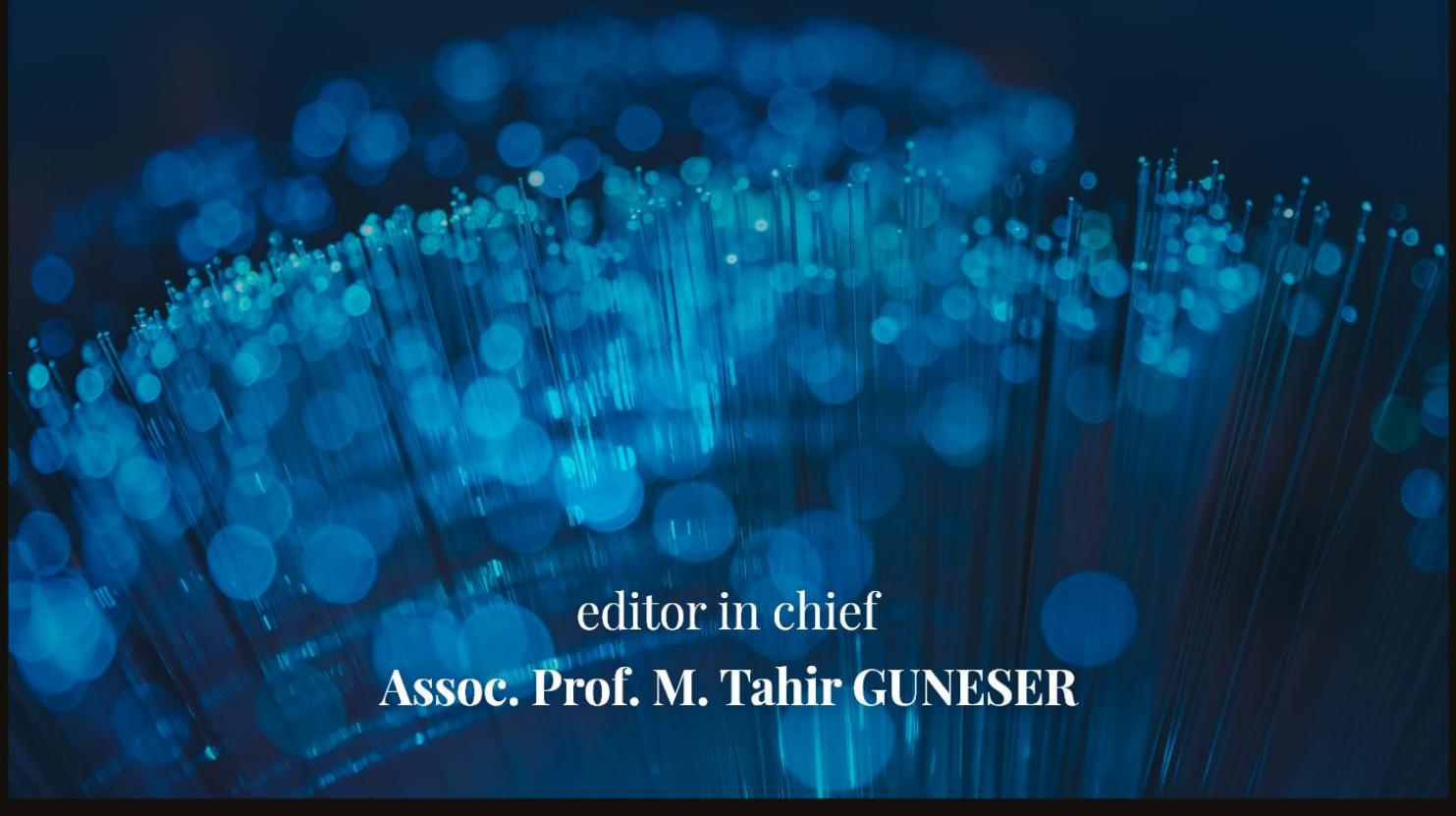
Volume: 1 Issue: 2 Year: 2021

JOMCOM

Journal of Millimeterwave Communication, Optimization and Modelling



editor in chief
Assoc. Prof. M. Tahir GUNESER

CONTENT

About the Journal

Journal of Millimeterwave Communication, Optimization and Modelling (JOMCOM) is an international on-line and refereed journal published 2 times a year (June and December) in English. Journal of Millimeterwave Communication, Optimization and Modelling (JOMCOM) published its first issue in 2021 and has been publishing since 2021. Manuscripts in JOMCOM Journal reviewed of at least 2 referees among the referees who have at least doctorate level in their field.

Journal of Millimeterwave Communication, Optimization and Modelling (JOMCOM) is an international online journal that is published 2 times in a year in English.

The purpose of JOMCOM is publishing the scientific research in various fields of communication.

All kinds of transactions and the application about the journal can be made from **https://jomcom.org**

The scientific responsibility of articles belongs to the authors.

ISSN: 2791-9293

Editor in Chief:

Assoc. Prof. Dr. Muhammet Tahir GÜNEŞER

Karabük University

Faculty of Engineering

Department of Electrical and Electronics Engineering

Head of Communication Division

Karabük, TURKEY

jomcomeditor@gmail.com

PUBLISHER

Assoc. Prof. Muhammet Tahir GÜNEŞER

Aims & Scope

Communication Technologies: Journal of Millimeter-wave Communication, Optimization and Modelling (JOMCOM) publishes original research and review articles in Communication Technologies, Innovative Technologies, and Systems in the broad field of Information-Communication Technology. Purpose of JOMCOM; To create value in the field by publishing original studies that will contribute to the literature in wireless communication sciences and be a resource for academia and industrial application whole over the world. Besides, JOMCOM aims to bring the valuable work of researchers working in Communication studies to a broader audience at home and abroad. Readership of JOMCOM; valuable representatives of the wireless communication area, especially those who do academic studies in it, and those who do academic studies about modelling and system design and other interested parties. Since JOMCOM will appeal to a broader audience in article submissions, it prioritizes studies prepared in English.

Optimization and Modelling: Journal of Millimeter-wave Communication, Optimization and Modelling (JOMCOM), within the scope of Wireless Communication Sciences, publishes articles on communication theory and techniques, systems and networks, applications, development and regulatory policies, standards, and management techniques. It also reports experiences and experiments, best practices and solutions, lessons learned, and case studies. Additional studies on System Design, Modelling and Optimization. Subject areas of interest covered in the journal include the following but are not limited to:

5G-6G Technologies

Circuits for Optical Communication Systems

Antenna Design

Communication Design Materials

Fiber Optic Communication

Innovative Designs for Communications

Integrated Circuits for Communications

Optimization Methods on Engineering

Realization of Antenna Systems

Realization of Microwave, Radar, and Sonar Systems

RF Circuits

System Design

Visible Light Communication

Wireless Communication

Optimization of Battery Endurance By Using Thermal Regulation System

Abdullah Alazzawi
Department of Electrical and Electronics Engineering
Karabuk University
Karabuk, Turkey
adnab2@gmail.com

***Abstract*—Thermal runaway is one of the most prevalent problems that is related to batteries. The problem of unwanted thermal runaway and the unexpected decrement temperatures that happens both directly or indirectly by internal and external influences poses a risk to the efficiency and the lifespan of batteries. The medium for using batteries differs from place to place, each medium has its different temperature conditions. So the problem's solution that is being discussed in this paper is being shortly showed as enhancing battery endurance via balancing the voltage ratios in each cell, tracking and monitoring battery temperatures while taking into account the variation of mediums that the battery will be used in. The temperature degrees are being elevated and reduced by employing an Arduino microcontroller that works passively with the fluid pump so it can indirectly manage the temperature of batteries. This management of temperature degrees improves the efficiency of batteries and prevents their structure from being damaged.**

Keywords—battery, battery thermal management, battery cooling system, electric vehicles, thermal runaway

I. INTRODUCTION

Recently, there has been a change in the global energy system, as it gradually began to abandon energy sources that may cause problems to the ecosystem. Therefore, a greater trend has been made to use sustainable electric energy [1]. Batteries are an essential part of this sustainable energy system. Batteries are used in both small and large industries and we see remarkable progress in this field, especially in the electric vehicles sector, and from here comes our main topic (batteries). One of the most prominent problems with batteries is thermal runaway [2]. The abnormal temperature change may cause damage to some components of the battery and leading the insulating materials that are replaced between cathode and anode to lose their properties causing a rupture or leakage even in worse cases causing an explosion. Batteries are energy storage components that convert chemical energy into electrical energy.

Most large projects do not operate with a single battery, but rather depend on more than one battery, especially if we look at the field of electric vehicles, we see that electric vehicles battery system is composed of multiple cells which are designed in series and parallel combinations that form a battery pack to produce a desired rate of energy. At the point when the battery is associated with a load for supplying the demand of energy the battery gradually gets empty then comes the need of recharging the battery, so we need a recharge process.

The process of discharging and recharging generates heat, this temperature changing happens by utilizing what we call joule heating. The abnormal increment in temperature may cause physical damage to the battery structure or even in worse cases leading to battery explosion [3]. And it may lead to the release of high amounts of toxic and flammable gas [4]. Preventing such problems is our priority in this research. So our aim in this study is to ensure that we get accurate voltage and current values by maintaining a constant temperature.

There are several cooling techniques utilized in the battery system to maintain batteries temperature under control and to prevent the overheating of the battery [5]. In contrast to other cooling methods, the system we used in our study was chosen to be simple, efficient, reliable, and cheap in comparison with other cooling techniques.

We managed to automate a system that can regulate itself according to the temperature degree of the battery that it receives so whenever the level of temperature exceeds the usual levels that we defined before, the cooling system works on restoring the temperature to the optimum degrees to ensure that the system works at peak performance. We managed to simulate the system's temperature using Matlab while charging and discharging and also we made an observation on how the battery temperature changes while it is used with a cooling system and also without using a cooling system.

Air cooling systems are well known in the industrial field for its simplicity, low cost, and reliability, but it is not appropriate for being operated with batteries that run at a high ambient temperature or with a high discharging rate so in these cases air cooling systems are considered to be ineffective [6]. There are a lot of types of cooling techniques [7] which are used in battery thermal managing system, as it is depicted in Fig. 1.

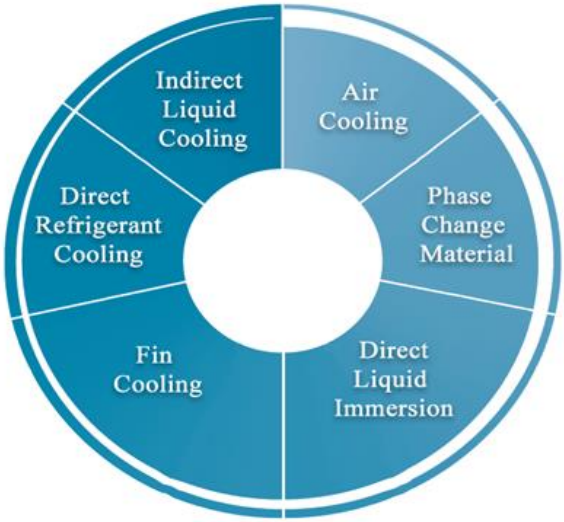


Fig. 1. Traditional battery thermal management cooling systems

II. BATTERY MANAGING SYSTEM

A. Battery Thermal Runaway

The chemical reaction that takes place inside the battery to produce energy is the result of electrons being transferred from the anode to the electrode, this electronic discharge is being occurred with the help of the electrolyte, which is a chemical medium that allows electrons to pass through it so that the chemical potential works on balancing the two ends of the battery. The constant flow of electrons between the two processes of charging and discharging generates heat as a result of Joule's law: P=R*I^2 [8].

Some of the energy loss converts into heat and it happens by the current that flows through the internal resistance of the batteries. The temperature increment is limited by the amount of energy inside the battery.

B. Cooling System Hardware

Fig. 2 depicts the hardware design in which a 12V battery is used during this process to highlight the variance and disparity between the two battery packs behavior in a different graph while one of the batteries is being operated with a cooling system and the other one is not to make a comparison to inspect how efficient and effective the cooling system is.

As shown in the above design, a thermal sensor of the LM35 type was used. The temperatures that this sensor can measure range from -55 to 150 Celsius. This type of sensor has a structure similar to that of an ordinary transistor, and the working principle of this sensor is by converting the temperatures measured in the surrounding physical medium into an analog voltage. The relationship between the voltages and the temperature is directly proportional, so the higher the temperature, the greater the amount of voltage.

The cooling system used in this research is based on regulating the temperature by using fluids for cooling when needed.

As a result, when the sensor detects elevated temperatures, a signal is transmitted to the fluid pumps connected with the Arduino input ports, causing the coolant fluids to be pumped.

We have two major components in our system that need to be cooled down in case of abnormal increment in temperature degree and the two major components are the load and the battery, so we attached the fluid pump to each of them. So when the temperature of the battery reaches the set point, the cooling device inside the thermal system is activated, after activating it, the temperature of the battery will be reduced and it will allow the system to operate within its normal operating range.

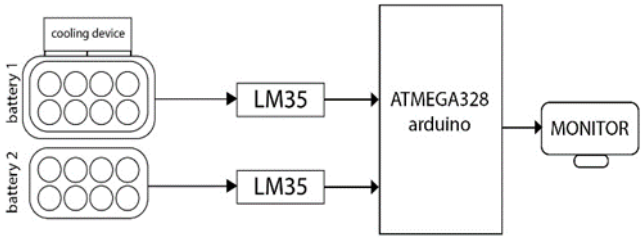


Fig. 2. Hardware Design

III. METHODOLOGY

The cooling system can produce higher thermal transfer at much lower mass flow levels. And as it is acknowledged that the fluid-cooled system is typically utilized where massive heat loads or large power densities must be dissipated because of its ability to transfer heat out of the battery while the air cooling technique needs a much high flow rate. Although air cooling has advantages such as weight, low cost, and ease of maintenance, it is not suitable for batteries operating under abusive operating conditions like high discharging level or high ambient temperature due to air's poor heat transfer characteristics. The most common disadvantage in the liquid cooling system is that it can supply small amounts of liquid in comparison to the almost infinite volume of air that can circulate into a cell. The fluid Cooling tube is in charge of transferring heat from the battery with heavy heat degrees to the fluid used in the temperature control system. The reliability of these parts is critical to the efficiency of the fluid system. The battery cooling mechanism depends on supplying the motor pump with a 12V DC source and it is used to give the ability to the pump to transfer liquid over the transmitting tube from the battery to the circumstance of the battery. We also wired the data transmitters to the microcontroller and the LM35 temperature sensor to the dc power supply. The cooling mechanism is regulated using Arduino software. As a result, the battery can operate within standard operating conditions in this battery cooling system. We also attached various loads at different times to observe the battery as it was discharging. The cooling system is utilized to maintain the temperature under control. Two pumps are being employed in the battery cooling device to move liquid through one side towards the other, while the second pump is being employed to drain liquid into the tank. And we used to keep tracking the battery's proper functioning by using the battery managing systems monitor so the all the temperature degrees, voltage values, and current values, and power level inside each battery cell inside the battery pack. By using the fluid motor pump that is considered an essential part of the battery control units we were able to regulate the liquid flow rate based on the battery cell's temperature value. The plate of metal which is connected to the top of the battery acts as a transmitter and as a rapid cooler for improving efficiency.

