CIBERATAQUES APLICADOS A UNA PLATAFORMA EXPERIMENTAL DEL INTERNET DE LASCOSAS ROBÓTICAS (IORT)

Mtro. Flores Montaño Luis Alberto
Email: luisfloresmontano@hotmail.com
Mtro. Rodrigo Vázquez López
rodrigo_em2@hotmail.com
Dr. Juan Carlos Herrera Lozada
jlozada@ipn.mx
Dr. Jacobo Sandoval Gutiérrez
j.sandoval@correo.ler.uam.mx

Instituto Politécnico Nacional
Centro de Innovación y Desarrollo Tecnológico en Cómputo
Universidad Autónoma Metropolitana Unidad Lerma Departamento de Procesos Productivos

Boletín No. 85
1o. de julio de 2021

Resumen

incremento del uso del internet ha creado distintas vertientes en las cuales las personas se han visto beneficiadas en sus actividades cotidianas. Una de estas vertientes es lo que se conoce hoy en día como el Internet de las Cosas (en inglés IoT), dicha tecnología se ha encargado del censado de diversas actividades humanas, especialmente de la industria y el hogar; a partir del concepto de IoT surgieron otras tecnologías, las cuales se han encargado de tareas aún más específicas, como es el caso de la medicina, industria, robótica, entre otras. Esta última es conocida como el Internet de las Cosas Robóticas (en inglés IoRT), la cual está enfocada a dispositivos robóticos, que censan y actúan físicamente en las actividades especialmente en la industria.
Sin embargo, el aumento de conexión a internet de este tipo de dispositivos ha provocado diversas dificultades para conseguir una seguridad plena, esto debido a distintos factores. Por ejemplo, los ciberataques han aumentado por las diversas vulnerabilidades en dichos dispositivos, provocando así una desconfianza en el uso de esta tecnología.
En esta investigación se implementó el uso de una plataforma basada en la tecnología IoRT, en la cual se analizaron las posibles amenazas y vulnerabilidades; estas últimas se evalúan con diversos ciberataques, conocidos como de esnifeo y suplantación. Adicionalmente se especifica el seguimiento de los pasos realizados para este tipo de ataques.

Palabras Clave: Ciberseguridad, IoRT, Ciberataque, Esnifeo, Suplantación.

Abstract

The increase in the use of the internet has created different aspects in which people have benefited in their daily activities. One of these aspects is what is known today as the Internet of Things (in English IoT), this technology has been responsible for the census of various human activities, especially in industry and the home; From the concept of IoT, later technologies emerged, which have been in charge of even more specific tasks, such as medicine, industry, robotics, among others. The latter is known as the Internet of Robotic Things (IoRT), which is focused on robotic devices, which physically register and act on activities, especially in industry.
However, the increase in the Internet connection of this type of device has caused various difficulties in full security, due to different factors. For example cyberattacks have increased due to the fact that various vulnerabilities have been found in said devices, thus causing distrust in the use of this technology.
This research implements the use of a platform based on IoRT technology, in which possible threats and vulnerabilities are analyzed; the latter are evaluated with various cyberattacks, known as sniffing and spoofing. Additionally, the monitoring of the steps carried out for this type of attack is specified

Keywords: Cybersecurity, IoRT, Cyberattack, Sniffing, Impersonation.

I. Introducción

Actualmente el incremento del uso de la red de internet ha creado distintas vertientes en las cuales las personas se han visto beneficiadas en su uso diario. Una de estas tecnologías que está en aumento en cuanto a desarrollo y uso, es lo que se conoce como el Internet de las Cosas. También conocido por su acrónimo en inglés IoT (Internet of Things), dicha tecnología se ha encargado del censado de diversas actividades humanas (Lesjak et al., 2015), especialmente de la industria y el hogar; a partir del concepto de IoT surgieron tecnologías, las cuales se encargan de tareas aún más específicas, como es el caso de la medicina, industria, robótica, entre otras (Li et al., 2016). Esta última es conocida como el Internet de las Cosas Robóticas (en inglés IoRT), la cual está enfocada a dispositivos robóticos, que censan y actúan físicamente en las actividades de la sociedad (Shah, 2016).

