ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Jammers: A Case Study

Subodh Chouhan[1], Sushil Kumar[2], Aman Singh[3], Prateek Rawat[4], Vishwajeet Singh[5]
Student[1, 2, 3, 4, 5]
Department of Electronics & Communication Engineering[1, 2, 3, 4]
Department of Mechanical Engineering[5]
Technovision Education Group, Lucknow, Uttar Pradesh, India

Abstract:
It's a comprehensive analysis of three types of jammer known today. The mobile phone, radio & radar jamming techniques are discussed here, the legality of the issue at international level in different countries & the subtypes of it. The counter measures of radar jamming are also discussed in brief. Also the electronic circuits of following are shown.

Keywords: Jamming, Interference, Subtle, Stealth, Chaff, Decoys, Corner Reflectors, Spot, Sweep, Barrage

I. INTRODUCTION

MOBILE PHONE JAMMER

Figure.1. Mobile Phone Jammer

A **mobile phone jammer** is an instrument used in defense & investigation field to prevent cell phones from receiving signals from base stations of mobile networking system. When used, the jammer effectively disables all cellular phones in the coverage area. These devices can be used practically, in any location, but these are found primarily in places where a phone call would be particularly disrupted for some investigation purpose.

A) Legality

Since, these jammers actively broadcast radio signals in the area, in particular countries they may or may not be legal to possess or operate based on the specific laws of that specific country. Some examples are given below: -

i) **India:** Illegal by law, and allowed for common mass, except for security and military agencies, & usage in jail, theatres, mosques, schools etc. with prior permit from respective authorities and jamming strictly limited to the firm perimeter zone with zero leakage.

ii) **Australia:** Illegal to operate Mobile Phone Jammer, supply or possess unless the user(agency) has a National PMTS C telecommunications license under the Radio communications (Interpretation) Determination2000.

iii) **Brazil:** Illegal, but installation of the device in jails has been proposed for security reasons.

iv) **Canada:** Illegal, except by federal law-enforcement agencies who have obtained approval.

v) **European Union:** Highly Illegal, according to the rule of European Commission's "Interpretation of the Directive 1999/5/EC".

vi) **New Zealand:** Illegal to sell& marketing, manufacture or use unless one holds prior permission. Legal inside jails by Department of Corrections, Govt. of New Zealand.

vii) **Pakistan:** Illegal to use without prior permission. The individuals or institutions must get No Objection Certificates (NOCs) before installation of such devices from government or associated agencies.

viii) **Singapore:** Illegal to manufacture, market, import, use or sell radio jamming equipment's. Exceptionally can be deal with the permitted persons for specified use.

ix) **South Africa:** Highly Illegal. No organization in the country is allowed to jam cellular signals, or any device is strictly prohibited which is used to jam signals.

x) **Sweden:** Illegal. Legal inside jails and for military use in the country.

xi) **Ukraine:** Legal by law, is planned to be used in schools for effective surveillance.

xii) **Italy:** Illegal both to own personally and use accordingly, But if law is violated according to the Penal Code of the country, offenders are punished with imprisonment up to 4

years. Can be used under strict authorization for enforcement in exceptional cases by Italian law enforcement agencies, such as Polizia Di Stato and Carabinieri.

xiii) **United Kingdom:** Illegal to use, but legal to own with specifications. After having been proposed by prison inspectors of respective police station, installation and use of jammers in jails has been legal since the end of 2012 in the country.

xiv) **Iran:** Illegal to use without permissions but permitted after specified controlled permission by government.

xv) **United States of America:** Cell phone blocking devices are used by federal agency officials under certain circumstances with legal provisions. Privacy rights of property owners may affect the policy and application of law within buildings & arena. For radio communications, it is illegal to operate, manufacture, import, or offer for sale individually, including advertising (Communications Act of 1934). Blocking radio communications in public can carry fines of up to $112,000 and/or imprisonment of up to 1 year as per law. The Homeland Security Act of 2002, United States of America may override the Communications Act of 1934.