In our study, we employed a light bulb as a load and we chose it to be at a high watt rate so it can drain a good amount of energy out of the battery to observe how good is the fluid cooling system while it's working on cooling down the battery's temperature. The operating temperature of Li-ion battery should be kept between 20°C and 40°C. Operating at higher temperatures deteriorates the performance, lifespan and safety of Li-ion batteries and may endure thermal runaway under extreme conditions [9].

The time that light bulb we have chosen before being fully empty in:

Time = (7.5 AH/ The flow of current inside bulb /0.85) ^1.2)

And we divided the current over 0.85 because the duration of transforming direct current to alternative current power is approximately 85% efficient, so the amps ofthe light bulb should be divided by 0.85 to achieve the proper amp value from the battery.

Now with this formula, we can do the calculation of the discharging time of the load in connection with the battery.

There is no need to discharge the battery out. After discharging 50% of the charge, the battery will be reset to charge with the charging circuit. There are several techniques for calculating a battery's state of charge (SOC).

A. *Coloumb counting technique*

The coulomb counting technique, also known as ampere-hour testing and current integration, is the most commonly used method for determining SOC [10]. This system determines SOC values based on battery current readings that are numerically synchronized over the consumption time period and we can calculate its values by

$$\mathrm{SOC(t)} = \mathrm{SOC(t-1)} + \int_0^{\mathrm{t}} \frac{1}{\mathrm{C_{bat}}} d\mathrm{t} \quad (1)$$

A working battery's releasable limit (Crelease) is the discharged limit until it is fully released. Similarly, the SOC is described as the level of the releasable limit in comparison to the battery rated value (Cr) provided by the manufacturer [10].

$$SOC = (Crelease/Cr) * 100\% \quad (2)$$

The maximum releasable limit (Cmax) of a fully charged battery is not always the same as the appraised limit. In general, Cmax differs from Cr to some degree for a newly used battery and decreases with use time. This calculation can be used to calculate a battery's SOH.

$$SOH = (Cmax/Cr) * 100\% \quad (3)$$

Where Crelease is the maximum amount of current that can be produced. The differentiation of the D (t) in a working cycle is achieved by utilizing a deliberate charging-discharging current (Ib) where D (t) can be determined by

$$\Delta D = \frac{\int_t^{t+1} I_b(t).D(t)}{C_r} 100\% \quad (4)$$

Where Ib denotes battery current, which is negative when discharging and positive when charging and for calculating D in means of time we should use the following equation

$$D(t) = D(t_0) + \Delta D \quad (5)$$

The working proficiency denoted as (n) is taken into account to increase measurement accuracy so D becomes,

$$D(t) = D(t_0) + \eta \Delta D \quad (6)$$

While (n) is equal to (nd) during releasing stage and is equal to (nc) during the charging stage the SOC can be communicated as

$$SOC(t) = SOH(t) - D(t) \quad (7)$$

As we noticing from fig [3, 4] when the battery runs at a higher temperature, the battery performs optimally. However, this comes at an expense, since the battery's performance and lifetime are reduced.

The requisite amount of current would not be produced if the device was run at a low temperature [11]. As a result, to avoid adverse temperature effects, a battery thermal management system (BTMS) is required to maintain the proper temperature range and minimize the temperature gradient of these batteries [12]. And we also notice that the area where the battery's life and power intersect is where the battery performs most effectively.

IV. RESULTS

As we explained before, the performance of the battery in the case of charging and discharging can be highly affected by the temperature. So we aimed to gain the optimum performance of the battery by using an efficient and low-cost technique that can do the voltage balancing between battery cells and the observation and controlling of the battery pack.

The simulation that we did on MATLAB / SIMULINK is depicted in Fig.6. In this simulation, we managed to employ a motor to work as a load, and the water flows via pipes from a powered pump, increasing the flow rate as the battery temperature rises.

From the Fig.7 we can inspect three parameters that are related and complementary to each other so they can do the operation of controlling the battery pack's temperature. Whenever we see incensement in the pump power values we can declare that the system is in needs to be cooled down so the battery can operate optimally.

Fig.8 shows the cooling device model used in our study. We used water as a cooling liquid for its ability to transfer heat through it. And we also used a pump to do the water transferring from the tank through the tubes to the battery pack. Additional modifications are to be considered to further decrease the temperature in order to increase the lifetime of batteries and decrease the disparity between different batteries in the pack [13].

In this study, a comparison to inspect what are the differences between battery that operates with cooling system and with one which operates separately, we also estimated the battery heat degree dependency. In the above figure, the orange line the represents the battery that operates while using a cooling system is showing better results when time moves over and the opposite situation happens while not using the cooling system. In this study, we used two 9W DC bulbs with equal ratings.

As the battery temperature exceeds thirty degrees Celsius, the cooling mechanism steps cool the battery pack down to the optimum degrees.

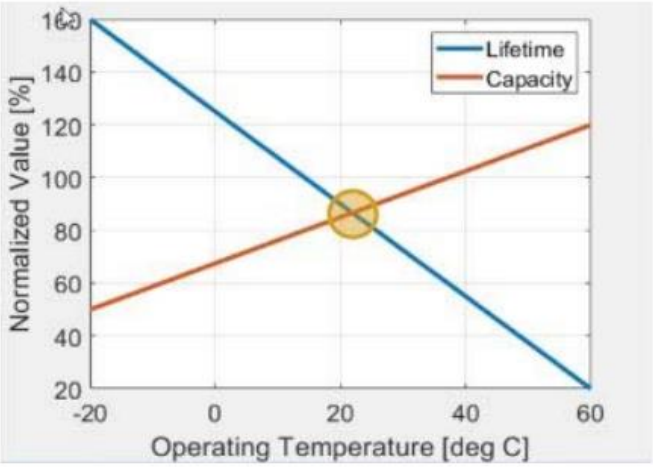


Fig. 3. Output characteristics of a battery

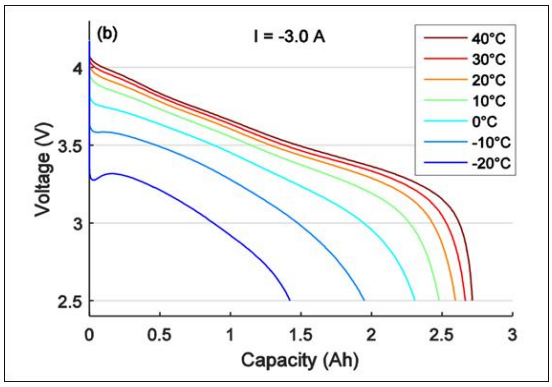


Fig. 4. Discharging the voltage of a Li-ion cell and temperature changing

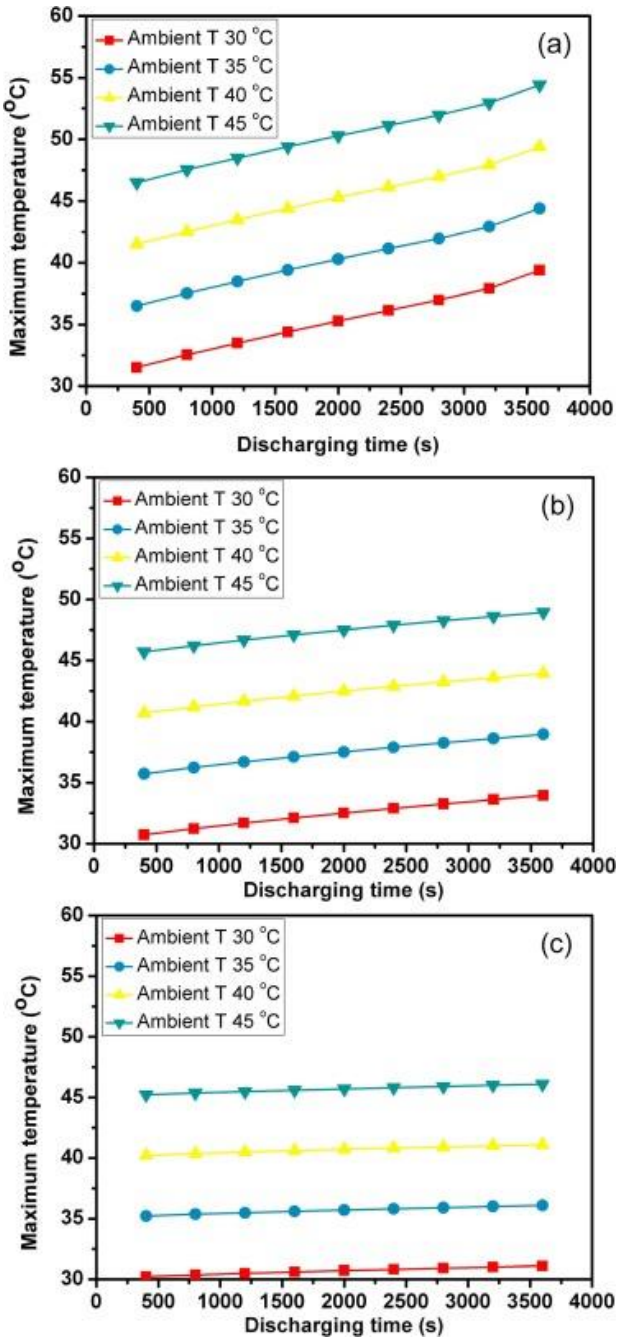


Fig. 5. The overall battery temperature varies in means of time at different ambient temperatures and the discharging rate of (a) 1 C, (b) 0.7 C, and (c) 0.4 C.

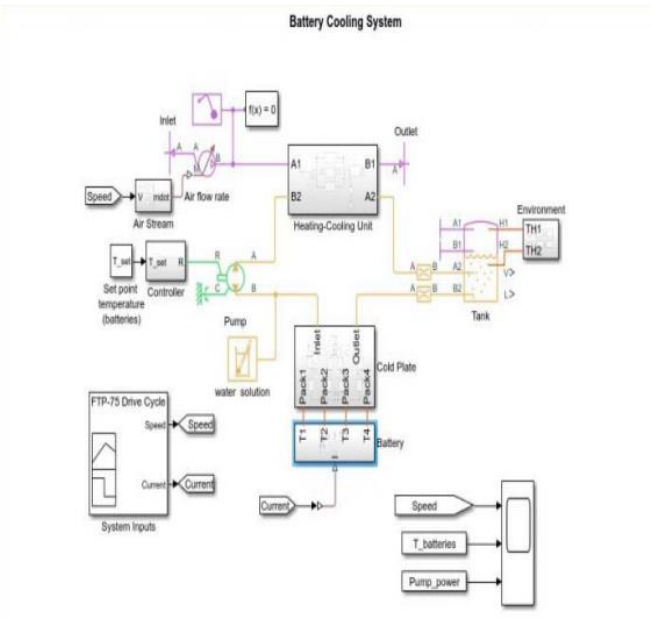


Fig. 6. The Matlab (Simulink) diagram of the Battery Management System

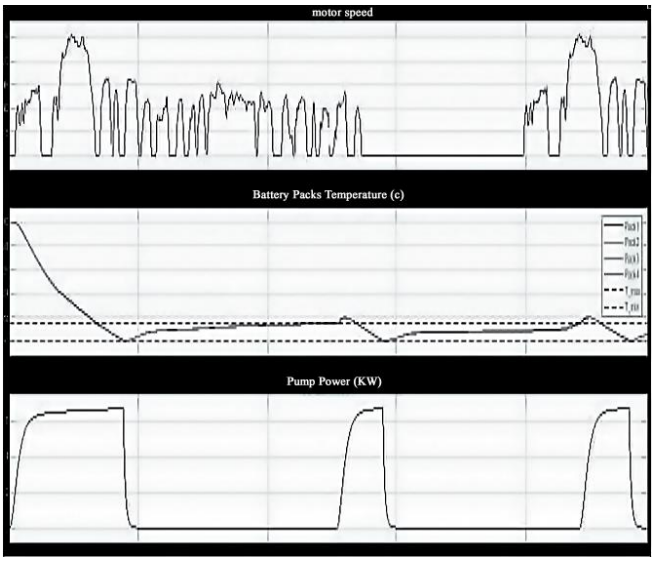


Fig. 7. Simulation Results

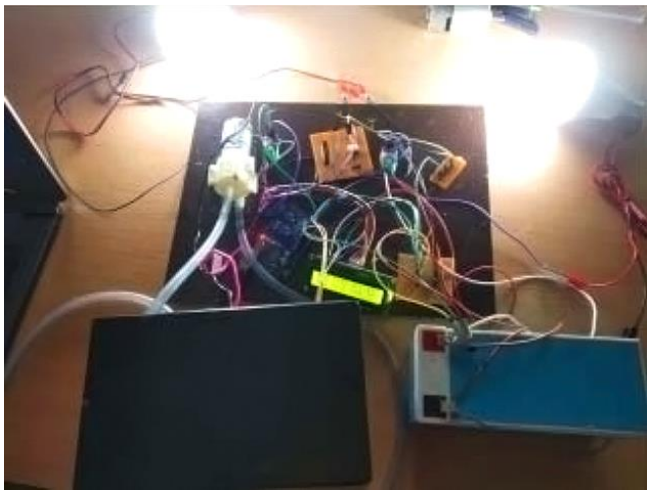


Fig. 8. The cooling device model

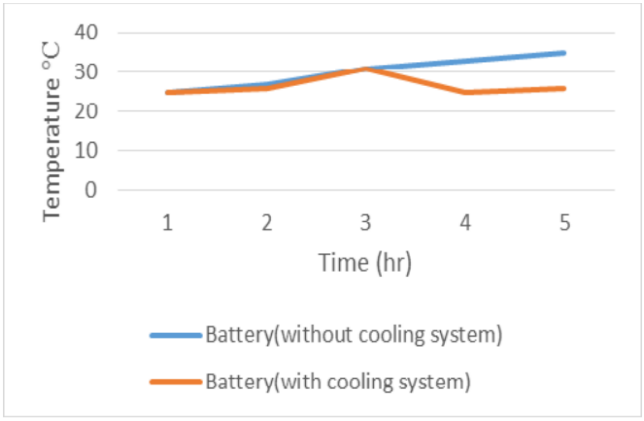


Fig. 9. Comparison between the battery characteristics while using the cooling system and while not using it

V. CONCLUSION

This study proposed a technique for modeling and improving the endurance of a battery by using a motor pump and cooling plates. We used the cooling plates as a heat reducer so the temperature of the battery pack can return to the optimum temperature degrees, thus the mechanism is used to release the unwanted heat generated by the battery. And we also observed the battery thermal behavior and we put it in a comparative study the alternative model solution changed the cooling layer structure even further. The cooling plates are designed to reduce the excess heat produced by the battery system during vehicle operation or in the process of charging or discharging. The regulation of the battery's temperature could be quite effective and inexpensive. Therefore, a liquid-cooled plate would circulate the liquid that is associated with the battery's outer structure in tubes. The cooling plates are circulated with the aid of the pump, which wants to limit heat transfer and preserve the temperature levels of the battery to the optimum thermal operation degrees.

