Wireshark tool is used to monitor the attacks that performed by different tools such Yirsinia and Goldeneye. However, Figure (9) illustrates the lunching of the DDoS attack, while Figure (10) exemplifies the snapshots of the running attacks on Wireshark tool

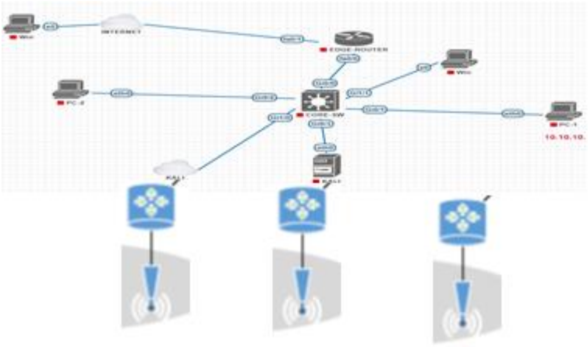
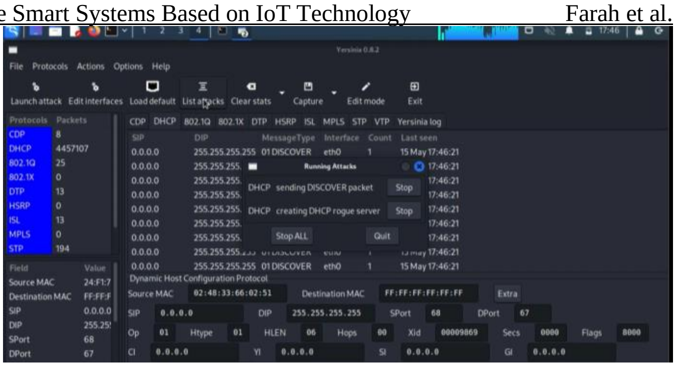
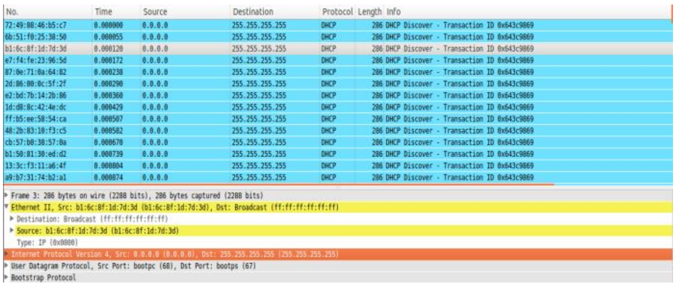


Figure 8: the virtual lab for the case study 2



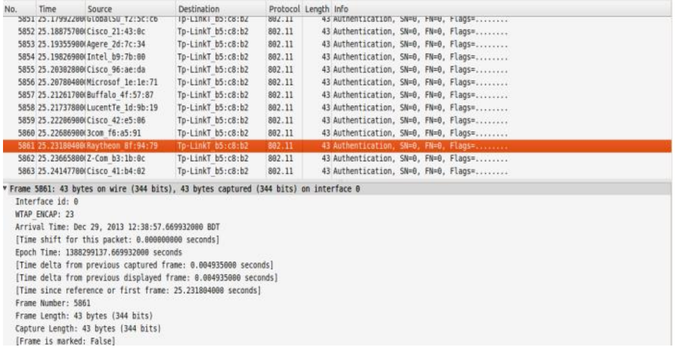
```
Protocols  Packets     CDP  DHCP  802.1Q  802.1X  DTP  HSRP  ISL  MPLS  STP  VTP  Yersinia log
CDP        8           SIP       DIP              MessageType  Interface  Count  Last seen
DHCP       4457107     0.0.0.0   255.255.255.255  01 DISCOVER  eth0       1      15 May 17:46:21
802.1Q     25          0.0.0.0   255.255.255.                                    17:46:21
802.1X     0           0.0.0.0   255.255.255.  DHCP  sending DISCOVER packet     17:46:21
DTP        13          0.0.0.0   255.255.255.                                    17:46:21
HSRP       0           0.0.0.0   255.255.255.  DHCP  creating DHCP rogue server  17:46:21
ISL        13          0.0.0.0   255.255.255.                                    17:46:21
MPLS       0           0.0.0.0   255.255.255.                                    17:46:21
STP        194         0.0.0.0   255.255.255.                                    17:46:21
                       0.0.0.0   255.255.255.255  01 DISCOVER  eth0       1      15 May 17:46:21
Field            Value
Source MAC       24:F1:7   Dynamic Host Configuration Protocol
Destination MAC  FF:FF:F   Source MAC  02:48:33:66:02:51   Destination MAC  FF:FF:FF:FF:FF:FF
SIP              0.0.0.0   SIP  0.0.0.0   DIP  255.255.255.255   SPort  68   DPort  67
DIP              255.25!   Op  01  Htype  01  HLEN  06  Hops  00  Xid  00009869  Secs  0000  Flags  8000
SPort            68        CI  0.0.0.0   YI  0.0.0.0   SI  0.0.0.0   GI  0.0.0.0
DPort            67
```