Sin embargo, conectar una gran cantidad de dispositivos a la red requiere un mayor esfuerzo por prevalecer la privacidad y seguridad de estos (Culot et al., 2019), es decir, tener un control de estos dispositivos es sumamente complicado debido a que su arquitectura computacional no es tan robusta como la de las computadoras convencionales (Lewis, 2006), por otro lado, la gran variedad de empresas dedicadas a esto utilizan distintos firmwares en los dispositivos que fabrican, tomando en cuenta que las actualizaciones de los firmwares de estos dispositivos no es muy común o en su defecto no es constante.

Lo anterior es un ejemplo de tantas problemáticas que se llegan a presentar con este tipo de dispositivos. Por ello, los cibercriminales pueden aprovechar estas vulnerabilidades para aplicar ciberataques y a su vez cierto tipo de amenazas a diversos sectores de la industria, ya sea del sector público o privado. Hay que tener en cuenta que si los dispositivos IoT son atacados pueden provocar pérdidas financieras; sin embargo, atacar un dispositivo IoRT puede provocar perdidas incluso en vidas humanas, ya que son dispositivos que interactúan físicamente en el mundo real (Hemsley & Fisher, 2018)

Debido a la inseguridad en este tipo de dispositivos, este proyecto se enfoca al análisis de dispositivos pertenecientes a IoRT, por lo que se propone una plataforma usando este tipo de tecnología, posteriormente se aplican cierto tipos de ciberataques con el propósito de analizar algunas vulnerabilidades, así como determinar que tan factible fue un ataque dentro de la plataforma.

II Plataformas de la industria 4.0

La plataforma IoRT que se utiliza en esta investigación es la que se muestra en la figura 1; dicha plataforma se comunica a través de un middleware de nombre Robotic Operative System (ROS), a través del protocolo de comunicación TCP/IP, entre estás comunicaciones se puede mandar información (carga de trabajo), entre el nodo maestro (MATLAB), hacía el nodo esclavo(Raspberry Pi) y posteriormente este último le dará las instrucciones al robot, en este caso se tomó en cuenta un servomotor, un brazo con 6 grados de libertad y una estación de trabajo Pegasus Amatrol; posteriormente la transmisión de

datos es enviada a la red por medio de protocolos de comunicación DNS y UDP, esto con el propósito de establecer una comunicación de envío de datos hacia el servidor de nombre ThingSpeak.

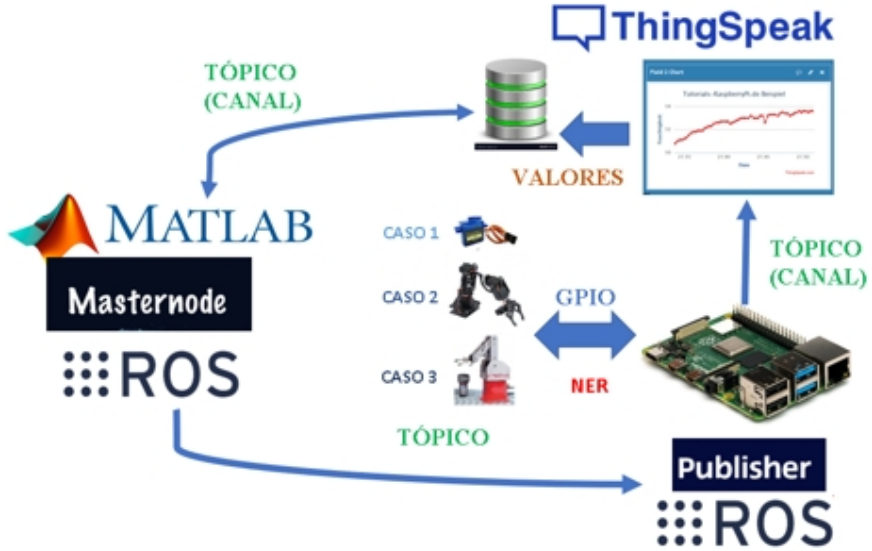

Figura 1. 1 Esquema general del funcionamiento del sistema IoRT.

Las pruebas de ataques realizadas en los tres robots fueron exactamente las mismas ya que el proceso de comunicación entre nodos es el mismo con excepción del nodo NER (que se muestra en la figura 1), ya que en este se cambia el dispositivo robótico, así como el Script de la carga de trabajo; cabe recordar que se utilizaron distintos nodos y diversos ataques para cada uno ellos; en este caso los enlaces NER, NMNE, NETS, TSNM entre el nodo esclavo, nodo maestro, dispositivo robótico y un servidor (ThingSpeak) respectivamente.