REFERENCES

[1] X. Yang, Y. Song, G. Wang, and W. Wang, "A Comprehensive Review on the Development of Sustainable Energy Strategy and Implementation in China," in *IEEE Transactions on Sustainable Energy*, vol. 1, no. 2, pp. 57-65, July 2010, DOI: 10.1109/TSTE.2010.2051464.

[2] M. Hartmann and J. Kelly, "Thermal Runaway Prevention of Li-ion Batteries by Novel Thermal Management System," 2018 IEEE Transportation Electrification Conference and Expo (ITEC), 2018, pp. 477-481, DOI: 10.1109/ITEC.2018.8450177.

[3] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[4] W. Golubkov, B. Brunnsteiner, et al., "Thermal runaway of large automotive Li-ion batteries", *RSC Advances*, vol. 8, pp. 4017240186, 2018.

[5] Mengyao Lu, Xuelai Zhang, Jun Ji, Xiaofeng Xu, Yongyichuan Zhang, Research progress on power battery cooling technology for electric vehicles, Journal of Energy Storage, Volume 27,2020,101155, ISSN 2352-152X

[6] Xinke Li, Jiapei Zhao, Jinliang Yuan, Jiabin Duan, Chaoyu Liang, Simulation and analysis of air cooling configurations for a lithium-ion battery pack, Journal of Energy Storage, Volume 35,2021

[7] You Lyu, Abu Raihan Mohammad Siddique, S. Andrew Gadsden, Shohel Mahmud, Experimental investigation of thermoelectric cooling for a new battery pack design in a copper holder, Results in Engineering, Volume 10,2021

[8] M. R. Cosley and M. P. Garcia, "Battery thermal management system," INTELEC 2004. 26th Annual International Telecommunications Energy Conference, 2004, pp. 38-45, DOI: 10.1109/INTLEC.2004.1401442.

[9] R. Rizk, H. Louahlia, H. Gualous and P. Schaetzel, "Passive Cooling of High Capacity Lithium-Ion batteries," 2018 IEEE International Telecommunications Energy Conference (INTELEC), 2018, pp. 1-4, doi: 10.1109/INTLEC.2018.8612368.

[10] M. R. Cosley and M. P. Garcia, "Battery thermal management system," INTELEC 2004. 26th Annual International Telecommunications Energy Conference, 2004, pp. 38-45, DOI: 10.1109/INTLEC.2004.1401442.

[11] Ma Zi-lin, Mao Xao-jian , Wang Jun-xi, Qiang Jia-xi, and Zhuo Bin, "Research on SOC estimated strategy of Ni/MH battery used for a hybrid electric vehicle," 2008 IEEE Vehicle Power and Propulsion Conference, 2008, pp. 1-4, DOI: 10.1109/VPPC.2008.4677462.

[12] S. Chowdhury, M. N. Bin Shaheed, and Y. Sozer, "An Integrated State of Health (SOH) Balancing Method for Lithium-Ion Battery Cells," 2019 IEEE Energy Conversion Congress and Exposition (ECCE), 2019, pp. 5759-5763, DOI: 10.1109/ECCE.2019.8912932.

[13] Jaewan Kim, Jinwoo Oh, Hoseong Lee,Review on battery thermal management system for electric vehicles,Applied Thermal Engineering,Volume 149,2019

[14] R. Rizk, H. Louahlia, H. Gualous and P. Schaetzel, "Passive Cooling of High Capacity Lithium-Ion batteries," 2018 IEEE International Telecommunications Energy Conference (INTELEC), 2018, pp. 1-4, doi: 10.1109/INTLEC.2018.8612368.

Modeling of Windmills for Improving Voltage Stability in Distribution Network

Wesam Anis Elmasudi
Electrical-Electronics Engineering
Karabuk University
Karabuk, Turkey
wesamanis806@gmail.com

***Abstract*— The most important factor in the power system is to provide stable and smooth electricity to the consumers in front of the big increase in the usage of the renewable energy, especially, wind power farms. This paper will study the effects of wind energy units on voltage stability in distribution networks. We will consider that the wind farms are connected to different locations of the unit to see how far the contribution of wind farms on the voltage stability is.**

Keywords*— *voltage stability, distribution system, penetration level, buses

I. INTRODUCTION

Nowadays, power systems are extremely huge, and contain hundreds of generators, transmission lines, transformers, and loads. All of those components are connected through thousand of bus bars. The more increase of loads, the more electric power need to be generated.

The voltage instability issue might be occurred in distribution or transmission systems or in both. For that, the problem of voltage instability in distribution units is considered very important [1, 2].

In some Distribution systems there might be small generators connected directly to these networks to generate low level voltage. Electrical engineers call these small generators the distribution generators. Usually, the wind turbines, thermal, and photovoltaic plants are called distribution generators[4,5].

When distribution generators are Connected to a distribution network, that could effect the system's performance regarding to the location and rating of the generators, and there are tow sides of the affects[6], good affects distribution generators can drop the power losses, improve power quality, and voltage magnitude[7,8]. Bad side, distribution generators or some types of it might cause voltage stability problems due to their variable output, such as solar energy converters and wind farms[9,10]. Wind farms effects sudden changes in the injected power into the system, because the power output from its generators can change rapidly on time. If the generation were low, there would be a voltage drop at the end of the distribution feeder. While the high generation would cause over voltage. All of that means voltage instability problems[11].

This paper aims to provide explanations of the impact of wind farms on distribution networks' voltage stability. A radial distribution network were suggested, and wind farms were connected to different nodes at different buses. A voltage collapse proximity indicator M, based on network load ability is used to find out the affect of wind farms on voltage stability. Powerworld® simulator was used to study the case.

II. VOLTAGE STABILITY INDEX

In this paper the voltage stability index L was created using a simple power system as shown in Fig. 1. [12]. From Figure (1). P, and Q can be written as for single phase:

$$\mathrm{P_{source}} = (\mathrm{P_s^2} + \mathrm{Q_s^2}) \cdot \frac{\mathrm{R}}{\mathrm{V_s^2}} + \mathrm{P_{load}} \quad (1)$$

$$\mathrm{Q_{source}} = (\mathrm{P_s^2} + \mathrm{Q_s^2}) \cdot \frac{\mathrm{X}}{\mathrm{V_s^2}} + \mathrm{P_{load}} \quad (2)$$

Regarding to the above equations:

Let assume that P.source and Q.source as variables, the above equations are quadratic in form and for Ps and Qs have real roots, given by:

$$[(\mathrm{X} \cdot P_L - \mathrm{R} \cdot Q_L)^2 + \mathrm{X} \cdot Q_L + \mathrm{R} \cdot P_L] \cdot 4 < 1 \quad (3)$$

From equation number (3) :

$$[(\mathrm{X} \cdot P_L - \mathrm{R} \cdot Q_L)^2 + \mathrm{X} \cdot Q_L + \mathrm{R} \cdot P_L] = \mathrm{L} \quad (4)$$

Where L can be defined as the voltage stability index. The closer the L to the unity 1.0 the closer the system to the voltage drop off point. The authors [13] in found that the single phase representation did not represent the actual system, and to solve this problem the L should be:

$$[(\mathrm{X} \cdot P_L - \mathrm{R} \cdot Q_L)^2 + (\mathrm{X} \cdot Q_L + \mathrm{R} \cdot P_L) \cdot \mathrm{V_s^2}] \cdot \frac{4}{\mathrm{V_s^4}} = \mathrm{L} \quad (5)$$

Where this equation can defined the L at any node. [14] The voltage stability index L also can be defined as the following ratio (7):

$$\mathrm{L} = \frac{Z_{SEQ}}{Z_{LEQ}} \quad (6)$$

Z.SEQ: Equivalent impedance for the system.

Z.LEQ: Equivalent load impedance for the load.

If the stability index approaches 1 p.u, that means the system is closer to the voltage collapse point or the system will be unstable.

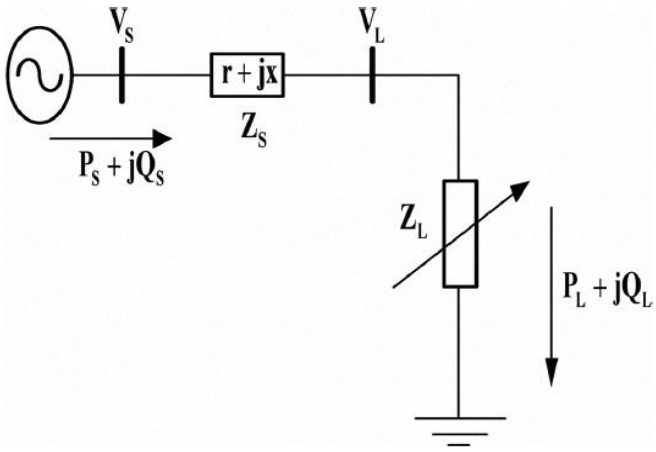


Fig. 1. A single-line system

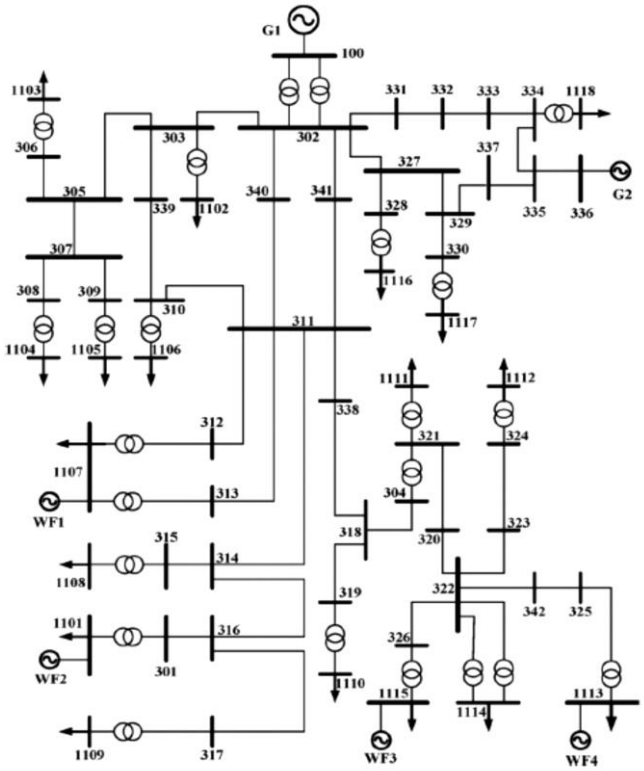


Fig. 2. A 61-bus radial sidtribution network with connecting 4 wind farms

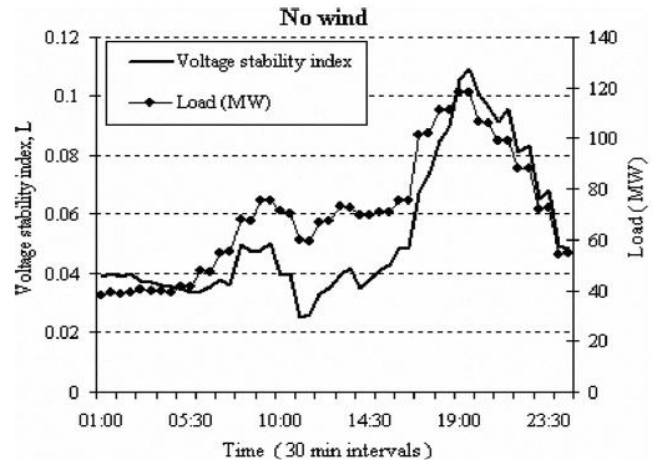


Fig. 3. Voltage stability idex of 61-bus network without wind generation

III. Testing the Radial Bus Distrubution System

A bus radial distribution network was simulated in Powerworld®, and it was used as the test system [15]. The (Fig. 2) shows bus radial distribution system with two thermal generators which supply power to the 18 load points through 132/33/ kV substation. The voltage level at the loads is 11 kV and the total load is 118 MW. The total generation capacity is 185 MW and the sending end voltage at Bus 100 and at Bus 336 is set to be 1.0 p.u. The Wind stations were connected at different buses at different penetration levels of wind generation with different scenarios, and the capacity of each wind farm was 65 MW.

IV. The Simulation Model

The simulation was done using Powerworld® utilizing with time-stop simulation option, where inputs can be varied at any time of the simulation window. Wind turbines were connected to the distribution system at different locations and at different MW outputs. The different wind generation are:

S1: 1 wind farm connected at bus 1107.

S2: 2 wind farms connected at bus 1107 and 1115.

S3: 4 wind farms connected at bus 1101, 1107, 1113 and 1115 respectively.

All wind farms' outputs were varied every 30 minutes to behave exactly like real wind farm under variable speed of wind, and the generation was varied between 15% and 30% of the total connected load. The voltage stability index L is calculated for each time step.