B) Mobile Phone Jammer Circuit Prototype

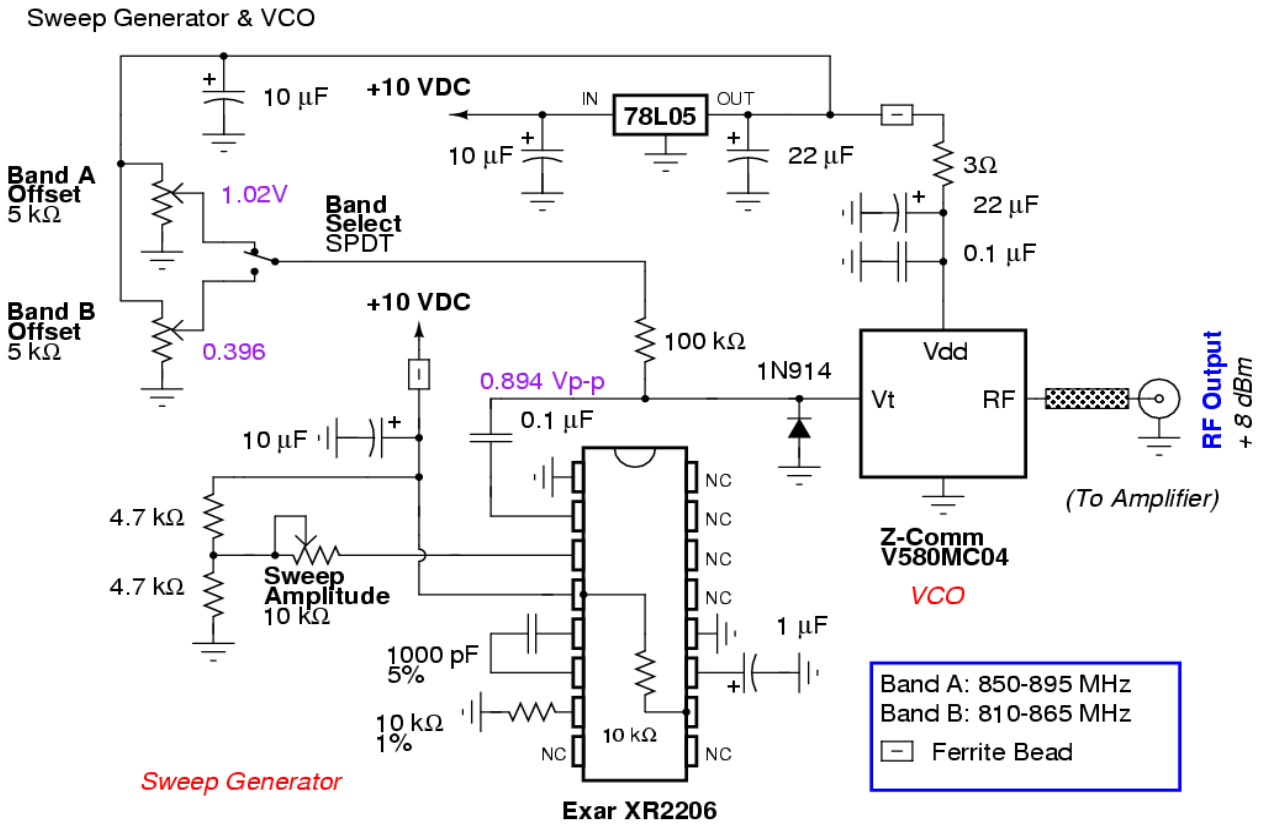


Figure.2.Mobile Phone Jammer Circuit Prototype

2. RADIO JAMMER

A radio jammer is an influential device that deliberately blocks, jams or interferes with authorized wireless communications in the particular arena. In the United States, jammers are illegal and their use can result in huge finesto user. In some cases, jammers work by the transmission of radio signals that disrupt the ongoing communications by decreasing the signal to noise ratio.The concept eventually can be used in wireless networks to disrupt information flow. It is a common form of censorship used in some countries, in order to prevent foreign radio stations& surveillance access points in border areas of nation from reaching the native country. Jamming is usually distinguished from interference, (normally mistaken) that can occur due to malfunctioning of device or other accidental situations.

Figure.3. Radio Signal Jammer

A) Distinction Between "Jamming" & "Interference"

Devices that simply cause interference in communication are regulated under different rules &regulations. Unintentional 'jamming' occurs when an operator transmits a frequency on a busy frequency without first checking it whether it is in use or not, or being unable to hear stations using the frequency. Another form of unintentional jamming occurs when equipment accidentally radiates or delivers a signal, such as a television cable plant that accidentally emits on an aircraft emergency frequency. Originally the terms “Jamming and Interference” were used interchangeably, but nowadays most radio users use the term "jamming" to describe the *deliberate* use of radio signals in an attempt to disrupt communication whereas the term "interference" is used to describe the *unintentional l* forms of disruption. However, the distinction is still not globally applied.