Por lo tanto, para el dispositivo Raspberry Pi 3 (nodo esclavo) se tiene una dirección IP 192.168.100.57, en el caso de la laptop (nodo maestro) 192.168.100.40, y el Gateway (Router) 192.168.100.1. Es importante mencionar que el equipo encargado de realizar los ataques es una PC, la cual tiene instalado un sistema operativo Kali Linux 2021; cabe destacar que este sistema operativo contiene diversas herramientas de hackeo ético en diferentes ámbitos; sin embargo, para las pruebas se utilizaron solo los ataques de tipo Esnifeo y Suplantación; siendo más específico se utilizaron ataques de tráfico de análisis/información en tránsito, suplantación de identidad y/o ataque de hombre en el medio.

El tipo de comunicación utilizado entre estos dispositivos son los protocolos DNS Y UDP, es importante mencionar que para las pruebas fue necesario obtener el ARP de los dispositivos conectados a la red, con el propósito de identificar cada uno y posteriormente poder plantear los objetivos. Para esto se utilizó el comando arp desde la consola, este comando puede ser utilizado en un dispositivo con un sistema operativo Windows, Linux o Mac (puede haber variantes en la sintaxis), para nuestro caso se utilizó en Linux (Kali), el comando sudo arp -scan -l, el resultado de este se muestra en la figura 2:

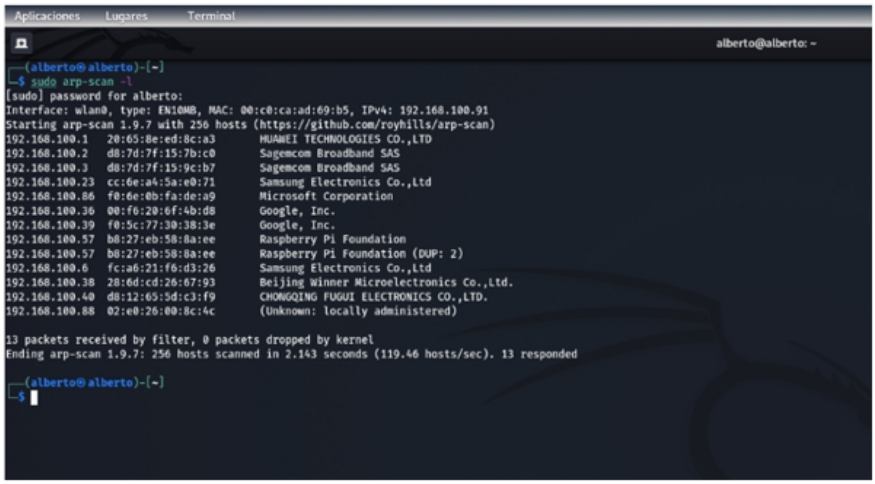

Figura 2. . Identificación de objetivos con uso de ARP.

Como ya se mencionó se tiene una tabla donde se muestra todos los dispositivos conectados a la red del Gateway, con el propósito de verificar de cada nodo sus IPs, MACs y por lo tanto tener identificado los objetivos a atacar. Cabe mencionar que para hacer un uso más optimizado de estas herramientas y otras por mencionar se utilizó un adaptador inalámbrico ALFA AWUS036NEH, con un Chipset rt3070, dicho adaptador es ideal para hacer pruebas de pentesting usado especialmente en Kali Linux.

Una vez identificado esto, se hace uso de la herramienta Ettercap, la cual es un interceptor, esnifeador y registrador para LANs con switch. Además, soporta direcciones activas y pasivas de varios protocolos, adicionalmente realiza los ataques de tipo Suplantación ARP (ARP Spoofing), el cual es un ataque de tipo de suplantación de identidad o de hombre en el medio, este tipo de ataques pueden ser realizados gracias a que hay una suplantación en la tabla de ARP, ya que la MAC del atacante es actualizada con las IP de los dispositivos que serán las víctimas, por lo tanto dentro de la lista se encontrarán direcciones MAC con la misma serie pero con diferente IP; la lista de objetivos se muestra en la siguiente imagen.