V. Simulation Results

Simulation results were concluded through two steps :

A. No windmills were connected

The presented results in Fig.3. were for a 24-hour period. The voltage stability index L of the network was calculated for every 30 minutes of the simulation by the equation (7). Figure 3 shows a plot of the load (MW) and the voltage stability index L when no wind generation was connected to the network. The maximum value (0.109) of L was recorded at peak load.

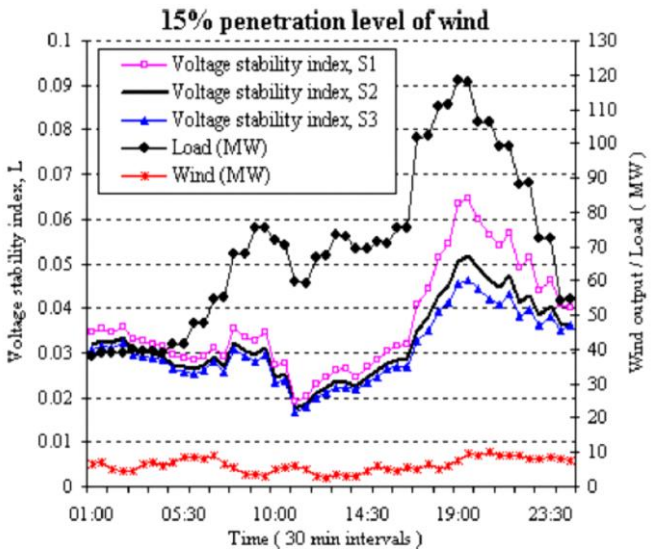


Fig. 4. Effects of wind generation on voltage stability index at a 15% penetration level of wind generation

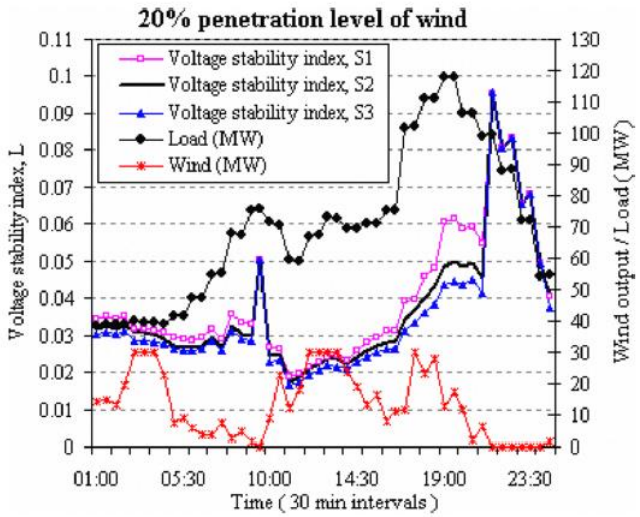


Fig. 5. Effects of wind generation on voltage stability index at a 20% penetration level

B. The windmills were connected in two different penetration levels at (15% and 20%)

The first wind generation was connected to bus 1107 (Sl) at penetration level (15%). Also wind generation was connected to bus 1115 1107 (S2) at the same penetration level. In the third scenario, wind generations were connected to buses 1101, 1107, 1113 and 1115 respectively (S3) with penetration levels at 15%. The corresponding voltage stability index L was recorded for S1, S2, and S3. The computed values of L for the scenarios S1, S2, and S3 are shown in Fig.4. for a 15% penetration level. The aim of connecting windmills at different " points and penetration levels " was to find out the effect on the voltage stability of the system. The value L dropped down with connecting the wind farm from (0.1) for no wind generation to (0.046) for case S3, (0.051) for S2 and (0.063) for Sl as shown in Fig. 4. Fig. 5. shows the index L for penetration level of 20%, and the plots for the voltage stability index L at a 20% wind penetration level was shown. It can be noticed that the voltage stability value was more stable for higher wind penetration levels. At 20% penetration level the index L went down to (0.043) for case S3, (0.049) for S2 and (0.061) for Sl as shown in Fig.4.

The results showed that for both penetration levels of wind generation the highest value of the index L was not related to the penetration level directly of wind generation; although, the voltage stability might be improved by connecting windmills by comparing L in Figure.4. to corresponding values for the 20% penetration level.

VI. CONCLUSIION

The index, of the voltage stability (L), for both penetration levels were analyzed, and the results did show an improvement in the voltage stability of the radial distribution system for higher penetration levels of wind generation. Although, the improvement did not show a direct relation to either the penetration level or the location of the wind generation. As the distribution network is expanding, this method that been showed could be used to ensure compliance with voltage stability limits in the network.

REFERENCES

[1] R.B. Prade and LJ. Souza, "Voltage stability and thermal limit:constraints on the maximum loading of electrical energy distribution feeders," lEE Proceedings-Generation, Transmission and Distribution,vo1.l45, Issue 5, pp.573-577, September 1998.

[2] Haiyan.Chen, Jinfu.Chen, Dongyuan.Shi, ianzhong.Duan, "Power flow study and voltage stability analysis for distribution systems with distributed generation," IEEE Power Engineering Society General Meting, June 2006.

[3] Thomas. Ackermann, Goran. Andersson, Lennart. Soder, "Distributed generation: a definition," Electric Power Systems Research, vo1.57, ppI95-204, December 2000.

[4] J.V. Milanoic, T.M. David., "Stability of distribution networks with embedded generators and induction motors," IEEEIPES Winter Meeting, 2002.voI.2, pp.1023-1028.

[5] "Technical requirements for connection of dispersed generating systems operating in parallel on the distribution network," Document CIO/II of the FPE/BFE, May 2002.

[6] V.Thong, J.Driesen, R.Belmans, "Transmission system operation concerns with high penetration level of distributed generation, UPEC 2007".

[7] T.K.A.Rahman, S.R.A.Rahim, LMusirin, "Implementation of embedded generation for voltage regulation and loss minimization in distribution system," International Journal of Engineering and Technology, vol.l , no.! , 2004, pp.!-12 .

[8] S.Conti, S.Raiti, G.Tina, "Small-scale embedded generation effect on voltage profile: an analytical method," Proc.IEE Gen.Trans.Dist, vo1.l50, no.J , 2003, pp.78-86.

[9] Le.Thu Ha, T. K. Saha, " Investigation of power loss and voltage stability limits for large wind farm connections to a subtransmission network," in Proc.2004, IEEE Power Engineering Society General Meeting ,voI.2, pp.2251-2256 .

[10] V.Akhmatov, P.B.Eriksen, "A Large wind power system in almost island operation-a danish case study," IEEE Transaction on Power System, vo1.22, no.3, August 2007.

[11] S.N.Liew, G.Strbac, "Maximising penetration of wind generation in existing distribution networks," lEE Proc-Gener.Transm.Distrib, vo1.l49, no.3, May 2002.

[12] G.B. Jasmon, Lee, L.H.C.C, "New contingency ranking technique incorporating a voltage stability criterion, .. lEE ProceedingsGeneration, Transmission and Distribution, vol. 140, no 2, March 1993.

[13] Liu. Jiang, Bi. Pengxiang, "The reduced analysis and optimization for distribution network," Electric Power Publishing company in Beijing, China, 2002.

[14] Chebbo, MJrving and M. Sterling, "Voltage collapse proximity indicator: Behaviour and implications," lEE Proc, Pt. C, vol 139, no. 3, May 1992, pp.241-252.

[15] United Kingdom Generic Distribution System. http://monaco.eee.strath.ac.uk/ukgds/ ,2006.

Design and Simulation of 2.4 GHz Microstrip Antenna

Ahmet Can Çakır
Department of Electrical and Electronics Engineering
Karabuk University
Karabuk, Turkey
2017010215058@ogrenci.karabuk.edu.tr

Cihat Şeker
Department of Electrical and Electronics Engineering
Karabuk University
Karabuk, Turkey
cihatseker@karabuk.edu.tr

***Abstract*— As a result of developments in communication systems in recent decades, the need for smaller, more lightweight, and higher-performance antennas has increased. One of the leading antenna types that can meet these needs is microstrip antennas. They provide many advantages such as their small size, easy to manufacture, and low cost. In addition to these advantages, they also have weaknesses such as low bandwidth. In this study, a rectangular microstrip patch antenna operating at 2.4 GHz resonance frequency is constructed. The antenna is designed on FR-4 substrate with a thickness of 1.6 mm and dielectric constant εr=4.4. It has three slots. Two on the patch and one on the ground plane. Desired patch antenna design is simulated by CST. The return loss of the designed antenna is –43 dB, and its bandwidth is 70 MHz.**

Keywords—2.4 GHz, microstrip patch antenna, bandwidth, CST Microwave Studio, return loss

I. INTRODUCTION

Antenna is a key device element in transmitting and receiving signals. Due to their appealing qualities such as light weight, easy fabrication, cheap cost, and compatibility with planar monolithic microwave integrated circuit (MMIC) components, microstrip patch antennas are preferred in wireless communication systems [1].

The most common band type used for microstrip patch antennas in home, office, and industrial applications is ISM (Industrial, Scientific, and Medical) band with 2400-2485 MHz. IEEE (Institute of Electrical and Electronics Engineers) the wireless network developed by WLAN (Wireless Local Area Network) the general name of the standard is IEEE 802.11 and the ISM wireless LAN operating in the 2.4 GHz band the standard is defined as IEEE 802.11b and IEEE 802.11g. Although there are the same differences between them, basically the 802.11 family uses the same protocols. In the literature, microstrip patch many studies have been carried out to increase the bandwidth and gain of antennas [2,4]. The essential microstrip receiving wire component involves a metal fix upheld over a bigger ground plane. The fix is normally printed on a microwave substrate material with relative permittivity in the range 2 to 10. Yet an assortment of materials might be utilized, contingent upon the application. Air or low-thickness froths normally offer the lowest loss and most elevated radiation productivity, but higher permittivity substrates result in smaller components with more extensive radiation designs [5]. The conducting patch is the key component of the microstrip antenna (MSA) that impacts antenna performance by modifying return loss, surface current distribution, band-width, impedance matching, harmonic suppression property and radiation pattern [6,7]. Essentially, the traditional structure of MSAs come about a metal radiating patch aspect that is on top of a grounded dielectric substrate of precise thickness [8].

II. DESIGN OF ANTENNA

In order to calculate the patch sizes of the antenna operating at the targeted frequency, several parameters must be determined beforehand. These are the antenna's resonance frequency ”fo”, the substrate thickness “h”, and the dielectric constant of the substrate material “εr” . In this study, FR-4 with relative dielectric constant εr=4.4, height h=1.6 mm are chosen as suitable substrate materials, and ground thickness is chosen as t=35 μm. In this study, it is aimed to reduce the return loss by keeping h, εr, fo as constant and by optimizing other parameters. With the specified parameters, the patch width (Wp) is calculated using equation (1) as follows,

$$W_p = \frac{c}{2f_0}\sqrt{\frac{2}{\varepsilon_r+1}} \quad (1)$$

Where:
c = free-space velocity of light.
f_o = resonance frequency.
ε_r = dielectric constant.

Since microstrip antennas do not have a homogeneous structure, it causes a change in the electrical transmittance value. ε_{reff} is calculated by equations (2) and (3).

$$\frac{W_p}{h} > 1 \quad (2)$$

$$\varepsilon_{reff} = \frac{\varepsilon_r+1}{2} + \frac{\varepsilon_r-1}{2}\left[1 + 12\frac{h}{W_p}\right]^{-\frac{1}{2}} \quad (3)$$

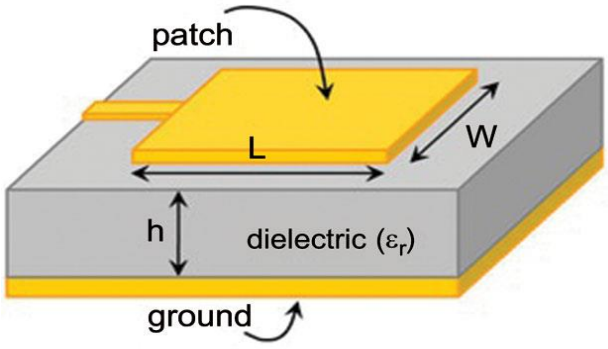


Fig. 1. Microstrip patch antenna

L_{eff} is the effective length of the patch and ΔL represents the length augmentation calculated by equations (4) and (5).

$$L_{eff} = \frac{1}{2f_r\sqrt{\varepsilon_{reff}}\sqrt{\mu_0\varepsilon_0}} \quad (4)$$

$$\Delta L = \frac{0.412h(\varepsilon_{reff}+0.3)\left(\frac{W_p}{h}+0.264\right)}{(\varepsilon_{reff}-0.258)\left(\frac{W_p}{h}+0.8\right)} \quad (5)$$

The reel length L_p of the patch is then calculated by the following equation (6).

$$L_p = L_{eff} - 2\Delta L = \frac{1}{2f_r\sqrt{\varepsilon_{reff}}\sqrt{\mu_0\varepsilon_0}} - 2\Delta L \quad (6)$$

As a result, Wp=38 mm, Lp=29.5 mm are found. The width of the ground plane is determined as Wg=76 mm and the length as Lg=59 mm. Microstrip feeding method is used as the feeding method and the length of the transmission line is optimized as 14.75 mm and the thickness as 3.147 mm. The width of the transmission line is determined by changing it according to the impedance match. Two symmetrical slots are made on the patch surface of the antenna. By changing the slot dimensions, the antenna is provided to operate at the desired resonance frequency and the return loss is reduced.

Another slot was opened on the ground plane. By changing the size of the slot opened on the ground plane, optimum value for the antenna performance was found. The length of the opened 17.93mm. The simulations of the designed antenna are carried out on the CST Studio Suite.

III. Results and Discussion

In the simulation of the designed microstrip antenna, optimized results were obtained by changing the slot dimensions and the thickness of the microstrip feeding line and by keeping other parameters constant. Results such as Return Loss, Gain, VSWR, Radiation Pattern were studied between 2 GHz and 2.8 GHz. Analysis results are shown with figures. The length of the slot was optimized by increasing from 1 mm to 59 mm by changing the length 1 mm in each step. The best performing result is obtained when the length of the slot is 17.93 mm. The return loss value is obtained

-44.78 dB, although the bandwidth is not very wide at the resonance frequency. It has been observed that the bandwidth at -10 dB is 70 MHz. The proposed antenna resonant ranges are between 2.36 MHz and 2.43 MHz. The mentioned results are shown in Table 2 and S-parameters shown in Fig.3.

It is shown in Fig.4 that the VSWR value of the designed antenna is 1.013 dB.