B) Methods

Intentional (known) communication jamming is usually aimed at to use radio signals to disrupt control over a specified communication field.A transmitter, tuned to the same frequency as the opponents' receiving equipment or point & with the same type of modulation used, with enough power, can override any signal at the receiver end. Digital wireless jamming for signals currently used such as Bluetooth &Wi-Fi are possible only with very low power. The most common types of this form of signal jamming are random noise, random pulse, stepped tones, warbler, random keyed modulated CW, tone, rotary, pulse, spark, recorded sounds, gulls, and sweep-through. These can be divided into two groups: -- obvious and subtle.

B.1) Obvious Jamming is easy to detect because it can be heard easily on the receiving equipment or point. It usually is a type of noise such as stepped tones (bagpipes), random-keyed code, pulses, music (often distorted), erratically warbling tones, highly distorted speech, random noise (hiss) and previously recorded sounds. Various combinations of these methods may be used often accompanied by regular identification signal to enable individual transmitters to be identified particularly in order to assess their efficiency. For example, China, which used jamming extensively and still does, plays a continuous loop of traditional Chinese music while it is jamming particular communication channels.The purpose of this type of jamming is to block reception of unwanted transmitted signals and to avoid any nuisance to the receiving operator.

B.2) Subtle Jamming is jamming during which no sound is heard on the receiving point. The radio doesn’t receive incoming signals unless everything seems superficially normal to the operator. These are often smart technical attacks on modern equipment, named such as "squelch capture". By FM capture effect, frequency modulated broadcasts may be eventually jammed, unnoticed by person, by a simple unmodulated carrier signal. Digital signals usea bit complex modulation techniques such as QPSK. These signals are very robust in presence of various interfering signals. However, the signal relies on hand shaking between the transmitter end & receiver end to identify and thereafter determine security settings and method of high level transmission of signal.

If the jamming device sends initiation data packets of the signal, the receiver will begin its working state to establish dual way data transmission communication. This method jams the receiver in an infinite loop where it keeps trying to start a connection but never completes it, which effectively blocks all possible legitimate communication. Bluetooth and other consumer radio protocols such as Wi-Fi have built in detectors in them so that they transmit only when the channel is completely free. Simple continuous transmission of a signal on a given channel will continuously stop a transmitter from transmitting the signal. Other jammers work by analyzing the packet headers & depending on the source or destination point, selectively transmit over the end of the message.

A) Mobile Phone Jammer Circuit Prototype

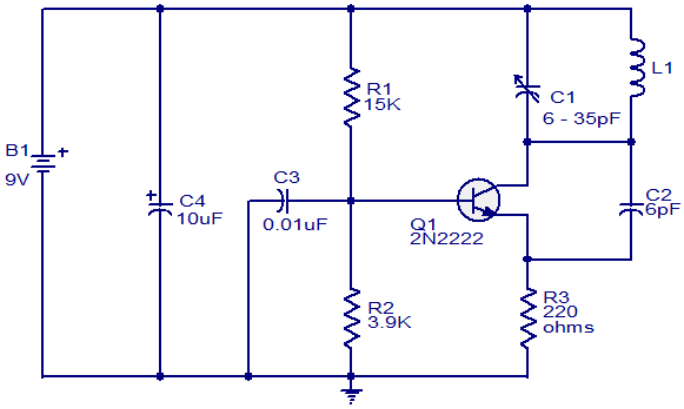


Figure.4.Radio Jammer Circuit Prototype

3. RADAR JAMMING & DECEPTION

Radarjamming and deceptionis the intentional (known) emission of the radio frequency signals to interfere with the operation of a radar in a fixed arenaby saturating its receiver with false information or noise. It can be classified into two types of radar jamming: *Mechanical* and *Electronic jamming*.

A) Mechanical Jamming

Mechanical jamming is caused by electronic devices which reflects or re-reflects radar energy back to the radar to produce false target returns signal on the operator's scope. Mechanical jamming devices include chaff, corner reflectors, &decoys.