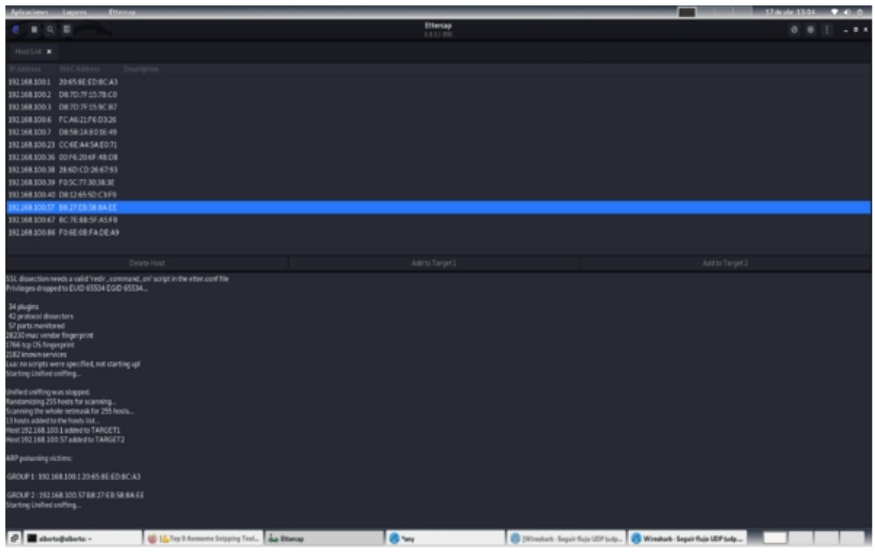

Figura 3. Interfaz de la herramienta Ettercap.

Posteriormente se hizo uso de la herramienta de Wireshark, la interfaz de dicha herramienta es mostrada en la figura 4, cabe mencionar que esta fue capaz de identificar un duplicado en las IPs (seleccionado en la lista), esto fue posible ya que los dispositivos habían sido suplantados con la herramienta de Ettercap.

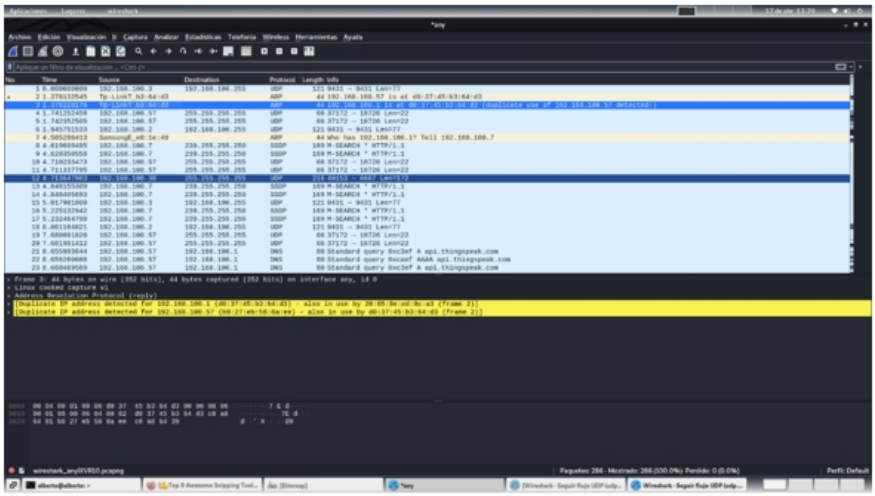

Figura 4. . Interfaz de la herramienta Wireshark.

Lo anterior quiere decir que existe una interferencia entre la comunicación, en este caso los objetivos fueron el dispositivo Raspberry (nodo esclavo), y el Gateway (que posteriormente se comunica el servidor ThingSpeak), como ya se mencionó el tipo de comunicación se realiza a través de diversos protocolos de comunicación como UDP y DNS, en este caso para probar la herramienta Ettercap, primero se hicieron pruebas con el acceso de diversas páginas web sin una encriptación como SSH, en las cuales fueron exitosas; sin embargo, en la plataforma IoRT, la información que es enviada, se hace a través de Scripts programados en Python, los cuales contienen los canales de comunicación y llaves, estos últimos vinculan los datos (carga de trabajo) al servidor ThingSpeak.