Radiation pattern, the antenna radiated is a graph showing the angular change of the power (electromagnetic field strength) at a fixed distance, which is created in the specific far area of the antenna. As seen Fig.5, for phi=90 at 2.4 GHz, the main lobe amplitude 4.7 dB and 3dB angular bandwidth (HPBW) for 107.3° and theta = 90 amplitude of the main lobe 0.778 dB and 3 dB angular bandwidth (HPBW) is 148.3°. The gain at resonance frequency 2.4 GHz is 4.702 dB. These values are powerful according to the literature.

IV. Conclusions

This paper made a review on improving the performance of the 2.4 GHz antenna. It has been observed that this antenna can be used in modern communication. The return loss has been measured to be quite efficient and its gain can be considered sufficient according to the literature. Furthermore, the bandwidth of the antenna is 2.91% of the resonant frequency.

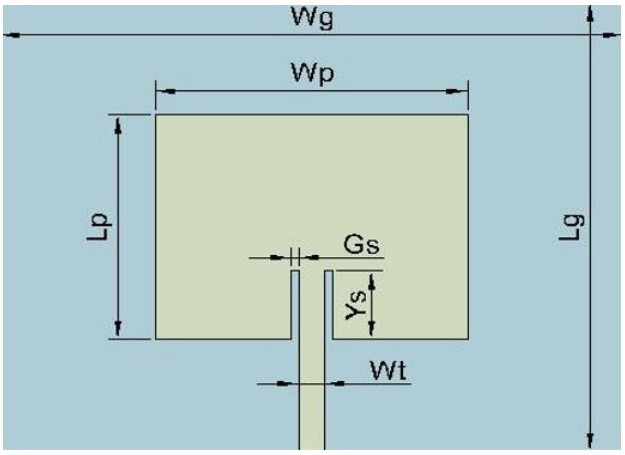


Fig. 2. Patch

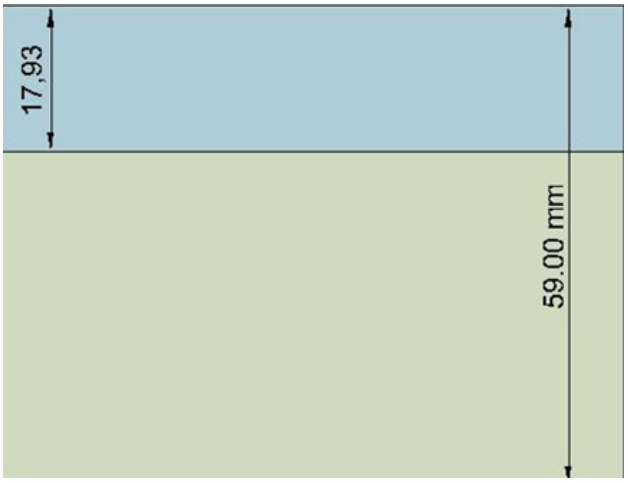


Fig. 3. Ground plane of antenna

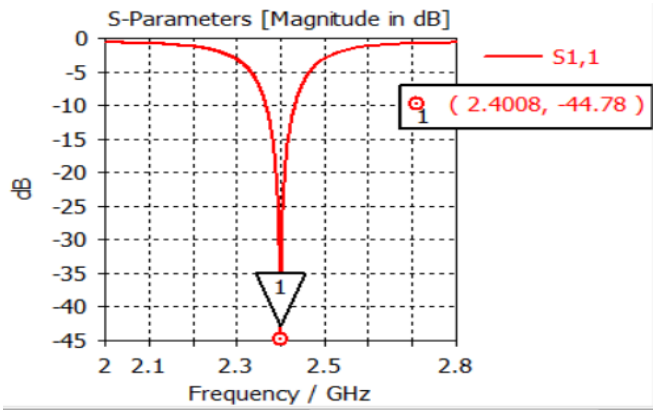


Fig. 4. S-Parameters

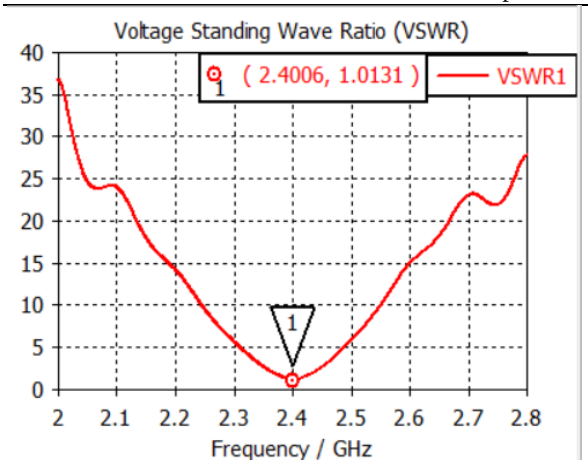
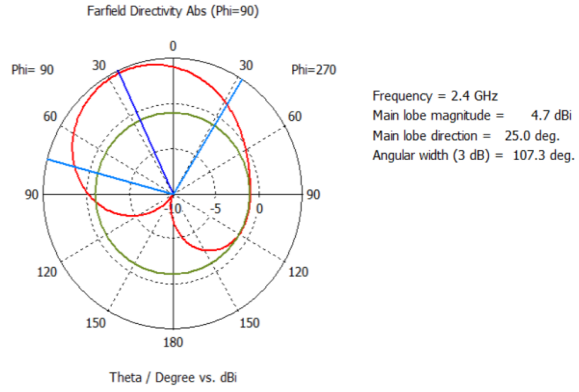
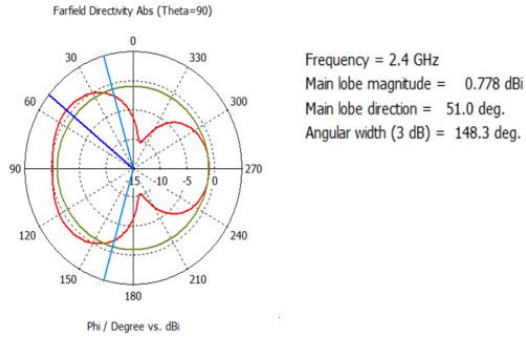


Fig. 5. VSWR simulation result



(a)



(b)

Fig. 6. a) phi=90 radiation pattern b) theta=90 radiation pattern

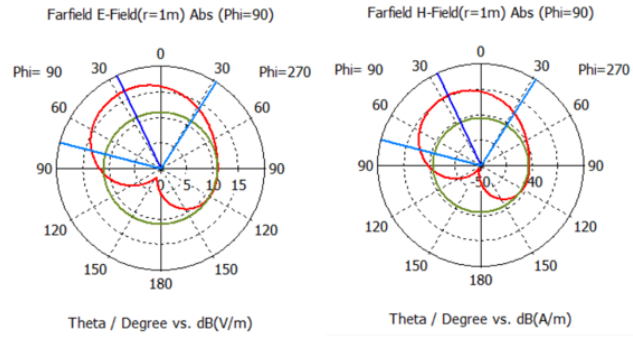


Fig. 7. Directivity at 2.4GHz E-plane and H-plane

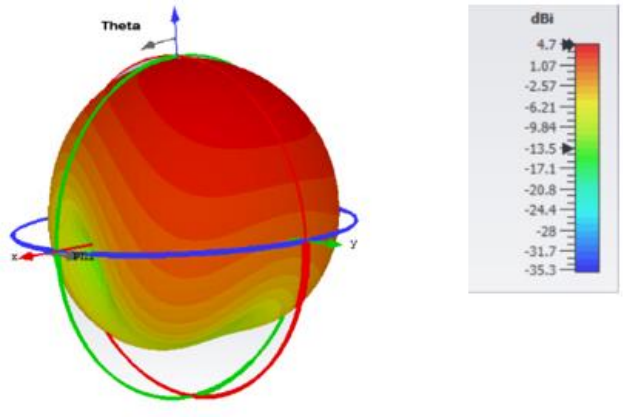


Fig. 8. Farfield of antenna

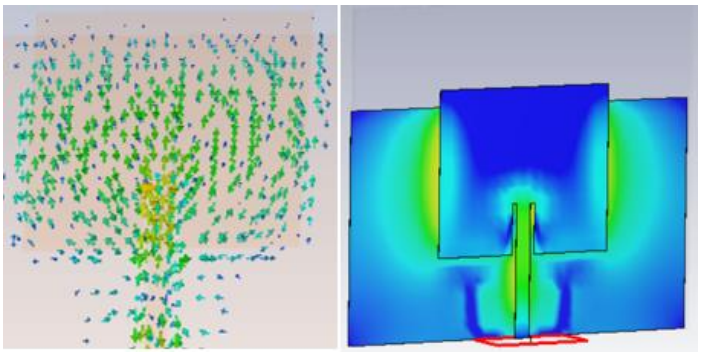


Fig. 9. Surface current at 2.4 GHz

TABLE I. ANTENNA PARAMETERS

parameter	value
fo	2,4 GHz
er	4,4
h	1,6 mm
Wg	76 mm
Lg	59 mm
Wp	38 mm
Lp	29,5 mm
Gs	0,93mm
Ys	8,97 mm
Wt	3,14 mm
t	0,035 mm

TABLE II. RETURN LOSS AND BANDWIDTH

Resonant frequency (GHz)	Return Loss (dB)	Bandwidth (MHz)
2.4	-44.78	70

TABLE III. DIRECTIVITY

Resonant Frequency (GHz)	Directivity in E-plane (dB)	Directivity in H-plane (dB)
2.4	4.702	4.702

REFERENCES

[1] W. A. E. Ali, E. K. I. Hamad, M. A. Bassiuny and M. Z. M. Hamdalla (2017) "Complementary Split Ring Resonator Based Triple Band Microstrip Antenna for WLAN/WiMAX Applications"

[2] C. Şeker and M. T. Güneşer, "Design and simulation of 26 GHz patch antenna for 5G mobile handset," 2019 11th International Conference on Electrical and Electronics Engineering (ELECO), 2019, pp. 676-678, doi: 10.23919/ELECO47770.2019.8990634.

[3] H. G. Akhavan and D. M. Syahkal, ―Study of coupled slot antennas fed by microstrip lines‖, 10th International Conference on Antennas and Propagation, Edinburgh, UK, vol. 1, pp. 1290–1292, 1997.

[4] R. Vaughan and J. B. Anderson, Channels, ―Propagation and Antennas for Mobile Communications‖, IEEE, London, 2003.

[5] Tansarıkaya, İ. (2007). Geniş Bandlı Yama Anten Tasarımı (Doctoral dissertation, Fen Bilimleri Enstitüsü).

[6] Wa'il, A., Shaaban, R. M., & Duffy, A. P. (2021). Design, simulation, and fabrication of a double annular ring microstrip antenna based on gaps with multiband feature. Engineering Science and Technology, an International Journal.

[7] Acıkaya, F. C., & Yıldırım, B. S. (2021). A dual-band microstrip patch antenna for 2.45/5-GHz WLAN applications. AEU-International Journal of Electronics and Communications, 141, 153957.

[8] Wa'il, A., Shaaban, R. M., & Tahir, A. (2020). Design, simulation and measurement of triple band annular ring microstrip antenna based on shape of crescent moon. AEU-International Journal of Electronics and Communications, 117, 153133.

Review on Size Reduction Techniques of the Microstrip Patch Antenna

Mustafa Ahmed Saadi
Department of Electrical and Electronics Engineering
Karabuk University
Karabuk, Turkiye
mustafa.ahmed.saadi@gmail.com

***Abstract*— During the past years, the patch antenna had been studied and used extensively worldwide and with various types of wireless communication devices. The design of the patch antenna consists of three layers placed on each other. The first layer is called the patch which it made of metallic material. The second layer is the substrate which it made of dielectric material. The last layer is ground plane, it made of metallic material also. This type of antenna has some merits like ease of integration with electronic circuit components. Lately, the world of communications has witnessed a great development in terms of the inclusion of some devices, such as tablets, smart watches and mobile phones, on multiple technologies in addition to the basic function of these devices. Therefore, the urgent need to reduce the components of these devices is located. Some of the main techniques that have been recently studied by researchers for the size reduction of antenna are discussed in this paper. The most important of these techniques include making defects and slots in the ground plane, shorting and folding, material loading, and reshaping the antenna. Also, each technology was discussed separately, and the main defects of each technology and its advantages were presented, and the impact of each technology on the performance of the antenna was also highlighted.**

Keywords— patch antenna, miniaturization, bandwidth, dimensions, microwave frequencies

I. INTRODUCTION

Wireless communication devices such as cellular mobile phones, Radio Frequency Identification (RFID) systems, tablets, GPS devices, laptops, satellite phones, receivers, AM and FM radios are used on a daily basis and some of these devices are used by everyone. These devices are found everywhere at the present time and their usage is continuously increasing. The antenna, being a fundamental piece of wireless communication systems, performs a crucial function in expressing the overall performance of those systems. For this reason, an antenna for any wireless communication system must be carefully constructed so one can assure accurate system-stage performance.

Among diverse varieties of antennas, printed antennas have acquired widespread interest throughout the past few years due to their ease of integration with related electronics, and their low-profile nature, which make them to be very appropriate to be used in built-in wireless communication system components. This type of antenna is usually manufactured using printed circuit technologies. Printed antennas have been first offered throughout the 1950s. However, they did not gain a lot interest till the early 1980s. Since then, printed antenna theories have been developed by meticulously analyzing many printed circuit designs in order to better understand of their characteristics and performance. Microstrip patch antennas, printed monopoles, and dipoles are among the most common printed antennas.

Many standards of wireless communication technologies, such as Wi-Fi, LTE, 5th generation and other technologies, are determined according to microwave frequencies, in other words, within the range of 700 MHz to 36 GHz. Therefore, the traditional antenna length at the minimum frequency band is large, approximately 210 mm at 700 MHz, which is considered very large compared to the specifications of communication devices such as tablets, mobile phones and other devices. Therefore, the dimensions of antenna must be made smaller to fit the dimensions of wireless devices. Furthermore, most wireless devices need the usage of multiple antennas, especially for multiple inputs and multiple output technology. Thus, multiple antennas must be sized to fit in a specific space. Although the size of the antenna must be small, these antennas should maintain some of their characteristics such as the desired radiation and the desired frequency.

A lot of studies that published about the topic of miniaturization of antenna came to the conclusion that; When the antenna size is reduced, its bandwidth and gain change [1,2]. These studies are helpful in determining performance measures for miniaturized antennas. Lately, a lot of new miniaturized designs of antenna have appeared, such as the miniaturized designs of microstrip patch antenna and printed monopole antenna. [3–5].

