ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

PRODUCTION OF ECONOMICAL PACKET SNIFFERS AND OBSTACLE AVOIDING COMPUTER SYSTEMS

Aaron Don M. Africa, Rafael Duenas, Macario Peralta and Jethric See
Department of Electronics and Communications Engineering, John Gokongwei Jr. College of Engineering,
De La Salle University, Manila, Philippines
E-Mail: aaron.africa@dlsu.edu.ph

ABSTRACT

With the advancements in technology, computers are more capable of solving more and more problems that are integrated into human activity. With sensors, microcontrollers, and processors, one can create a device that uses set theory, artificial intelligence, spatial imaging, data management, and transfer. Devices such as packet sniffers that monitor and analyzes the traffic that passes through a network, obstacle avoiding robots, or getting spied on by hackers, are now possible by using accessible materials. These devices can be the catalyst to the conception of more advanced technologies based on the fundamental concepts and problems that they solve. Such devices, more accurately computer systems, are what connect the physical world to the digital world.

Keywords: obstacle avoidance, wireshark, arduino, packet sniffer.

1. INTRODUCTION

Microcontrollers are slowly getting more and more important in modern society. So, a little history is required in order for us to understand how such a chip was invented and distinguished away from microprocessors. Back in the 1970s, the same time that the company Intel was inventing something called a microprocessor, Gary Boone, an engineer from Texas Instruments was also on the same page. During that time, pocket calculators weren't even a thing yet and development was on the way. Boone Design a single integrated circuit chip that has all the necessary elements in order to make the pocket calculator, despite lacking a keypad or display yet. It was then called a microcontroller [1]. In order for it to be distinguished from a microprocessor, let's define what a microprocessor is. A microprocessor is an important part of a computer system. Without it on the computer, it won't be able to do anything. It allows the user to have input and apply arithmetic and logical operations that will have the desired output. micro-processors are usually used in groups also and need the help of multiple elements such as chips and circuits to make it work efficiently [2]. On the other hand, microcontrollers are independent of other chips and require fewer chips to help them despite it being able to do more limited functions. The basic definition of a microcontroller is a small low-cost and independent computer in a chip that can be used as an independent system [3]. Some parts of the microcontroller are the CPU, memory, Input/output ports, Timers and ADC or analog to digital converter [4]. Today, the accessibility of microcontrollers has increased because they are produced in billions each year, are inexpensive, and can be observed in many common appliances in one's household [5]. Now, we have access to capable and inexpensive microcontrollers such as Arduinos and raspberry pi's which can be used for a plethora of things and are able to be programmed, thanks to their own integrated development environment or IDE for short, as a powerful combination of hardware and software. These can be used as a medium for the connection of the digital world and the physical world or the IoT. Moreover, the microcontrollers have their own limitations. Microcontroller selection is essential depending on the degree of complexity a project requires [6]. It is only logical that one size does not fit all in the realm of computer systems but the depth and power a microcontroller has plays an important role in selection. IoT ecosystems supply information to web-enabled smart devices that have integrated processors, communication hardware and sensors, that act on, transmit, and receive data [7]. Such systems can be used as analytic tools, utility, safety equipment, and much more. These microcontrollers and mini- computers act as an IoT device that interact with both the digital and physical world. These devices depend on the use of data collecting hardware and monitoring devices [8]. These devices can act independently or with other devices, a prime example could be the use of packet sniffers because a packet sniffer acts as a singular node that intercepts data, but the user can add more nodes depending on the size of the network under study. Then the nodes can interact with each other or work together to have a collective of data that stems from the traffic of the network under study.

2. STATEMENT OF THE PROBLEM

As students, as well as residents of the Philippines, the group will tackle 2 key problems. Firstly, on campus, it is important to maintain the safety and integrity of the Wi-Fi network on campus by monitoring the activity of the network traffic Secondly, on the road to making computer systems autonomous, the combination of sensors and microcontrollers is a good way to explore further.