III. Análisis y resultados

Se determinó que la herramienta Ettercap, no fue capaz de mostrar ningún tipo de dato que es enviado a través de los 3 nodos (nodo maestro/esclavo y servidor); es importante mencionar que la transmisión de carga de trabajo es enviada a cada uno de los dispositivos que interactúan formando así un ciclo en la transmisión de carga de trabajo.

Posteriormente la herramienta Wireshark, encargada de analizar los paquetes enviados a través de la red, muestra una serie de conexiones de todos los dispositivos conectados; sin embargo, únicamente se seleccionaron aquellos donde el nodo esclavo (Raspberry) se comunica al servidor (ThingSpeak), esto último se muestra en la figura 5:

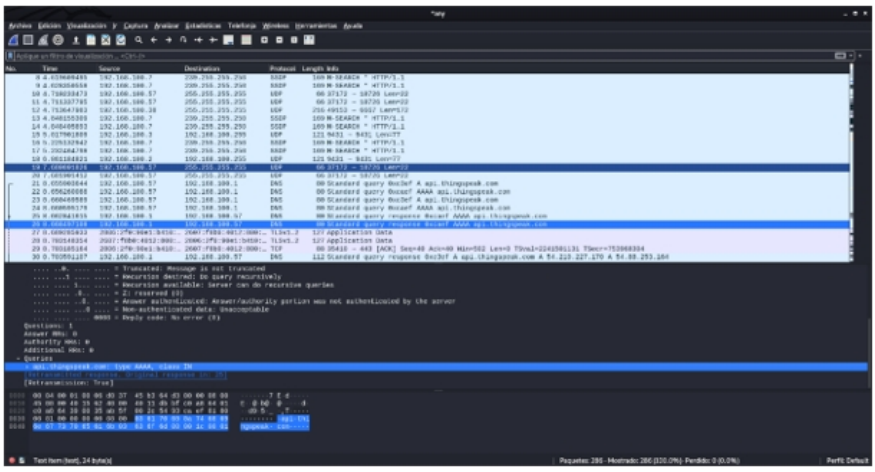

Figura 5. Esnifeo entre las comunicaiones objetivo.

Durante la revisión de paquetes se puede observar que hay diversos paquetes y distintos nodos que se comunican entre ellos, así como distintos protocolos, en este caso únicamente nos enfocaremos a la transmisión de datos de las IPs de nuestro interés en este caso los que corresponden los dispositivos que transmiten la carga de trabajo a través del Script. En la figura 6 se puede mostrar que los nodos de interés se comunican con el servidor (www.thingspeak.com) y se utilizar un protolo DNS:

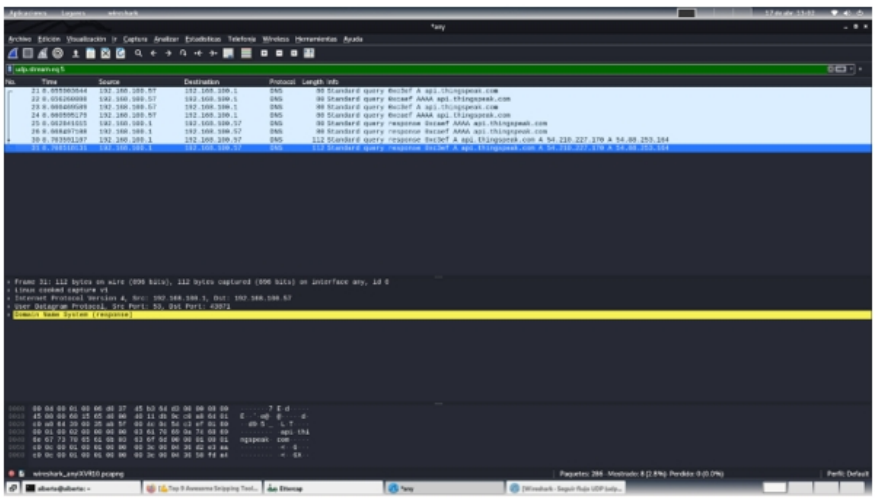

Figura 6. . Esnifeo de datos al servidor ThingSpeak .

Teniendo en cuenta que existen diversos protocolos de comunicaciones entre ellos también de tipo TCP y UDP, se procede a analizar los datos en dos formas en UTF8 y ASCII; sin embargo en el contenido de los protocolos que se analizó no se muestra ningún indicio de las llaves y datos de la carga de trabajo; esto se puede observar en la figura 7.