II. MICROSTRIP PATCH ANTENNA

The microstrip patch antenna is a type of printed antennas. The antenna usually consists of three layers placed on top of each other, where the first layer consists of a conductive material called the patch, the second layer consists of an insulating material called the substrate, and the last layer consists of a conductive material also called the ground plane [6]. The antenna has different shapes, rectangular, circle, pentagonal, hexagonal, F-shape, etc. The use of this type of antenna has spread in many applications, including tablets and mobile phones, because it is easy to design, as a result of the study of this type of antenna by many researchers, the ease of its manufacture and integration with other electronic devices as a result of its planer geometry, an effective cheap choice for wireless applications, and low profile. The cavity model is typically used to analyze the patch antenna [7].

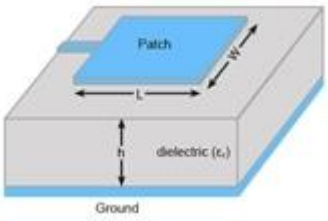


Fig. 1. Microstrip Patch Antenna

Microstrip patch antenna is considered as a cavity loaded with insulation with side walls of non-perfect electric conductor (PEC). Therefore, the radiation takes place from this cavity because of leakage from these side walls. The fields within cavities must be solved first, In order to determine the operation frequency and radiation characteristics of the patch antenna. The bottom and the top sides of the cavity are considered as PECs, while the sides are supposed to be perfect magnetic conductors (PMCs). By placing the suitable boundary terms on the walls of the cavity, the field distribution in the cavity could be found. Then, the result can be used to determine the radiation field of the antenna for various modes, and also to find the resonant frequency. From the same model, the quality factor and the input impedance can be found.

III. MINIATURIZATION TECHNIQUES

Antenna miniaturization techniques, including patch antennas, have been of interest to researchers for a long period of time. The first attempts to reduce the volume of the antenna were successful, and they came to the conclusion that when the antenna is reduced, it leads to reduce the gain and lower the bandwidth [1, 2, 8]. Basically, there are two methods to reduce the volume of the patch antenna. The first way is by changing the properties of the material of the substrate in order to reduce the effective wavelength in the region of the substrate. The second way is by changing the geometry of the microstrip patch antenna in order to increase the electrical size.

A. Material Loading

One of the easiest ways to make the antenna smaller is to increase the relative permittivity of the substrate. The square root of relative permittivity is inversely proportional to dimensions of the patch. The result of this method is decreasing the efficiency, lowering bandwidth, and increasing the excitation of surface wave. Changing the radiation properties and poor polarization purity are caused by the truncation of the ground plane. Different researches examine several kinds of material to get the suitable miniaturized antenna to the specifications of the wireless devices.

Microstrip patch antenna with high-relative permittivity of (10, 13) and a thick substrate was examined in [9]. It was found in this study that the values of radiation characteristics and the input impedance are not similar to the values of common patch antennas. By using a thin substrate, the input impedance is less than the antenna with the thick substrate. In [10], low-permittivity substrate is used that filled partially with high-permittivity. By using this approach, 50% of the antenna size was miniaturized with gain 6 dB and bandwidth of 10%.

Many researches have been done on the usage of ceramic substrates in patch antenna miniaturization. In [14], a 1/8 miniaturization was obtained using a ceramic substrate with $\varepsilon r = 100$ as compared to the conventional antenna that used a FR4 substrate. A substrate thickness equal to ($0.031\lambda o$) was used to eliminate the problem of narrow bandwidth. The performances of the antenna were a gain of 2.8 dBi and bandwidth of 7.2%. Lots of researches have also appeared in previous years that use different and modified materials as substrates in order to reduce the size of the antenna. As explained previously, the usage of different and modified substrates can provide a great size reduction with the cost of small bandwidth.

B. Shorting and Folding

The other size reduction technique is shorting posts and folding the antenna, and that lead to make the antenna electrically smaller [6]. The distribution of E-field has sinusoidal over the patch, where the E-field is at maximum amount at the edge and zero value at the middle. So, the antenna aperture could be reduced by putting the electrical wall at the center of the antenna. The resonant frequency and the Q-factor of this approach will be the same as the conventional antenna. However, this approach will reduce the directivity [6]. In [11], the antenna reduced to 1/8 of its size by folding it. The efficiency of the antenna was 90% and the bandwidth 4% was found as results of this approach. In [15], several parameters have analyzed. Multiple, double, single shorting posts were used. The size of the resultant patch antenna was 1/3 of the original patch antenna as a result of using the shorting posts.

However, this method of minimization comes with some disadvantages as it reduces the directivity and gain of the antenna. Furthermore, this method of miniaturization complicates the antenna design. But when this method is used correctly, the resulting antenna is very small with a little effect on its performance

C. Reshaping and Introducing Slots

The antenna can be made smaller by adding slots to the patch or changing its shape. By reshaping the patch, a large electrical length can be obtained fits the limited space. By making slots in the patch, a good efficiency can be obtained, but the bandwidth will reduce [5]. In order to overcome this problem, layers of conductors are used, and also this approach increases the gain and the bandwidth [12]. Where, the number of layer is directly proportion to the gain and the bandwidth. The usage of five layers improved the efficiency by 30%.

Many researches have shown that by making slots in the patch of the antenna, the antenna will be reduced in size. In [16], the size of the antenna was reduced by 40–75% by making slots in the patch of the antenna. By making identical slots in the patch of the antenna, the effect of this method by making the polarization poor will be reduced to its minimum. In general, this method does not have a design methodology. Although, it widely used by a lot of researchers and in many designs.

D. Modifications of the Ground Plane

By using this technology, the antenna can be made smaller by adjusting the ground plane. In order to reduce the size of the antenna, the size of the ground plane is reduced. Sometimes the reduction in size of ground plane a little bigger than the patch in order to get more reduction in the size of the overall antenna. Various studies [13, 17, 18] were analyzed and it was found that the miniature antenna was affected to its input impedance, and also had poor polarization purity. This caused by the edge diffraction, where the front lobe was decreased by the increment of the back lobe. Making slots and defects in the ground plane is one of the ways to amend the ground plane. The current path will increase inside the patch layer with the help of these holes [19]. This leads to a decrease in the resonant frequency which leads to size reduction. In [19], one slot of 1 mm was made in the ground plane, where the reduction in operational frequency was 52%, leads to a reduction in size of 90%.

IV. CONCLUSION

In this paper, an overview of the different kinds of size reduction techniques of patch antenna had presented. The theoretical side of the patch antenna was discussed. The main limits on some metrics were indicated. The most important techniques used to reduce the volume of the antenna and the most popular among the research community were discussed. It included the following technologies: the usage of untypical and modified substrate, inserting slots in the third layer of the antenna, modifying the antenna's shape, and folding and shorting of the antenna. Some of these methods provided a good size reduction, while others reduced the size by average manner in order to maintain some antenna characteristics at the lowest acceptable value. Some of these designs are easy and cheap to manufacture, while others are difficult and very expensive to manufacture. Such trade-offs between the performance of the antenna and the percentage of the size reduction will always exist, so the designer must choose the best technology for the application required to use such techniques. Therefore, there is an urgent need to clearly define how various factors affect antenna performance for a certain size reduction techniques. Also, there is an urgent need to clarify a physical view of the use of such techniques with different bands. Given these problems, it can be predicted that antenna size reduction techniques will remain the focus of researchers over the coming years.

REFERENCES

[1] Sievenpiper, D., Dawson, D., Jacob, M., et al.: 'Experimental validation of performance limits and design guidelines for small antennas', IEEE Trans. Antennas Propag., 2012, 60, (1), pp. 8–19

[2] Volakis, J.L., Chen, C., Fujimoto, K.: 'Small antennas: miniaturization techniques & applications' (McGraw-Hill, 2010, 1st edn.)

[3] Dong, Y., Toyao, H., Itoh, T.: 'Design and characterization of miniaturized patch antennas loaded with complementary split-ring resonators', IEEE Trans. Antennas Propag., 2012, 60, (2), pp. 772–785

[4] Ouedraogo, R.O., Rothwell, E.J., Diaz, A.R., Fuchi, K., Temme, A.: 'Miniaturization of patch antennas using a metamaterial-inspired technique', IEEE Trans. Antennas Propag., 2012, 60, (5), pp. 2175–2182

[5] Oraizi, H., Hedayati, S.: 'Miniaturization of microstrip antennas by the novel application of the Giuseppe Peano', IEEE Trans. Antennas Propag., 2012, 60, (8), pp. 3559–3567

[6] Garg, R., Bhartia, P., Bhal, I., Ittipiboon, A.: 'Microstrip antenna design handbook' (Artech House, MA, USA, 2001)

[7] Lee, K.F., Luk, K.M.: 'Microstrip patch antennas' (Imperial College Press, London, UK, 2011)

[8] Wheeler, H.A.: 'Fundamental limitations of small antenna', Proc. IRE, 1947, 35, no. 12, pp. 1479–1484

[9] Schaubert, D.H., Yngvesson, K.S.: 'Experimental study of a microstrip array on high permittivity substrate', IEEE Trans. Antennas Propag., 1986, AP-34, (1), pp. 92–97

[10] Lee, B., Harackiewicz, F.J.: 'Miniature microstrip antenna with a partially filled high-permittivity substrate', IEEE Trans. Antennas Propag., 2002, 50, (8), pp. 1160–1162

[11] Li, R., Dejean, G., Tentzeris, M.M., Laskar, J.: 'Development and analysis of a folded shorted-patch antenna with reduced size', IEEE Trans. Antennas Propag., 2004, 52, (2), pp. 555–562.

[12] Latif, S.I., Shafai, L., Shafai, C.: 'An engineered conductor for gain and efficiency improvement of miniaturized microstrip antennas', IEEE Antennas Propag. Mag., 2013, 55, (2), pp. 77–90

[13] Huang, J.: 'The finite ground plane effect on the microstrip antenna radiation patterns', IEEE Trans. Antennas Propag., 1983, AP-31, (4), pp. 649–653

[14] Kula, J., Psychoudakis, D., Liao, W.-J., Chen, C.-C., Volakis, J., Halloran, J.:'Patch antenna miniaturization using recently available ceramic substrates', IEEE Antennas Propag. Mag., 2006, 48, (6), pp. 13–20

[15] Waterhouse, R., Targonski, S., Kokotoff, D.: 'Design and performance of small printed antennas', IEEE Trans. Antennas Propag., 1998, 46, (11), pp. 1629–1633

[16] Kakoyiannis, C.G., Constantinou, P.: 'A compact microstrip antenna with tapered peripheral slits for CubeSat RF payloads at 436 MHz: miniaturization techniques, design, and numerical results'. IEEE Int. Workshop on Satellite and Space Communications (IWSSC08), October 2008, pp. 255–259

[17] Bhattacharyya, A.: 'Effects of finite ground plane on the radiation characteristics of a circular patch antenna', IEEE Trans. Antennas Propag., 1990, 38, (2), pp. 152–159

[18] Lier, E., Jakobsen, K.: 'Rectangular microstrip patch antennas with infinite and finite ground plane dimensions', IEEE Trans. Antennas Propag., 1983, AP-31, (6), pp. 978–984

[19] Sarkar, S., Majumdar, A.D., Mondal, S., Biswas, S., Sarkar, D., Sarkar, P.P.: 'Miniaturization of rectangular microstrip patch antenna using optimized single-slotted ground plane', Microw. Opt. Technol. Lett., 2011, 53, (1), pp. 111–115

Evaluation of IoT: Challenges and Risks on Communication Systems

Mostafa Alghentawi
Department of Electrical and Electronic Engineering
Karabuk University
Karabuk, Turkey
Mustafa.alghentawi@gmail.com

***Abstract*— Internet of Things (IoT) is a new-fangled prototype, which supplies a chain of new services/products for the upcoming technological innovations wave. IoTs' applications are roughly boundless in terms of enabling a smooth integration between the digital world and the physical world; where IoT can be implemented everywhere like smart (environment, city or businesses), security, smart business process, home automation, energy sector, education, healthcare and so on. Moreover, despite all the massive efforts of researchers, developers, experts to cover the full potential of IoT, there are still various problems and challenges need to deal with. In this survey paper, we will present a preface on some important aspects, applications and protocols with regards to the emerging area of IoT. This paper also will highlight the challenges of IoT might face, applications that have the possibility to achieve a fundamental change in human life, in addition to the risks of IoT and its impacts on our life in terms of privacy invasion and security issues. Moreover, SWOT Analysis will be conducted by identifying the Internal Factors of the IoT (Strength and Weaknesses) as well as the External Factors (Opportunities and Threats).**

Keywords*— *internet of things, vision and mission, IoT's architecture, implications of IoT, network protocols, challenges, risks, SWOT analysis

I. INTRODUCTION

The Internet has become ever-present, where it touched roughly each corner surrounding and affected human life in inconceivable paths. Today, the universe is getting into the Internet of Things era (famous as IoT). The 'IoT' expression has been founded in 1999 [1], whereas the earliest IoT principles have been published shortly after by Neil Gershenfeld in his book 'When Things Start to Think' [2]. Several authors have defined IoT as a term in different ways. Under [6], the authors have gone through two of the most popular definitions of IoT.

The first has defined simply as "an interactivity between the digital and physical worlds using a numerous number of actuators and sensors", while the other has defined as "A model in which networking and computing aptitudes are embedded at any kind of imaginable objects". The purpose of using these aptitudes is to know and control the status of the object or to alter its status if required; for achieving complex functions that need high intelligence.

A. Vision and Mission Statement

The vision statement concentrates on tomorrow (future) and what the organizations and industries want to ultimately become, while the mission statement concentrates on today and what the organizations or industries do and spend to achieve it. The purpose of displaying those statements is both of them are vital in directing goals in the organizations [7]. Here, we will display the vision and mission statement of three of the most top companies involved in IoT [8,9,10].

- Tesla

Vision: "to build the most persuasive vehicles company presently by driving the world's changeover to electric transportations."

Mission: "to speed up the world's changeover to green energy."

- Microsoft

Vision: "to assist persons and enterprises over the world recognize their complete potentials."

Mission: "to enable people and businesses on the earth for implementing more."

- Samsung

Vision: "Affect the world with our progressive products and technologies, and layout that emboss people's lives and contribute to social growth by designing a modern future."