3. SIGNIFICANCE OF THE STUDY

In our modern world today, all the technology that is invented is in order to help the society to be a better place for everyone and for the greater good. The chosen systems that were analyzed in this study are programs or hardware that can help a computer to be more efficient and user-friendly. The first system; Packet Sniffer is used to monitor network data. The machine communication system mainly

ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

relies on packets; hence, it is crucial to understand its operation, uses, and vulnerabilities to develop further knowledge on how machinery interact with one another [9]. Basically, one of its uses is it just tracks the user's patterns and preferences so that the computer can further adapt to the user's personalization. But for this study, we focused more on troubleshooting the data that is being monitored by the Packet Sniffer. The packet Sniffer can check for errors in the system and can help the administrator to process the errors effectively. Our second system is the Arduino Uno PCB. It's a newly developed microcontroller that can be used in a lot of different ways depending on the user's preferences and usage. For this study, we focused on its usage as an obstacle-avoiding robot. There are a lot of videos floating on the internet showing robots that are avoiding obstacles using sensors to detect if an object is in front of them. Many chips and circuit boards were used in the early days, and now it is possible with just a simple Arduino board. This technology can be one of the progenitors of future advance AI that can build our society.

4. IN-DEPTH DESCRIPTION OF THE SYSTEM

4.1 Packet Sniffer

Packet sniffers are tools that monitor network traffic and can be used for multiple things, generally, a packet sniffer is a combination of hardware and software which communicate and coordinate with each other to do the following tasks [10]:

a) Raw binary data is collected by the sniffer

b) The data is then converted into readable text

c) The data is then analyzed by the packet sniffer

Initially, the data passes through a computer or an external node that uses a NIC to connect it to a network. The packets are then converted to a readable form and now can be analyzed by the system. There are two settings for the NIC [11]:

a) Non-Promiscuous mode

b) Promiscuous mode

In promiscuous mode, the packet sniffer will intercept and read all the packets that go through it. Whereas in non-promiscuous mode, the packet sniffer will only read the data if the network address included in the packet sniffer is theirs. The hardware components of a packet sniffer, are as follows [12]:

A. Capture driver

The capture driver is responsible for capturing the data from the network then passing it onto the buffer.

B. Buffer

The data is stored in this sector.

C. Decode

It makes the data understandable by articulating the data.

D. Packet editing/transmission

If, allowed, the packets may be edited before transmitting it to the network.

E. Packet analysis

(Figure-1.) Packets can either be analyzed after storage or on live real-time. The actual and header data are analyzed whenever data is stored in the memory or real-time analysis tasks are performed. Lastly, the decoder obtains packets by decoding the data store created a packet sniffer using a raspberry pi microcomputer (seen in Figure-2.). A raspberry pi is a small device that acts as a mini-computer meaning it is equipped with the basic components a computer needs to operate such as a micro-processor, Ram, HDD, and SD card slots [13]. Essentially, a Raspberry Pi is a mini-computer that can be hooked up to computer peripherals and act as a computer but in this case, a packet sniffer, The Raspberry Pi was geared towards use in the school setting for students to have a budget-friendly way to learn computer programming [14].

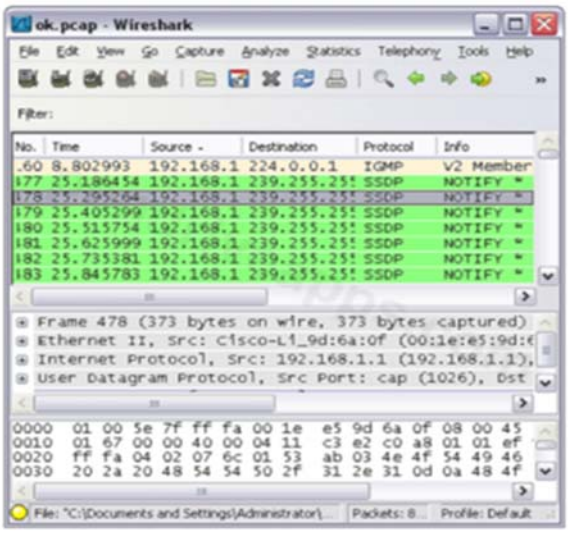

Figure-1. Wireshark System.

ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

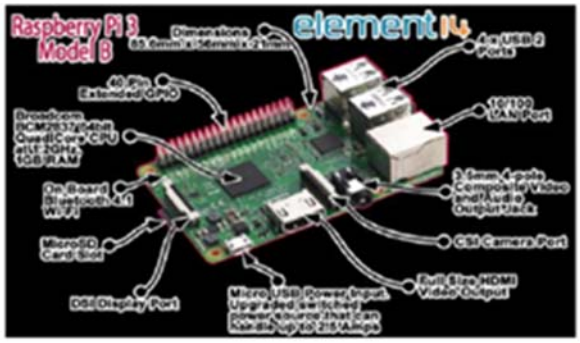

Figure-2. Raspberry Pi 3.

4.2. Obstacle Avoiding Robot

Figure-3. Arduino UNO.

The Arduino UNO is one of the members of the Arduino family. Arduino boards are microcontrollers that can perform a plethora of things with the right hardware and code using its Integrated development environment. They are small, inexpensive and capable little boards. Arduino boards are microcontrollers built on the foundation of Amtel microcontroller units. There are some boards that feature microprocessors which provide additional processing-power [15].

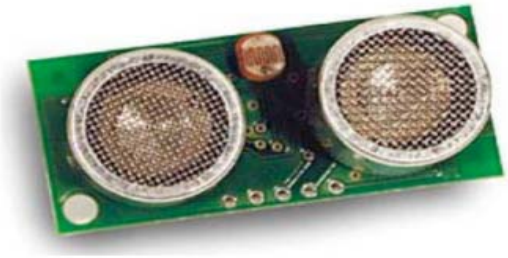

Figure-4. Ultrasonic Sensor.

The ultrasonic sensor used in the obstacle avoiding robot was utilized as an obstacle sensing tool that would sense how close the robot is to the obstacle by means of sound waves and depending on the code implemented on the Arduino, will determine where the robot will maneuver. Ultrasonic sensors work on the guideline of estimating the time between sending usually a couple of exceptionally short pulses and receiving the reflection of the propagated wave. The transmitter and receiver are the two main components of an ultrasonic sensor [16].

An obstacle avoiding robot utilizes sensors to "see" its environment and decide on how to maneuver around in it. A simple ultrasonic sensor or the like (infrared) will do just to exemplify the fundamental idea and operation of an obstacle avoiding robot. It also enables robots to travel through unknown environments without accidents. Robot route issues can be commonly named global or local, with respect to the surroundings of the robot. to utilize global navigation, the robot must know its surroundings then it chooses a path that avoids the obstacles in its environment. When the robot has little to no information on its surroundings, it uses local navigation wherein it uses sensors to detect obstacles and collision avoidance system [17]. The cooperation between the product and equipment are what allow the robot to move around collision-free.

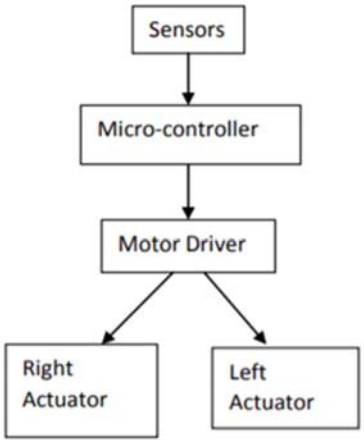

Figure-5. System block diagram.

5. REVIEW OF RELATED LITERATURE

5.1. Packet Sniffer System

The application of a packet sniffer ranges from home, virtual to commercial use. In the home environment, Wireshark and SmartSniff are open-source virtual packet sniffing tools for household intended purposes. These open-source packet analyzers are widely used for troubleshooting the network, analysis, software and communications protocol development, and occasionally education. They are very accessible to the average user since they are

ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

distributed to the Windows and macOS platforms. [18] The tapping of packets done across a network by a sniffer can either be filtered or unfiltered. Filtered is used when only specific data packets have to be captured and Unfiltered is used when all the packets have to be captured. A user can execute several techniques in order to identify sniffers on the network and protect the data from sniffers. Hence, packet sniffers can either serve as an administrative tool or for malicious purposes. It is solely based on the user's discretion since packet sniffing can monitor and validate network traffic with the aid of network administrators. Alternatively, it can simply be an application utilized for network administration, to read packets or interpret data that traverses in the layer of the network in the Transmission Control Protocol/Internet Protocol, which is widely known to users as TCP/IP.