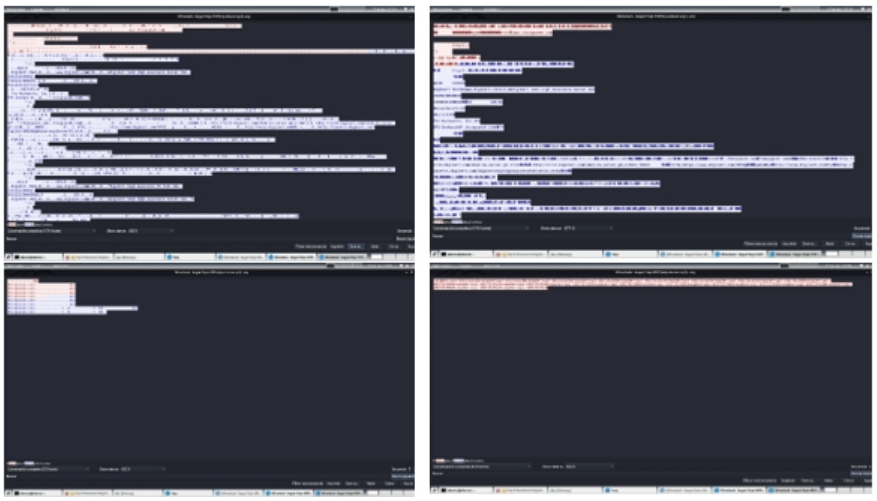

Figura 7. Muestra del contenido en UTF8 y ASCII.

III. Conclusiones

En este artículo se realizó una plataforma experimental basada en la arquitectura IoRT, cabe mencionar que no se profundizó en el tema de la plataforma debido a que esta investigación se enfoca más a los cibereataques de esnifeo y suplantación realizados a esta.

Como se observó en la parte de los resultados el ciberataque de suplantación no fue exitoso debido a que principalmente la herramienta de Ettercap suele obtener información a través de los protocolos TCP/IP, y por lo tanto está más enfocado a la suplantación en páginas Web; lo mismo ocurrió para el ataque de esnifeo donde se utilizó la herramienta de Wireshark, ya que aunque se podía visualizar el tipo de protocolos de comunicación y los sitios a donde era enviada la información, no fue posible visualizar, los datos que se transmitían en el script de la carga de trabajo del robot. Por otro lado, se determinó que la información de dicha carga va encriptada con un algoritmo tipo SHA 2, de esa manera, aunque se tenían los datos no era posible identificar la información ya que se maneja de manera encriptada, cuando es enviada al servidor de ThingSpeak.

Finalmente se concluye que al descartar algunas vulnerabilidades y amenazas que pudieran surgir al implementar a estos dispositivos con este tipo de arquitectura, son relativamente bajas en términos de ciberataques de esnifeo y suplantación utilizando en este caso las herramientas de Wireshark y Ettercap respectivamente; es de suma importancia ir descartando los posibles ataques en este tipo de arquitecturas IoRT, ya que empiezan a tener un auge en la industria 4.0 y muy posiblemente en un futuro muy cercano en las actividades cotidianas de diversos sectores de la sociedad.

Referencias

1. Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (**2019**). Addressing Industry 4.0 Cybersecurity Challenges. *IEEE Engineering Management Review*47(3), 79–86. https://doi.org/10.1109/EMR.2019.2927559

2. Hemsley, K., & Fisher, R. (**2018**). A history of cyber incidents and threats involving industrial control systems.*IFIP Advances in Information and Communication Technology*542, 215–242. https://doi.org/10.1007/978-3-030-04537-1_12

3. Lesjak, C., Hein, D., & Winter, J. (**2015**). *Hardware-Security Technologies for Industrial IoT:TrustZone and Security Controller.*

4. Lewis, J. A. (**2006**). *Cybersecurity and Critical Infrastructure Protection.*

5. Li, X.-Q., Zhang, Y., & Zhao, H.-W. (**2016**). IoT Family Robot Based on Raspberry Pi *IoT Family Robot Based on Raspberry Pi* . https://doi.org/10.1109/ISAI.2016.136

6. Shah, V. (**2016**).*). IOT ROBOT MAJOR PROJECT REPORT.*