Figure 9: demonstrates that the attack is running against the IoT network by Yirsinia tool.



```
No.                Time      Source   Destination      Protocol Length Info
72:49:08:46:b5:c7  0.000000  0.0.0.0  255.255.255.255  DHCP     286 DHCP Discover - Transaction ID 0x643c9869
6b:51:f0:25:38:50  0.000055  0.0.0.0  255.255.255.255  DHCP     286 DHCP Discover - Transaction ID 0x643c9869
b1:6c:8f:1d:7d:3d  0.000120  0.0.0.0  255.255.255.255  DHCP     286 DHCP Discover - Transaction ID 0x643c9869
e7:f4:fe:23:96:5d  0.000172  0.0.0.0  255.255.255.255  DHCP     286 DHCP Discover - Transaction ID 0x643c9869
87:0e:71:0a:64:82  0.000238  0.0.0.0  255.255.255.255  DHCP     286 DHCP Discover - Transaction ID 0x643c9869
2d:86:00:0c:5f:2f  0.000290  0.0.0.0  255.255.255.255  DHCP     286 DHCP Discover - Transaction ID 0x643c9869
e2:bd:7b:14:2b:86  0.000360  0.0.0.0  255.255.255.255  DHCP     286 DHCP Discover - Transaction ID 0x643c9869
1d:d8:8c:42:4e:dc  0.000429  0.0.0.0  255.255.255.255  DHCP     286 DHCP Discover - Transaction ID 0x643c9869
ff:b5:ee:58:54:ca  0.000507  0.0.0.0  255.255.255.255  DHCP     286 DHCP Discover - Transaction ID 0x643c9869
48:2b:83:10:f3:c5  0.000582  0.0.0.0  255.255.255.255  DHCP     286 DHCP Discover - Transaction ID 0x643c9869
cb:57:b0:38:57:0a  0.000670  0.0.0.0  255.255.255.255  DHCP     286 DHCP Discover - Transaction ID 0x643c9869
b1:50:81:30:ed:d2  0.000739  0.0.0.0  255.255.255.255  DHCP     286 DHCP Discover - Transaction ID 0x643c9869
13:3c:f3:11:a6:4f  0.000804  0.0.0.0  255.255.255.255  DHCP     286 DHCP Discover - Transaction ID 0x643c9869
a9:b7:31:74:b2:a1  0.000874  0.0.0.0  255.255.255.255  DHCP     286 DHCP Discover - Transaction ID 0x643c9869
▸ Frame 3: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits)
▾ Ethernet II, Src: b1:6c:8f:1d:7d:3d (b1:6c:8f:1d:7d:3d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: b1:6c:8f:1d:7d:3d (b1:6c:8f:1d:7d:3d)
    Type: IP (0x0800)
▸ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
▸ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
▸ Bootstrap Protocol
```