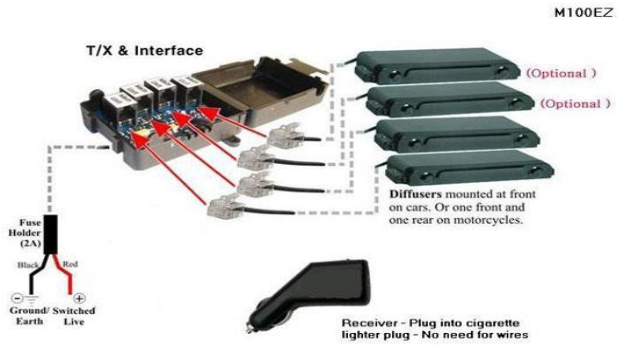


Figure. 5. Radar Jamming Equipment

- **Chaff**is made of different length metallic strips, which reflect different frequencies, so as to create a large area of false returns in which a real contact would be difficult to detect easily. Modern chaff is usually manufactured in of aluminum coated

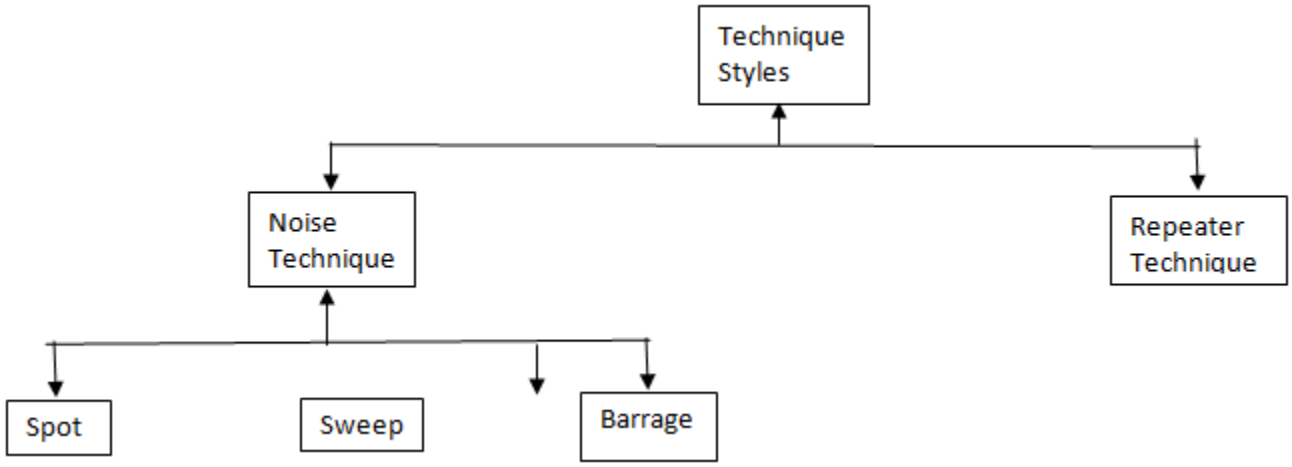
glass fibers of various lengths accordingly. Their extremely low weight and small size allows them to form a dense, long lasting cloud of interference.

- **Corner reflectors** have the same effect as chaff but are physically very different from these. Corner reflectors are multi-sided objects that re-radiate radar energy mostly backward to its source. An aircraft can't carry as many corner reflectors as it can chaff easily.

- **Decoys**are maneuverable flying objects that are intended to deceive or to fool a radar operator into circle believing that they are actually aircraft but it isn't true. They are much dangerous as they can clutter up a radar with false targets making it much easier for an attacker to get within weapons range and neutralize the radar easily. Corner Reflectors can be fitted on decoys to make them appear larger than they are, as illusion, thus furthering the illusion that a decoy is an actual aircraft, but it isn't. Decoys also have a deliberately sacrificial purpose, if needed i.e. defenders may fire guided missiles at targeting the decoys, thereby depleting limited stocks of expensive weaponry which might otherwise have been used against genuine targets effectively.

B) Electronic jamming

Electronic jamming is a form of electronic warfare where jammers radiate interfering signals toward an enemy's radar, blocking the receiver with highly concentrated energy signals barring the communication.



Flowchart 1.Jamming Styles Brief Description

Figure.6.German Luftwaffe Tornado ECR. This fighter specializes in electronic warfare.

- **Spot jamming** takes place when a jammer focuses all of its power contained on a single frequency. While this would degrade the ability to track on the jammed frequency, a frequency-agile radar would hardly be affected since the jammer can only jam one frequency at a time. While multiple jammers could possibly jam a definite range of frequencies, this would consume a great deal of resources to have an effect on a frequency-agile radar, and would probably still be ineffective.

- **Sweep jamming** is when a jammer's full power is shifted from one frequency to another at a time. While this has the advantage of being able to jam multiple frequencies in quick succession at an instant, it does not affect them all at the consecutive time, and thus limits the effectiveness of this type of jamming to a certain extent.