5.2. Robot System

In order for this robot to run smoothly, it needs to have the right hardware and software such as Sensor selection, which can be considered important. Basically, the objective of having an obstacle-avoiding robot is to have an autonomous function with no human intervention. In their study, they were able to find out that there were a lot of sensors that are available for obstacles detection. Such examples are the infrared sensor, ultrasonic sensor, and LIDAR (laser-based sensor system), which according to them are considered to have one of the best detecting sensors that are cost-efficient and reliable. They also gave some description of the chosen sensors that can be used. Infrared sensors use infrared radiation in order to detect an object's distance. When the distance is measured by a beam, the light of the beam bounces back to the receiver with an angle after the reflection [19].

Another type of sensor that was mentioned is the PIR sensor. PIR sensors also called as Pyroelectric Infrared sensor, or Passive Infrared sensor can detect the jump in temperature, thermal radiation like for example a human body or an animal hotter the detected object, the greater the emission occurs in PIR sensor.

However, these systems have limitations as well. Performance of IR sensors is limited because of their low tolerance to bright lights. Such examples are a bright light or any bright coloured objects [19].

6. METHODOLOGY

6.1. Packet System

The administrators used MTR, a capable network diagnostic tool. It can weed out network errors and give the administrator important information on network status to upstream providers. MTR can capture the IP address of the AP and show the packet loss percentage that occurs in the network. This was used to analyze the incoming data traffic passing through the node (raspberry pi). To get the raspberry pi to perform such actions, the administrator needed to updated and upgraded using the "$ sudo apt-get update" and "$ sudo apt-get upgrade" commands. To install the MTR diagnostic tool the command "$ sudo apt-get install mtr" was used. Lastly, to send reports created by the sniffer on a text file, the command sudo mtr-r was used.

Figure-5. Shows the framework the raspberry pi acted as a node which intercepted the data being transferred over the network. Which it stored, converted and transferred via email to the administrator of the network [20].

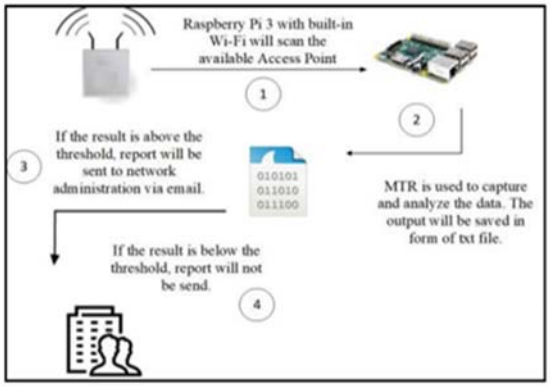

Figure-6. Built in system.

6.2. Robot Implementation

The project was implemented by programming the Arduino to make its own decisions, emulating artificial intelligence by analyzing the data it receives from the ultrasonic sensor and using the Arduino as a microcontroller for the robot [21].

The robot was coded initially to move forward by initializing Trigger and Echo pin as low. The ultrasonic sensor then detected obstacles in close proximity and the system calculates the time and distance from the obstacle and made the decision on how to avoid said obstacle based on the algorithm.

ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

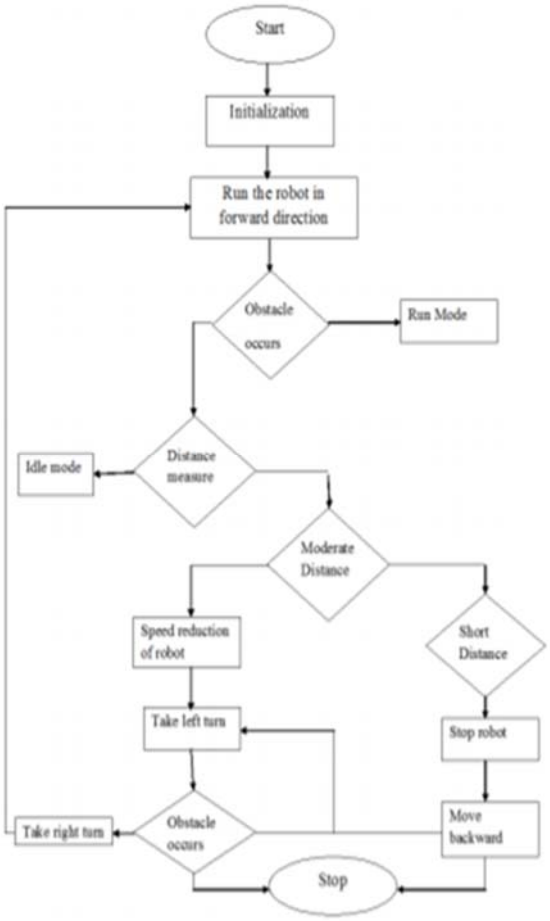

Figure-7. System flow chart.

Using a breadboard, the sensors were connected to the microcontroller. The software and hardware cooperate and coordinate with each other such that the DC powered motor driver navigates left or right depending on the situation.

7. RESULTS/DISCUSSIONS

7.1. The Packet Sniffer

The data traffic through the network was successfully intercepted by the packet sniffer. It was also able to save the data on a text file and send it to the administrator via email and indicated when packet loss was greater than 10 percent.

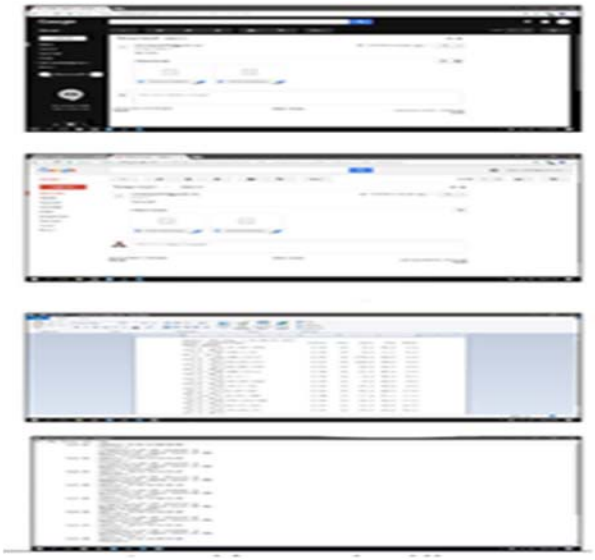

Figure-8. System Program

7.2. Avoiding Robot System

It is noted that the robot maneuvered around obstacles while checking for them continuously. In the event that there was an object in the way, the controller would send an order to the motor to stop and move left or right [22].

8. ANALYSIS OF DATA

The data that the packet sniffer intercepted was successfully transmitted to the administrator. Also, when the packet loss was 10 percent, the data was automatically sent to the administrator for review and troubleshooting. The data received by the admin was stored in a text file which was automatically saved by the updated and upgraded Raspberry Pi.The plate recognition unit utilizes a multi-layered ANN with training data which may not closely match the processed inputs fed into by the camera. Thus, it is necessary to retrain the neural network to fit our new set of data [38]. Furthermore, the input delay of the neural network must be accounted for as the goal of the system is to produce results in real-time.

The Arduino effectively commanded the robot to navigate through the obstacles with the data it receives from the ultrasonic sensor. The algorithm implemented onto the Arduino was successful, it acted as the A.I. or the brain of the robot and its decisions were dissipated by the Arduino to the motor and wheels [23].