Mission : "Samsung will devote the technology and human resources to set up top products and services that contribute to a benefidcent global society."

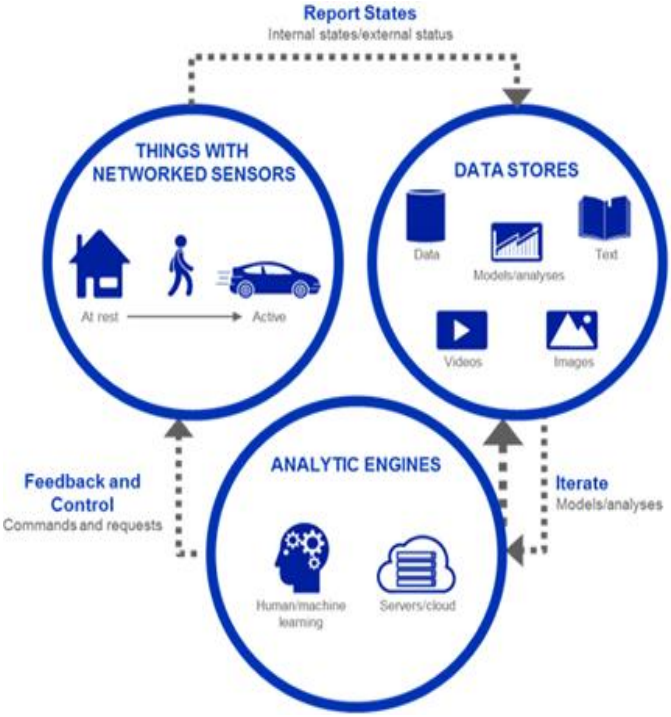


Fig. 1. The Data Processing Stage in IoT

TABLE I. THE BEST IOT COMPANIES IN 2018 [16]

Name	2018 CRN IoT Categories
SAP	IoT Software and Services
ARM	Iot Hardware
Google	Iot Hardware
Samsara	Iot Hardware
Nvidia	Iot Hardware
Fortinet	Iot Security
Siemens	Industrial IoT Providers
Cisco Systems	Iot Hardware
Cradlepoint	Iot Security
Schneider Electric	Industrial IoT Providers
Dell Technologies	Iot Hardware
Intel	Iot Hardware
Amazon Web Services	IoT Software and Services
Sierra Wireless	Iot Hardware
GE	Industrial IoT Providers
Eaton	Industrial IoT Providers
IBM	IoT Software and Services
PTC	IoT Software and Services
Qualcomm	Iot Hardware
Verizon	IoT Software and Services
Oracle	IoT Software and Services
AT&T	IoT Software and Services
SonicWall	Iot Security
Ayla Networks	IoT Software and Services
Hewlett Packard Enterprise	Iot Hardware
Honeywell	Industrial IoT Providers
Johnson Controls	Industrial IoT Providers
PAS	Industrial IoT Providers
ForeScout	Iot Security
Eurotech	Iot Hardware
Samsung	Iot Hardware
Vertiv	Iot Hardware

II. IOT REVOLUTION

According to Gartner Research [14], the number of connected things around the world is estimated to reach 14.2 ones thousand million and 25 thousand million in 2019 and 2021 respectivelly. Moreover, Gartner mentioned that the sensor's prices of IoT will be declined in 2019, which will give the means to the companies to use them in order to earn insights in different industries such as retail, energy, manufacturing and others.

In 2020, each of logistics and transportation, discrete manufacturing, and utility industries are separately planning to outlay more than $40 thousand million on IoT services platforms and systems [15].

Also, McKinsey forecasts that the IoT market in 2020 will be worth $581Billion with an annual growth rate ranging from 7-15%. In 2021, only the Industrial market is predicting to reach $123 Billion of IoT with an annual growth rate of 7.3% [15]. Table 1 shows the best IoT companies in 2018 and their specializations [16].

A. IoT Components

The mechanism of IoT is based fully on actuators and sensors apparatus, which ease the interaction with the physical material. The actuators are tools used for creating effects, these effects can make modifications or changes to the environment (Ex: the AC temperature controller), while the sensors are collecting the stored surrounding data and then processing these data intelligently for deriving beneficial inferences from it (Ex: a mobile phone can be considered as a sensor, provided that supply responses about its present status) [6]. Industries are using diverse types of sensors longly. Yet, the revolution of the IoT has taken the development of sensors into an altered level. The below points show the list of the most crucial sensors which extremely being used in the IoT world. For farther details, the explanation of each sensor and its uses can be found in [11].

- Sensors of Temperature
- Sensor of Chemical
- Sensors of Accelerometer
- Sensor of Proximity
- Sensor of Pressure
- Sensor of Smoke
- Sensor of Gas
- Sensors of Level
- Sensor of Water quality
- Sensors of Image
- Sensors of Motion detection
- Sensor of IR
- Sensors of Humidity
- Sensors of Accelerometer
- Sensors of Gyroscope
- Sensors of Optical

The second component is connectivity, where the collected data is transmitted to a cloud infrastructure over different mediums of transportations (Ex: Wi-Fi, cellular networks, Bluetooth, WAN (Wide-Area Networks, etc.,) [13]. The third component is data processing as shown in Fig. 1., after the cloud obtains the collected data, the software starts to process these data whether the data is simple or complicated (Ex: checking the reading temperatures on appliances if it within an appropriate range or identifying objects using visual devices) [13]. Finally, the last main component is the user, where the information can be available to the end user by triggering alarms on their phones or emails [13].

B. IoT's Architecture

IoT's implementation is relying on an architecture which consists of sundry layers ranging from the acquired data layer at the basis, to the application layer upward. The architecture layers are designed to meet the requirements of various organizations whether were private, public or governmental. The Fig. 2. is showing the common layered architecture of IoT. The layered architecture is divided into two separated parts at the top of the internet layer for serving the communication purpose of common media and using data in applications. The two layers at the bottom of the internet layer are contributing to capturing data [17].

- Application layer is accountable for the delivery process of various applications (such as logistics, healthcare, retail, manufacturing, etc) to the end IoTs' users.
- Middleware layer is accountable for essential functions such as information and managing device, beside its responsibility towards access control, semantic analysis, Object Naming Service, data aggregation, information discovery, filtering and information service. It can be run in bidirectional mode, so it is considered as the critical layer in IoT architecture.
- Access gateway layer is responsible for routing, diffusing and subscribing message, besides, it contributing to performing cross-platform communication if needed. This layer is considered as the initial stage of data handling.
- Edge layer is the layer of hardware, where it is comprising of embedded systems (Ex: information processing), sensor networks (Ex: information collection), radio-frequency identification tags (Ex: providing identification and information storage).

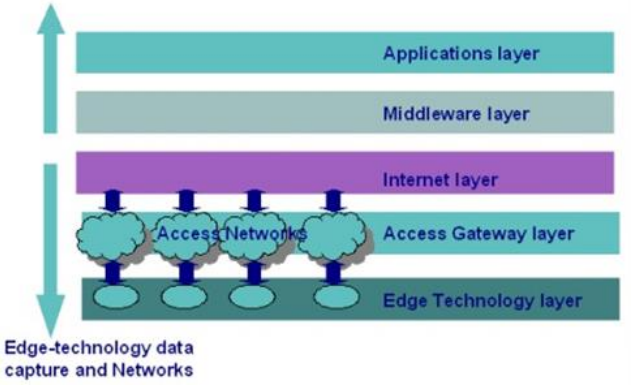


Fig. 2. The Main Layers of IoT Architecture

C. Software Architecture Options

According to [3,4,5], the systems of IoT are involving several trade-offs and design drivers. significant factors include cost, energy efficiency, update, security, communication latency and dynamic programmability. These factors are broadly determining the architecture options that will be shown in Figure 3. On the other hand, software architecture choices are divided into seven classes, ranging from the simple class to the most complicated one as following:

- Architectures of no-OS (Operating System)
- Architectures of language-runtime
- Architectures of server-OS
- Architectures of full-OS
- Architectures of app-OS
- Architectures of RTOS (Real-Time OS)
- Architectures of container-OS

D. IoT Security

Several papers and researches had been done with regards to the area of IoT security, some of them will be reviewed in this section. Hwang and Kim have declared that the standards of security are classified into six groups which they are: authorization, availability, authentication, confidentiality, non-repudiation and integrity. The consequences based on their research were the majority of previous works are dealing with the standards of authentication, authorization, confidentiality and integrity, but the studies on availability and nonrepudiation were insufficient [25]. The security requirements and elements have been mentioned in research conducted by Oh and Kim, these requirements are classified into three groups of IoT characteristics which are resource constraint, heterogeneity and dynamic environment, while the elements are IoT network, server, Platform, user, attacker and cloud [24]. Furthermore, Yun et al. have gone with a study on the method of interworking using Interworking Proxy Entity (IPE) between one-M2M and non-one-M2M systems by applying the OAuth 2.0 framework for the security issues [26]. Yet, there are few limitations that can be used like allowing people to intervene in some scenarios, especially in the process of issuing access token where the login or authorization code is needed. As known, IoT appliances are generally automated, and these appliances are integrated with the security process, while the consequence of appliance use will be limited if the security process is not automated. Therefore, the resource owner password credentials grant form can exceed this restriction in issuing access token. This grant form allows issuing access token with no further process that requires human involvement when the needed data are given in advance. So, only the trusted appliances can use this form, due to; the sensitivity of the resource owner's credentials [12].

E. Standards and Protocols

The greatest number of connected appliances through the internet is known with so-called machine-to-machine (M2M) systems; where the term of M2M is usually used to describe the exchanged information and its performance between the device and network without any assistance by humans.

Feature	Architecture option					
	No OS or RTOS	Language runtime	Full OS	App OS	Server OS	Container OS
Typical devices	Simple sensor devices, heartbeat sensors, lightbulbs, and so on	Feature watches, more advanced sensing devices	"Maker" devices, generic sensing solutions	High-end smartwatches	Solutions benefiting from a portable webserver and edge-computing capabilities	Solutions benefiting from fully isomorphic apps—that is, code that can be migrated between the cloud and the edge
Minimum required RAM	Tens of kilobytes	Hundreds of kilobytes	A few megabytes	Hundreds of megabytes	Tens of megabytes	Gigabytes
Typical communication protocols	Constrained (MQTT, LWM2M, CoAP)	Constrained (MQTT, LWM2M, CoAP)	Standard Internet protocols (HTTP, HTTPS)	Standard Internet protocols (HTTP, HTTPS)	Standard Internet protocols (HTTP, HTTPS)	Standard Internet protocols (HTTP, HTTPS)
Typical development language	C or assembly	Java, JavaScript, Python	C or C++	Java, ObjectiveC, Swift	JavaScript	Various
Libraries	None or system-specific	Language-specific generic libraries	OS libraries, generic UI libraries	Platform libraries	Node.js npm modules	Various
Dynamic software updates	Firmware updates only	Yes	Yes	Yes	Yes	Yes
Third-party apps supported	No	Yes	Yes	Yes	Yes	Yes
Isomorphic apps possible	No	Yes	Only if the hardware architectures are binary compatible	Yes	Yes	Yes

Fig. 3. Architecture's Options Used in IoT

Lightweight M2M Protocol is responsible for the communication process and used for operating the communication between the M2M objects like M2M management, client software, and service enablement platform, which is included in server software. This protocol also aids in service fulfillment and application management remotely to the devices connected with the internet. Lightweight M2M protocol has some specific features, such as the dependence on efficient and secure Internet Engineering Task Force (IETF) standards (such as Constrained Application Protocol (CoAP) and Datagram Transport Layer Security (DTLS)). The interfaces of Lightweight M2M Protocol implicate some processes as services reporting, management processes, and registration [18].

Constrained Application (CoAP) Protocol is also responsible for the communication process, but can be considered as a recent one in terms of communication protocols. CoAP is mainly destined for IoT physical tools and insufflated by the Hypertext Transfer Protocol (HTTP). CoAP is using the connection of one-to-one type, but could not support the Transmission Control Protocol/Internet Protocol (TCP/IP) due to its design, which is only suitable for lightweight and thin IoT hardware. Moreover, CoAP uses User Datagram Protocol (UDP) over IP; and is a more efficient and dynamic protocol compared to HTTP, especially when the use of lesser resources and implementations of more features such as executing, observing (notifying any change in the status of server or device), discovering features (finding the surrounding devices), reading and writing [18].

Message Queue Telemetry Transport (MQTT) Protocol is a messaging protocol which proceeded over TCP/IP. MQTT is a lightweight communication protocol but it is not M2M communication due to its use of a message broker server between devices. It consists of three major elements (subscriber, broker and publisher). Concerning security area, MQTT supports Transport Layer Security (TLS) and Secure Sockets Layer (SSL) [18].

In general, there what is good and what is better. The choose of the best protocol depends on which category of IoT's application is involved. For example, MQTT is better for WAN network condition due to the existing concept of the broker, while CoAP is better for web services due to its harmonic with HTTP.

III. IoT Applications

As claimed by John Stankovic in his survey that the main IoTs' applications can be classified into14 fields, where these fields are: retails, smart homes, healthcare, smart factories, environment, smart cities, Lifestyle, user interactions, supply chains, energy, agriculture, transportations, emergency and culture and tourism. However, Stankovic's survey was

conducted over 30 countries and he found the most used applications were in 4 areas which are: transportations, healthcare, smart cities and smart homes [18].

A. Retail and Logistics

Retail and supply chain management is a very common term nowadays, so applying IoT in this sector will have lots of advantages, which are including the monitoring of inventory over the supply chain, product tracking and payment processing. Besides, IoT puts forward abundant applications like quick payment solutions, guidance of products places and prices in accordance with the shopping list and control the rotation of products on shelves to automate inventory process within the shop itself or in a warehouse. In this type of IoT's application, two main IoT elements are used, which are WSN and RFID, but the implemented bandwidth range is small. On the other hand, the IoT in logistics may include item location, quality of shipment, flee tracking, storage incompatibility detection, etc. Compared to retail felid, logistics used the same two IoT elements but the difference in bandwidth, where it ranges from medium to large in logistics [21]. Lots of information of IoT domains on retails, supply chain and logistics can be found in [22].