- **Barrage Jamming** is the jamming of multiple frequencies at an instant by a single jammer. The advantage is that multiple frequencies can be jammed simultaneously; however, the jamming effect can be limited to a limit because this requires the jammer to spread its full power between these defined frequencies.

- **Digital radio frequency memory, or DRFM jamming**, or **Repeater jamming** is a technique that manipulates received radar energy and re-transmits it to change what the radar sees. This technique can change the range the radar detects, by changing the delay in transmission of pulses, the velocity the radar detects by changing the Doppler shift of the transmitted signal, or the angle to the plane by using Amplitude Modulation techniques to transmit into the side lobes of the radar.

C) Countermeasures

- Constantly alternating the frequency that the radar operates on over a finite rangewill limit the effectiveness of most jamming. Modern jammers can track a pre-predictable frequency change, so, the more random is the frequency change, the more likely it is to counter the jammer effectively.

- Cloaking the outgoing signal with random noises makes it highly difficult for a jammer to figure out the exact frequency that a radar is operating on.
- The most important method to counter radar jammers is known as operator training. Any system can be easily fooled with a jamming signal but a properly trained operator pays attention to the raw video signal& can detect abnormal patterns on the radar screen.
- The best indicator to check the jamming effectiveness to the jammer is the countermeasures taken by the operator. The jammer does not know if their jamming is effective or not before operator starts altering radar transmission settings.
- Using EW countermeasures will give away radar capabilities easily, thus on peacetime operations most military radars are used on pre fixed frequencies, at minimum power levels& with blocked sectors towards possible listeners.
- Mobile fire control radars are usually kept passive or inactive when military operations are not ongoing to keep radar locations secret from enemy.
- Active electronically scanned array (AESA) radars are innately difficult to jam and can easily operate in Low Probability of Intercept (LPI) modes to reduce the chance of radar detection.
- A quantum radar system would automatically detect attempts made at deceptive jamming, which might otherwise go unnoticed & may turn to havoc later.

D) Stealth

Stealth technologies like radar-absorbent materials can be used effectively to reduce the return of a target increasing the security control.

E) Jamming police radar

Jamming radar for the purpose of defeating police radar guns is simpler than the military-grade radar jamming. The laws about jamming police radars are different in every country, sometimes it is illegal and in other countries it's legal.

F) Jamming in nature

The jamming of bat sonar by certain tiger moth species found in somespecial evergreen tropical areas has recently been confirmed. This can be seen as nature's equivalent of radar jamming.