Figure 10-A: Wireshark output of a DDoS attack



```
No.   Time         Source             Destination        Protocol Length Info
 5851 25.17992200( GlobalSu_f2:5c:c6  Tp-LinkT_b5:c8:b2  802.11   43 Authentication, SN=0, FN=0, Flags=........
 5852 25.18875700( Cisco_21:43:0c     Tp-LinkT_b5:c8:b2  802.11   43 Authentication, SN=0, FN=0, Flags=........
 5853 25.19355900( Agere_2d:7c:34     Tp-LinkT_b5:c8:b2  802.11   43 Authentication, SN=0, FN=0, Flags=........
 5854 25.19826900( Intel_b9:7b:00     Tp-LinkT_b5:c8:b2  802.11   43 Authentication, SN=0, FN=0, Flags=........
 5855 25.20302800( Cisco_96:ae:da     Tp-LinkT_b5:c8:b2  802.11   43 Authentication, SN=0, FN=0, Flags=........
 5856 25.20780400( Microsof_1e:1e:71  Tp-LinkT_b5:c8:b2  802.11   43 Authentication, SN=0, FN=0, Flags=........
 5857 25.21261700( Buffalo_4f:57:87   Tp-LinkT_b5:c8:b2  802.11   43 Authentication, SN=0, FN=0, Flags=........
 5858 25.21737800( LucentTe_1d:9b:19  Tp-LinkT_b5:c8:b2  802.11   43 Authentication, SN=0, FN=0, Flags=........
 5859 25.22206900( Cisco_42:e5:06     Tp-LinkT_b5:c8:b2  802.11   43 Authentication, SN=0, FN=0, Flags=........
 5860 25.22686900( 3com_f6:a5:91      Tp-LinkT_b5:c8:b2  802.11   43 Authentication, SN=0, FN=0, Flags=........
 5861 25.23180400( Raytheon_8f:94:79  Tp-LinkT_b5:c8:b2  802.11   43 Authentication, SN=0, FN=0, Flags=........
 5862 25.23665800( Z-Com_b3:1b:0c     Tp-LinkT_b5:c8:b2  802.11   43 Authentication, SN=0, FN=0, Flags=........
 5863 25.24147700( Cisco_41:b4:02     Tp-LinkT_b5:c8:b2  802.11   43 Authentication, SN=0, FN=0, Flags=........
▾ Frame 5861: 43 bytes on wire (344 bits), 43 bytes captured (344 bits) on interface 0
   Interface id: 0
   WTAP_ENCAP: 23
   Arrival Time: Dec 29, 2013 12:38:57.669932000 BDT
   [Time shift for this packet: 0.000000000 seconds]
   Epoch Time: 1388299137.669932000 seconds
   [Time delta from previous captured frame: 0.004935000 seconds]
   [Time delta from previous displayed frame: 0.004935000 seconds]
   [Time since reference or first frame: 25.231804000 seconds]
   Frame Number: 5861
   Frame Length: 43 bytes (344 bits)
   Capture Length: 43 bytes (344 bits)
   [Frame is marked: False]
```

Figure 10-B: Wireshark output of a DDoS attack

6. Conclusion

IoT applications for farming are transforming the sector by raising production, environmental responsibility, driving profitability. Producers are able to arrive at well-informed decisions that result in improved resource management, decreased environmental impact, and increased revenue by utilizing technology and real-time information. The application in IoT in agriculture will probably grow whenever innovation develops further, providing further creative answers for the obstacles of contemporary farming.

The first experiment presented a comparison analysis of IoT infrastructure in terms of ZigBee based on IEEE 802.15.4 protocol of wireless sensor networks in terms of IoT using OPNET simulation tool. The simulation study involved an exploration to three different scenarios of topological features (Star, Mesh and Tree) and effectiveness of the IEEE 802.15.4 standard. However, with terms of IEEE 802.15.4 MAC Throughput; the Tree topology has recorded the highest value (Throughput value of 43,000bps, whereas the Mesh topology gained the second highest Throughput about 37,000 bps; but the Star topology has the registered the lowest Throughput value which is around 10,000 bps. Furthermore, in terms of end-to-end delay the Tree and Mesh topologies reported same end-to end delay value i.e., less than 0.05 sec which is much less than the star topology which touches 0.65 sec value?

The second experiment illustrated that a lot of IoT devices need more protection against different cyber security attacks specifically DDoS attacks which work against availability of the IoT systems such as those in agricultural field, which has a large impact on food industry.

7. Future Prospects

We emphasize the potential for IoT to transform traditional agricultural practices into intelligent systems that can significantly improve productivity and sustainability. This field still needs more scientific research and technological developments in order to maximize the advantages of IoT for smart farming to eliminate current obstacles, as long as appropriate measures are implemented to address these issues, enhancing cyber security, education, and technological advancements are needed.

8. References

[1] Pooyan Habibi, Mohammed Farhoudi, Sepehr Kazemian, Siavash Khorsandi, Alberto Leon-Garcia, Fog Computing: A Comprehensive Architectural Survey, IEEE Access, Vol.4, 2016, pp.1-29.

[2] Tariq Qayyum, Asad Waqar Malik, Muazzam A. Khan, Samee U. Khan: Modeling and Simulation of Distributed Fog Environment using FogNetSim++,

[3] Alzahrani, S. and Hong, L.: Generation of DDoS Attack Dataset for Effective IDS Development and Evaluation, Journal of Information Security, Vol. 9, August 2018, pp.225-241, Scientific Research Publishing Inc.