B. Smart Cities

The integration between cities and IoT technologies has created a new term with so-called smart cities as well as led to developing the smartness of cities by launching many applications which will contribute and sustain the development's acceleration in this sector. Some of these applications are the instantaneous monitoring of vibrations for buildings and bridges of the city, monitoring the availability spaces of parking, monitoring the vehicles and traffic jam, sound and visual monitoring of some rough and tough levels within the city, smart highway roads in the option of climate conditions and unexpected circumstances, detection of waste and trash level within the container (waste management), smart parking, noise urban maps, smart lighting, intelligent transportation systems and so on. This domain of IoTs' applications is using single sensors, WSN and RFID as elements of IoT, while the bandwidth is ranging from small to large due to abundant and diversified of its application [21].

C. Medical and Healthcare

The use of IoT technologies has consequence many benefits over the healthcare sector, these benefits can be in tracking for devices, patients as well as the authentication of people and staff (tracking is a function used to identify objects and their motions if required), sensing and automatic data collection [20]. Sensors devices are used to diagnosing patient's status and providing the up to date information about the patient's health. Sensors can be applied to improve the monitoring methods of vital functions like heart rate, temperature, blood pressure, blood glucose, etc. The automatic data collection is applied for automating care, reducing processing time, automating processes and medical inventory management. This domain of IoTs' applications is using WSN, RFID, NFC, Bluetooth WiFi, etc, while the bandwidth is ranging from small to large due to the abundant and diversified of its application [21]. Lots of information on IoT domains in healthcare can be found in [22].

D. Environment Domain

Utilization of IoT technologies is one of the farthest hopeful market segments at the point of conserve the environment; where will be a boost of Wireless Identifiable Devices (WID) usage within the friendly programs that specializes in the environment topics. [17].

IV. CHALLENGES

The workflows in homes, firms or industries will be characterized by cross-organization integration, which will lead to requiring a high operation dynamic as well as the ad-hoc relations. For now, the availability support of Information and Communication Technologies (ICT) is very slight. The following part highlights the most key challenges that face the IoT technologies so far:

A. Network Foundation

The limitations of the existing IoT's are considered as the prime challenge to IoT in terms of manageability, scalability and mobility [17].

B. Security, Privacy and Trust

The barriers that face IoT in terms of security are:

- Architecture's securing to be ensured at both design and execution time.
- Proactive identification and preservation from the malignant software.
- Proactive identification and preservation from the arbitrary attacks.

The barriers that face IoT in terms of privacy are:

- Data privacy (such as controlling over personal's information) and location privacy (such as monitoring over individual's physical location).
- The necessity for imposing protection laws as well as privacy enhancement technologies.
- The development of tools, standards, protocols and methodologies which will lead to the identity management of objects.

The barriers that face IoT in terms of trust are:

- The necessity to exist a fluid exchange for critical and sensitive data (Ex: the communication with trusty services will be done by smart objects instead of users or organizations themselves).
- Trust must be a key part of IoT's design and its architecture and must be contributed in.

C. Managing Heterogeneity

Overseeing and being in charge of heterogeneous applications, objects, devices and environments account for a major challenge. The challenges can be comprised of:

- Providing smart and useful services by collecting a large amount of surrounded information and data.
- Enhancement in the mechanisms of sensor data stream processing.
- Designing techniques for sensor data discovery.
- Designing a dynamical architecture for sensor storage and networking.
- Sensor data management, correlation and aggregation filtering techniques design.

D. Regulatory and Legal Issues

It can mainly be applied on devices return to medical, insurance, banking, manufacturing equipment and infrastructure equipment. Most of these issues are complying with chronic and elderly laws such as HIPAA, Directive 95/46/EC, GAMP 5, CFR 21 part 11, etc. These laws may delay in the process of bringing products to the market as well as the rise of their cost over time [23].

E. Architecture and Standardization Shortage

The persistence of fragmentation in the implementation of IoT may increase the cost and decrease the value of IoT to the end clients [23].

V. Risks of IoT

IoT is a technology like other technologies that have been invented by humans, where it has many advantages as well as many disadvantages and negative aspects. Any object linked to the Internet has an address called Internet Protocol (IP), this IP indeed is a networking software, and responsible for performing specific tasks as well as the interacting of objects with internet. It can easily be hacked due to the weakness of security system [27]. This part will highlight the critical problems and risks that may face IoT's industry world.

A. Significant Risks

- Material losses which cause to harming users (Ex, home appliances) by intervening and manipulating their properties.
- The potential of robbery operations due to exploiting location data of those IoT devices (Ex, determining the car Coordinates).
- Monitoring users and privacy issues of sensitive data which might put the user data in a risky position.
- Employing the IoT devices for hacking electronic governments and critical organizations that are fully connected to the Internet [28].

B. Security Vulnerabilities

In computer security, the vulnerability can be considered as a high weakness point to implement unauthorized actions within the system by attackers. A security vulnerability includes privacy, sabotage and denial of service. Undoubtedly, the effects of sabotage and denial of service can widely be taken into consideration more than concentrating on privacy itself despite its importance. For Instance, "changing the mix ratio of disinfectants at a water treatment plant or stopping the cooling system at a nuclear power plant could potentially place a whole city in instant danger" [23].

C. Types of IoT Security Gaps

- Weakness in the authentication process [29].
- Vulnerabilities and gaps in communication interfaces between the user and IoT is insecure, where the user can control, access and bypass the device.
- The use of unconfident protocols for data transfer.
- Lack of identification methods where the unauthorized people can log in into most devices easily.
- The simplicity of scanning and knowing the devices linked to the internet.

VI. SWOT Analysis

The issues of IoT are very various and have several aspects that should be taken into consideration, such as business models, enabling technologies, applications, social and environmental effects. Two analyses must be used before launching any service/product into local or globe market. SWOT analysis is one of most important analyses, it will be used in this paper to conclude and summarize the internal factors of IoT as well as the external factors as following below:

A. Strength Points

- *The possible use of IoT lead to reduce businesses costs and increase the profits over time:* as mentioned above, the earning of IoT use will be up to $123 Billion in 2021 and more with an annual growth rate of 7.3%.
- *Environment-Friendly:* linked appliances to the internet such as smart cars, homes, etc, can be utilized to bring down the harmful emissions and consequently limit the use of energy and help protect the environment.
- *Easiness of Use:* IoT can make the devices connect with each other easily.
- *Innovation:* the studies and sciences conducted, in terms of IoT innovations, have driven the technology industry towards the top.

B. Weakness Points

- *Security:* which can be considered as the most drawback point in IoT in terms of the possibility of how it can be hacked by some mischievous hackers.
- *Data Challenges:* collect, analyse and store the data are a complex process and not that much simple process as known, where it needs a robust infrastructure that can absorb the amount of data flowing every time and from everywhere.

C. Opportunities Points

- *Emerging markets:* they are fast-growing zones which enable IoT to swiftly expand.
- *Increase the innovation of wearables devices:* smart-watches and smart-glasses carry the ‘smart’ tag, whereas watches nowadays are not only responsible for knowing time, but also able to record the daily activities and work as small smartphone and more. From this point, it can be transmitted every wearable thing into a smart piece.
- *Infrastructure Management:* as mentioned in weaknesses points that IoT has a weak infrastructure, and by increase the forces and forts on this sector, it may be a strong basis for the IoT.
- *Attractive zone for investors:* IoT brings with it an array of potential investment opportunities.

D. Threats Points

- *Vulnerability to hackers:* hackers are trying to control the surrounding things; the loopholes of the internet are forming real threats for users through being vulnerable to attack by infiltrators.

- *The possibility of not meeting customers' expectations:* IoT has reached to peak, whereas humans have over-the-top expectations from IoT. These exaggerated hopes put the IoT's products at a risky level if the products defeat to satisfy these expectations.

VII. CONCLUSIONS

The diversity of emerged new devices which connected to the Internet will produce an overflow of data which need to be collected, processed and analysed by the organizations. Despite that the organizations will identify new business opportunities according to this data, new risks will emerge. The IoT has the capability to bring together each aspect of different networks. Hence, security at both levels of networks as well as devices is critical for the IoT's operation. The same intelligence that authorises appliances to perform their tasks has also to enable them to recognize as well as counteract threats.

Safeguarding of the IoT's propagation besides harnessing its economic value at the same time, requires a regular and methodical study of various risk factors. Most of the cyber-attacks are targeting IoT devices, and as observed, the ability of attackers is growing continuously, thus however can predict the severity of attacks in the future and how much these attacks will affect on people's life, business and the IoT itself.

REFERENCES

[1] P. Radanliev et al., "Future developments in cyber risk assessment for the internet of things", Computers in Industry, vol. 102, 2018. Available: 10.1016/j.compind.2018.08.002.

[2] N. Gershenfeld, When things start to think. New York, NY, USA: Henry Holt, 1999.

[3] A. Taivalsaari and T. Mikkonen, "A Taxonomy of IoT Client Architectures", IEEE Software, vol. 35, no. 3, pp. 83-88, 2018. Available: 10.1109/ms.2018.2141019.

[4] A. Celesti et al., "Exploring Container Virtualization in IoT Clouds", Proc. 2016 IEEE Int'l Conf. Smart Computing (SMARTCOMP 16), 2016.

[5] D. Cassel, "JavaScript Popularity Surpasses Java PHP in the Stack Overflow Developer Survey", The New Stack, Mar. 2016, [online] Available: thenewstack.io/javascript-popularity-surpasses-java-php-stack-overflow-developer-survey.

[6] Pallavi Sethi and Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," Journal of Electrical and Computer Engineering, vol. 2017, Article ID 9324035, 25 pages, 2017. https://doi.org/10.1155/2017/9324035.

[7] B. Skrabanek, "Difference Between Vision and Mission Statements: 25 Examples", ClearVoice, 2018. [Online]. Available: https://www.clearvoice.com/blog/difference-between-mission-vision-statement-examples/.

[8] C. ROWLAND, "Tesla, Inc.'s Mission Statement & Vision Statement (An Analysis) - Panmore Institute", Panmore Institute, 2018. [Online]. Available: http://panmore.com/tesla-motors-inc-vision-statement-mission-statement-analysis.

[9] L. GREGORY, "Microsoft's Mission Statement & Vision Statement (An Analysis) - Panmore Institute", Panmore Institute, 2019. [Online]. Available: http://panmore.com/microsoft-corporation-vision-statement-mission-statement-analysis.

[10] V. MARTIN, "Samsung's Mission Statement & Vision Statement (An Analysis) - Panmore Institute", Panmore Institute, 2019. [Online]. Available: http://panmore.com/samsung-corporate-vision-statement-corporate-mission-statement-analysis.

[11] R. Sharma, "Top 15 Sensor Types Being Used in IoT - Sensor Types & their IoT use", Finoit Technologies, 2018. [Online]. Available: https://www.finoit.com/blog/top-15-sensor-types-used-iot/.

[12] S. Oh and Y. Kim, "Development of IoT security component for interoperability", Cairo, Egypt, 2017.

[13] DataFlair Team, "How IoT Works - 4 Main Components of IoT System -DataFlair", DataFlair, 2018. [Online]. Available: https://data-flair.training/blogs/how-iot-works/.

[14] Gartner, "Gartner Identifies Top 10 Strategic IoT Technologies and Trends", Gartner, 2018. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends.

[15] L. Columbus, "10 Charts That Will Challenge Your Perspective Of IoT's Growth", Forbes.com, 2018. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2018/06/06/10-charts-that-will-challenge-your-perspective-of-iots-growth/#406f0a8c3ecc.

[16] L. Columbus, "The Best IoT Companies To Work For In 2018 Based On Glassdoor", Forbes.com, 2018. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2018/06/19/the-best-iot-companies-to-work-for-in-2018-based-on-glassdoor/#31313d9a3b63.

[17] D. Bandyopadhyay and J. Sen, "Internet of Things: Applications and Challenges in Technology and Standardization", Wireless Personal Communications, vol. 58, no. 1, pp. 49-69, 2011. Available: 10.1007/s11277-011-0288-5.

[18] C. Sharma and N. Gondhi, "Communication Protocol Stack for Constrained IoT Systems", Bhimtal, India, 2018.

[19] J. A. Stankovic, "Research directions for the Internet of Things", IEEE Internet Things J., vol. 1, no. 1, pp. 3-9, Feb. 2014.

[20] A.M. Vilamovska, E. Hattziandreu, R. Schindler, C. Van Oranje, H. De Vries, J.Krapelse, RFID Application in Healthcare–Scoping and Identifying Areas for RFID Deployment in Healthcare Delivery, RAND Europe, Feb 2009.

[21] R. Porkodi and V. Bhuvaneswari, "The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview," 2014 International Conference on Intelligent Computing Applications, Coimbatore, 2014, pp. 324-329.

[22] C. Forsey, "7 Ways IoT Is Changing Retail in 2019", Blog.hubspot.com, 2019. [Online]. Available: https://blog.hubspot.com/marketing/iot-retail.

[23] Peerbits, "Internet of things in healthcare: applications, benefits, and challenges", 2019. [Online]. Available: https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-and-challenges.html.

[24] W. Nyambi, "The IoT Revolution: challenges and opportunities", Geneva Business News | Actualités: Emploi, RH, économie, entreprises, Genève, Suisse., 2016. [Online]. Available: https://www.gbnews.ch/the-iot-revolution/.

[25] S.-R Oh, Y.-G Kim, "Security Requirements for Internet of Things", IEEE 2017 Platform Technology and Service (PlatCon), pp. 1-6, February 2017.

[26] I.T. Hwang, Y.-G. Kim, "Analysis of Security Standardization for the Internet of Things", IEEE 2017 Platform Technology and Service (PlatCon), pp. 1-6, February 2017.

[27] Jaeseok Yun, Ramnath Chekka Teja, Nan Chen, Nak-Myoung Sung, Jaeho Kim, "Interworking of oneM2M-based IoT Systems and Legacy Systems for Consumer Products", Information and Communication Technology Convergence (ICTC), pp. 423-428, October 2016.

[28] M. Tawfik, A. Almadni and A. Alharbi, "A Review: the Risks And weakness Security on theIoT", IOSR Journal of Computer Engineering, vol. 2278-0661, no. 2278-8727, pp. PP 12-17, 2017.

[29] C. Qiang, G. Quan, B. Yu and L. Yang, "Research on Security Issues of the Internet of Things", International Journal of Future Generation Communication and Networking, vol. 6, no. 6, pp. 1-10, 2013. Available: 10.14257/ijfgcn.2013.6.6.01.

[30] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, A Review on Internet of Things (IoT), International Journal of Computer Applications (0975 8887) Volume 113 -No.1, March 2015.