G) Radar Jammer Circuit Prototype

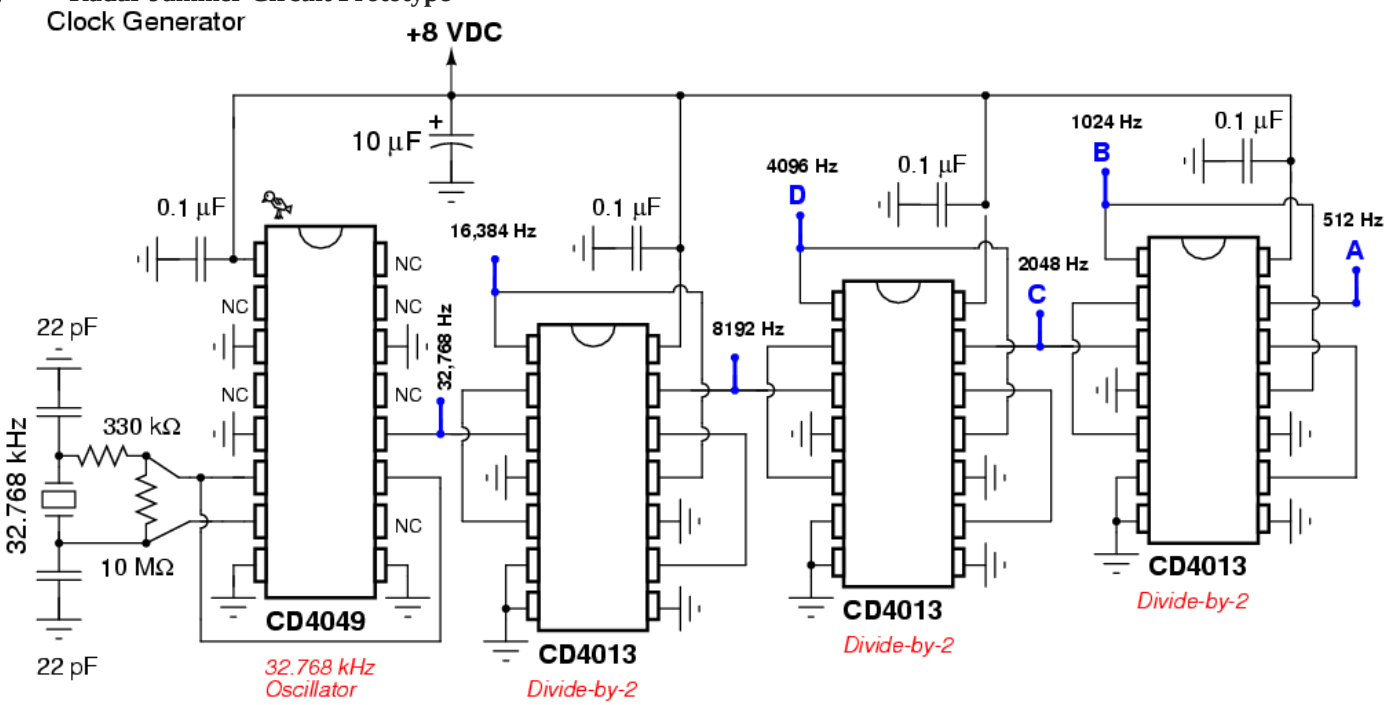


Figure.7.Radar Jammer Circuit Prototype

4. CONCLUSION & RESULT:

The above described paper covers the subject of jammer techniques widely. It defines the jammer, its types, legality, preventions, international laws etc. It also undergoes the detailed description & usage of jammers in engineering& defense & security sectors. It also gives the electronic circuit of its. This paper serves as the short & effective capsule for the electrical, electronics & communication engineering students.

5. ACKNOWLEDGEMENT:

We take this opportunity to express our deep sense of gratitude & whole hearted thanks to our Institution "Technovision, Lucknow, Uttar Pradesh" for inspiring and encouraging us to explore ourselves. Our Institute has always focused on providing us a framework for better future for mankind. Also in shaping us to become effective, skilled professionals in coming future. We are very thankful to the Institute's Management & our Director Sir for his kindness, constant encouragement, influential leadership & for the valuable time which he devoted to us. Also, thanks to our family & friends who directly & indirectly helped, supported & motivated us along the due course of completion of this informative paper

.

6. REFERENCE

[1]. A first course in electronic warfare By David Adamy, page 196

[2]."Radar Jammer Laws".

[3]. Corcoran, A. J.; Barber, J. R.; Conner, W. E. (16 July 2009). "Tiger Moth Jams Bat Sonar". Science. 325 (5938): 325–327. PMID 19608920. doi:10.1126/science.1174096.

[4]. "European Commission, Enterprise and Industry, Interpretation of the Directive 1999/5/EC". Retrieved 20 October 2014.

[5]. "Mobiles jammed in prisons". One News. August 21, 2007. Retrieved October 25, 2011.

[6]. FCC: Wireless Services: Cellular Services: Operations: Blocking &Jamming Archived November 18, 2016, at the Wayback Machine.

[7]. Office of Research, USIA (1983), Jamming of Western Radio Broadcasts to the Soviet Union and Eastern Europe, United States Information Agency

7. AUTHOR PROFILE

a) Mr. VISHWAJEET SINGH is persuing the B.Tech in Mechanical Engineering from Rajarshi Rananjay Sinh Institute of Management & Technology, Amethi. Currently, He is a student of Third Year (B. Tech). He has published 5 International papers till date with different Journals. He has also received an award for academic excellence by INDUS Foundation in International Indo-American Summit September, 2016 in New Delhi.

b) Mr. SUBODH CHAUHAN is persuing the B.Tech in Electronics & Communication Engineering from Rajarshi Rananjay Sinh Institute of Management &Technology, Amethi. Currently, he is a student of Third Year.

c) Mr. SUSHIL KUMAR ispersuing the B.Tech in Electronics & Communication Engineering from RajarshiRananjaySinh Institute of Management &Technology, Amethi. Currently, he is a student of Third Year.

d) Mr. AMAN SINGH is persuing the B.Tech in Electronics & Communication Engineering from RajarshiRananjaySinh Institute of Management & Technology, Amethi. Currently, he is a student of Third Year.

e) Mr. PRATEEK RAWAT is persuing the B.Tech in Electronics & Communication Engineering from Rajarshi Rananjay Sinh Institute of Management & Technology, Amethi. Currently, he is a student of Third Year.