9. CONCLUSIONS

As we are now dwelling on the computer age, technological advancements remain a pursuit as companies tend to compete with each other in offering better technology for the consumers [24]. As packet sniffing enters the technological aspect of this world, it poses benefits and drawbacks that can either harm or help us. Security measures must be taken into accounts such as the encryption of sensitive data and the securing of an

ARPN Journal of Engineering and Applied Sciences

organization's website. It is a must for organizations to take security measures to protect their data from packet sniffing. Encryption is one way of securing the information obtained by the packet sniffer, but it does not entirely prevent the packets from being sniffed [25]. As hackers become more and more sophisticated, packet sniffing will be an issue that would affect businesses in the future. It is essential for an organization to protect from any security threat by integrating security training. According to the SSL specialist, Thawatchai Chomsiri, implementing stricter security standards would be more cost-efficient and less damaging to the data than getting breached by hackers [26]. In the home setting, packet sniffing can also be prevented by encrypting sent or received data serves as a priority. Connecting to trusted Wi-Fi networks only can also be a great practice in preventing packet sniffing. Lastly, regularly scanning the network for issues or possible dangers.

On the contrary, it can also serve many advantageous purposes. IoT devices have been "domesticated" in the sense that they can adaptively and effectively manage our household appliances and keep track of them. We can take in the obstacle avoiding robot as an example, Chinese electronics companies like Xiaomi integrate packet sniffers with their vacuum robot cleaners to act as sensors for the obstacles [27]. Wireshark and Paketsender can even be used to packet sniff the robot vacuum cleaners [28].

10. RECOMMENDATIONS

For our recommendations, we suggest future researchers of the similar topic to study in depth other possible alternatives in the specific computer systems that we used. They can also look for more possible functions that are capable of being implemented in these computer systems, especially the utilization of microprocessors and microcontrollers. As these components are extremely flexible, so if one understands the functions that these systems are capable of, they will not be limited to the functions aforementioned in the paper. A blend of IR sensors and Ultrasonic Sensors perform better on all types of objects a robot comes across [29]. Ultimately, we suggest that one reads into other types of sensors and how they differ from ultrasonic sensors because they may present advantages over ultrasonic sensors, and the combination of multiple sensors may impact the performance of the robot. The group also recommends that one learn the function of Wireshark for packet analysis. Wireshark is a powerful tool for data analysis because it provides users with a GUI and it also filters data accordingly [30]. The data of the system can be transferred using a USB transfer device [31]. When converting the system into a database it can follow the format of these studies [32, 33, 34].

REFERENCES

[1] Microcontroller. (n.d.). Retrieved from https://ethw.org/Microcontroller.

[2] Srivasthav Girish, Kumar A., Yong Salem A,, Naharwara and Mishra P. 2017. Microcontroller Basics, Types and Applications. Retrieved from https://www.electronicshub.org/microcontrolers/.

[3] Baškys A. 2012. Microcontrollers.

[4] Microcontroller. 2017. Retrieved from https://ethw.org/Microcontroller.

[5] Gridling G. and Weiss B. 2007. Introduction to Microcontrollers. Vienna University of Technology Institute of Computer Engineering Embedded Computing Systems Group.

[6] Vaglica J. J. and Gilmour P. S. 1990. How to Select a Microcontroller. IEEE Spectrum. 27(11).

[7] What is internet of things (IoT)? (n.d.). Retrieved from https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

[8] Patnaikuni D. 2017. A Comparative Study of Arduino, Raspberry Pi and ESP8266 as IoT Development Board. International Journal of Advanced Research in Computer Science. 8(5).

[9] Vimalesvaran M. 2012. Packet Sniffing: What it's Used for, its Vulnerabilities, and How to Uncover Sniffers. Amonia Calculations.

[10] Astrodia P. and Patel H. 2012. Analysis of Various Packet Sniffing Tools For Network Monitoring and Analysis. International.

[11] Shah S., Shah A. and Bhattcharjee S. 2015. Intrusion Detection using Packet Sniffer. International Journal of Electronics, Electrical and Computational System. 4(10).

[12] Nagalakshmi S. 2017. Network Monitoring And Detecting Packets Using Packet Sniffing Method. International Journal of Scientific & Engineering Research. 8(4).

[13] Nur Haziq Mohd Safri, M., Wan Nik, W., Mohamad, Z. and Mumtazimah, M. 2018. Wireless Network Traffic Analysis and Troubleshooting using Raspberry Pi. International Journal of Engineering and Technology(UAE). 7: 58-60.

[14] Chaudhari H. 2015. Raspberry Pi Technology: A Review. International Journal of Innovative and Emerging Research in Engineering. 2(3).