[4] R. Roman, J. Lopez, M. Mambo, Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges. Future Generation Computer Systems Journal, issue 78 part 2, pp.680–698, Science Direct, Elsevier publisher, January 2018.

[5] K. Lee, D. Kim, D. Ha, U. Rajput and H. Oh, "On security and privacy issues of fog computing supported Internet of Things environment," 2015 6th International Conference on the Network of the Future (NOF), 2015, IEEE, pp. 1-3, doi: 10.1109/NOF.2015.7333287.

[6] Yehia I. Alzoubi, Valmira H. Osmanaj, Ashraf Jaradat, Ahmad Al-Ahmad: Fog computing security and privacy for the Internet of Thing applications: State-of-the-art, Security and Privacy, 2021; 4:e145, John Wiley & Sons Ltd, https://doi.org/10.1002/spy2.145.

[7] Adrien Bonguet, Martine Bellaiche: A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing, Future Internet Journal, Vol. 9, Issue 3, 43, MDPI, https://doi.org/10.3390/fi9030043 , August 2017.

[8] Routray, S.K., Javali, A., Sharma, L., Ghosh, A., & Sahoo, A. , “Internet of Things Based Precision Agriculture for Developing Countries”. *International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 1064-1068, 2019.

[9] Kim, W.-S., Lee, W.-S., & Kim, Y.-J., “A review of the applications of the Internet of Things (IoT) for agricultural automation. Journal of Biosystems Engineering”, 45(1), 1-17, 2020.

[10] Akhtar, M.N., Shaikh, A.J., Khan, A., Awais, H., Bakar, E.A., & Othman, A.R., “Smart Sensing with Edge Computing in Precision Agriculture for Soil Assessment and Heavy Metal Monitoring: A Review”. *Agriculture, 11*, 475,2021.

[11] Yazdinejad, A., Zolfaghari, B., Azmoodeh, A., & Duncan, E., et al., “A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures”. *Applied Sciences, 11*(16), 7518. 2021.

[12] Yang, X., Shu, L., Chen, J., Ferrag, M.A., Wu, J., Nurellari, E., & Huang, K.. A Survey on Smart Agriculture: Development Modes, Technologies, and Security and Privacy Challenges. *IEEE/CAA Journal of Automatica Sinica, 8*, 273-302, 2021.

[13] Yue, S., Du, Y., & Zhang, X., “Research and application of agricultural Internet of Things technology in intelligent agriculture”. *Journal of Physics: Conference Series, 1769*(1), 012020, 2021.

[14] Jinyuan Xu, Baoxing Gu, Guangzhao Tian, “ Review of agricultural IoT technology, Artificial Intelligence in Agriculture”, Volume 6,Pages 10-22, ISSN 2589-7217, 2022.

[15] Quy VK, Hau NV, Anh DV, Quy NM, Ban NT, Lanza S, Randazzo G, Muzirafuti A. “IoT-Enabled Smart Agriculture: Architecture, Applications, and Challenges”. *Applied Sciences*. 12(7):3396, 2022.

[16] Vangala, A., Das, A. K., Chamola, V., Korotaev, V., & Rodrigues, J. J. P. C. “Security in IoT-enabled smart agriculture: architecture, security solutions and challenges”. *Cluster Computing*, 25(1), 1-20. doi:10.1007/s10586-022-03445-5. 2022

[17] Pawar, A., & Deosarkar, S. B. ,IoT-based smart agriculture: an exhaustive study. *Wireless Networks*, *29*(6), 2457-2470. 2023

[18] Kumar, S., & Ambhaikar, A. Implementing intelligent monitoring systems for agricultural machinery using IoT and AI. In *BIO Web of Conferences* (Vol. 82, Article 05007), 2024.

[19] Haval, A. M., & Rahman, F. "Application of machine learning techniques and the Internet of Things for smart, sustainable agriculture". *BIO Web of Conferences,* Vol. 82, Article 05021), 2024

[20] Shwetabh, K., & Ambhaikar, A. (2024). Smart Health Monitoring System of Agricultural Machines: Deep Learning-based Optimization with IoT and AI. BIO Web of Conferences.

[21] Prem R., Abhratanu G., Satadal A., Suchandra B., “Internet of Things and smart sensors in agriculture: Scopes and challenges”, Journal of Agriculture and Food Research,Vol. 14, 100776), 2023