ARPN Journal of Engineering and Applied Sciences

[15] Cvjetkovic, V. M. and Matijevic, M. 2016. Overview of Architectures with Arduino Boards as Building Blocks for Data Acquisition and Control Systems. International Journal of Online Biodemical Engineering. 12.

[16] Koval L., Vanus J. and Bilik P. 2016. Distance Measuring by Ultrasonic Sensor. IFAC-PapersOnLine.

[17] Ankit, V., Jigar, P., and Savan, V. 2016. Obstacle Avoidance Robotic Vehicle Using Ultrasonic Sensor, Android And Bluetooth For Obstacle Detection. International Research Journal of Engineering and Technology (IRJET). 3(2).

[18] Ansari S., Rajeev S. and Chandrashekar H. 2003. Packet sniffing: A brief introduction. Retrieved from https://ieeexplore.ieee.org/abstract/document/1166620.

[19] Esmail, R. *et al*. 2016. Obstacle-avoiding robot with IR and PIR motion sensors. IOP Publishing Ltd: Materials Science and Engineering. 152(1).

[20] Safri M., Wan Nik, W., Mohamad Z. and Mumtazimah M. 2018. Wireless Network Traffic Analysis and Troubleshooting using Raspberry Pi. International Journal of Engineering and Technology(UAE). 7: 58-60.

[21] Bhagat K., Deshmukh S., Dhonde S. and Sneha G. 2016. Obstacle Avoidance Robot. International Journal of Science, Engineering and Technology Research (IJSETR). 5(2).

[22] Kumar R. C. *et al*. 2013. Obstacle Avoiding Robot - A Promising One. The International Journal of Advanced Research in Electrical Engineering and Instrumentation Engineering. 2(4).

[23] Bresnahan T. F. and Greenstein S. 2003. Technological Competition and the Structure of the Computer Industry. The Journal of Industrial Economics. 47(1).

[24] Tabassum F., Susmita L., Muhammad T. and Ferdosi B. 2017. Obstacle Avoiding Robot. Global Journal of Researches in Engineering: H Robotics & Nano-Tech. 17(1).

[25] Biswas J. and Ashutosh. 2014. An Insight into Network Traffic Analysis using Packet Sniffer. International Journal of Computer Applications. 94: 0975-8887.

[26] Chomsiri T. 2007. HTTPS Hacking Protection. 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07).

[27] Sharma V. and Timari R. 2016. A review paper on "IOT" & It's Smart Applications. International Journal of Science, Engineering and Technology Research (IJSETR). 5(2).

[28] Leyden J. 2018. Doctor, doctor, I feel like my IoT-enabled vacuum cleaner is spying on me. Retrieved from https://www.theregister.co.uk/2018/07/20/iot_insecurity_robo_vacuum_cleaners/.

[29] Adarsh, Kaleemuddin, Bose and Ramachandran. 2016. Performance comparison of Infrared and Ultrasonic sensors for obstacles of different materials in vehicle/ robot navigation applications. IOP Conf. Series: Materials Science and Engineering.

[30] McRee R. 2006. Security Analysis with Wireshark. ISSA Journal.

[31] Africa A., Mesina A., Izon J. and Quitevis B. 2017. Development of a novel android controlled USB file transfer hub. Journal of Telecommunication, Electronic and Computer Engineering. 9(2-8): 1-5.

[32] Guevarra G., Koizumi, A., Moreno, J., Reccion J., Sy, C. and Del Rosario J. 2018. Development of a quadrotor with vision-based target detection for autonomous landing. Journal of Telecommunication, Electronic and Computer Engineering. 10(1-6): 41-45.

[33] Magsino and Ho I. 2018. Roadside Unit Allocation for Fog-based Information Sharing in Vehicular Networks. CitiFog 2018 - Proceedings of the 1st Workshop on Smart Cities and Fog Computing, Part of SenSys. 7-12.

[34] Navea R., Buenvenida P. and Cruz C. 2019 Stress Detection using Galvanic Skin Response: An Android Application. Journal of Physics: Conference Series. 1372(1).