IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 4, April 2017

Security Issues in IoT Based Smart and Multi-Functional Energy Meter

Mr. Lalit Ajit[1], Prof. Yogesh Bhute[2]

M.E. Student, Dept of IT, Abha-Gaikwad Patil College of Engineering, Nagpur, India[1]

HOD, Dept. of IT, Abha-Gaikwad Patil College of Engineering, Nagpur, India[2]

Abstract: The IoT based Smart and Multi-Functional Energy meter is designed to send actual enrgy consumption date of the consumer to the server of the electricity office with the help of Zigbee technology .This data is stored on the database where different parameters are observed such as tampering of meter. We are using zigbee module at the transmitter side and receiver side. Data is stored on the local database with the help of serial port of the computer. Remote connection and disconnection can be done from the electricity office side. External tampering of meter can also be prevented. In this process, there should not be any unwanted interference from the external attackers. Different types of attacks can be possible such as DoS attack. The aim of this paper to discuss various security issues for transmitting consumption data whose integrity is very important for both consumer as well as for electricity board.

Keywords: Zigbee, IoT, Denial of Service (DoS) etc.

I. INTRODUCTION

Peer-to-Peer Network: A peer-to-peer (P2P) network is a group of computers each of which acts as a node for sharing of files within the group. Instead of having a central server to act as a shared drive, each computer acts as the server for the files stored upon it. When a peer to peer network is established over the Internet, a central server can b e used to index files,or a distributed network can be established over the Internet, a central server can be used to index files, or a distributed network can be established where the sharing of files is split between all the users in the network that are storing a given file. A Smart meter can use Session Initiation Protocol (SIP).SIP is an open and standards-based technology, which provides a robust communication medium for the smart grid applications.
In the most basic sense, a peer-to-peer network is a simple network where each computer doubles as a node and a server for the files it exclusively holds. However, when P2P networks are established over the Internet, the size of network and files.

II. SECURITY ISSUES IN SMART METER

Smart follows all the security goals such as Confidentiality, integrity and availability. Confidentiality: Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. Confidentiality not only applies to the storage of information, it also applies to the transmission of information.

Integrity: Information needs to be changed constantly. Integrity means that changes need to be done only by authorized entities and through authorized mechanism. Integrity violation is not necessarily the result of a malicious act, an interruption in the system ,such as power surge, may also create unwanted changes in some information.

Availability: The third component of information security is availability. The information created and stored by an organization needs to be available to authorized entities. Information is useless if it is not available. Information needs to be constantly changed, which means it must be accessible to authorized entities. The unavailability of information is just as harmful for an organization as the lack of confidentiality or integrity.

III. APPLICATIONS AND ADVANTAGES

Smart Grid System determines the need of aspects such as daily workflow, workforce management, asset management, call center philosophy, billing systematic etc. Smart meter can enhance the operations of SCADA system. As smart meter system provides several benefits such as efficient power system control and monitoring, operational decisions those are taken timely to minimize outages and losses. Particularly in micro-gridds, smart meters can perform energy cost allocation, fault analysis, demand control and power quality analysis. Smart meter can schedule preventive

DOI 10.17148/IJIREEICE.2017.5427

maintenance, and support the operation of check meters for accurate billing. Pattern recognition techniques can also be employed to be part of the Smart metering in order to gain access to the performance information of the devices and financial incentives to the customer.

Smart meters encourage consumers to conserve energy by helping them maintain the quantity and cost of their energy consumption. Power strip smart meters can be employed to monitor and control the appliances of customers. These meters provide data identity and location of home appliance under operation. Geographical Information System(GIS) can be integrated to the smart meter system in order to obtain specific operation regarding the geographical location of a potential fault. Advanced Metering Infrastructure(AMI):AMI includes the both the physical smart meter(a digital electricity meter located at the end consumer that enables two-way communication) as well as the communications infrastructure to transport the data that is generated.The latter involves the development of an intelligent field area network, that will facilitate the communications link back to the utility's operation and control center,but also to the network inside the home or building.One of the key outstanding questions in the AMI space is how smart meters will communicate with one another and with other devices on the grid.Here there are three main competing technologies:broadband over powerlines,radio frequency mesh networks, and cellular networks.

IV. SMART METER COMMUNICATION PROTOCOLS

DLMS(Distribution Line Message Specification) is an international communication standard running on a client-server principle. The connection here is established by the client. The client can communicate with more servers,or other way around, more clients can communicate with one server. The DLMS protocol became a global standard for Smart Meter designers. A Smart meter is an intelligent devices which can measure electronically how much energy is consumed and communicate the collected data to another device. For example, smart meters can send the electricity consumption data of household devices to a server on the Internet. The server is responsible for collecting data of household devices to a server on the Internet. The server is responsible for collecting the message from smart meter networks and analyzing the data delivered by these messages. Smart meters are transforming the traditional metering infrastructure towards the advanced metering infrastructure(AMI).Smart meter networks involve one-way or two-way communication depending on requirements of customers and providers. Many communications can either be from a meter to other devices inside the same local area network, from the meter to the providers information technology(IT) infrastructure or both. There are numerous communication technologies for both cases, including both wireless and wireline. Distributed denial of service(DDoS) is a common attack against availability. The main purpose of DDoS attacks in AMI is to attack data collector, preventing the normal communication between WAN and NAN. DDoS attacks against data collector. Assuming that the attacker's entry point is the smart meter by using the weaknesses of network .

V. DIFFERENT MESSAGE CLASSES IN SMART NETWORKS

Smart meter networks are part of service-based AMI. It supports the interaction between the provider and customers using predefined messages. This article proposes five fundamental message classes: control,request,billing,electricity usage and warning. Furthermore,these five message classes can be classified into three categories: operation,non-opertation and asynchronous event.

Operation:
Control messages: The server can send control messages to control smart meters or any electrical equipment in the smart meter network.
For example,the server can send a "Turn Off" control message to turn off a smart meter or an outlet.
Request messages:
The server can request information from the smart meters network when needed.
For example,the server can request the smart meter to transmit the electricity consumption data for a specific time period.

Asynchronous Event:
Warning messages:
When some emergency events happen, the smart meter can notify the server immediately.The server can take contingency measure to handle such critical events.
For example: When the value of voltage is over normal,the smart meter can send a warning message to notify the sever before the disaster occurs.

Securing Data Access: Securing data access is performed against any client access to all meter's objects.Three levels of security for authenticating the identity of a client establishing the connection are used.

DOI 10.17148/IJIREEICE.2017.5427

Based on this authentication,the client is granted access rights to individual objects.
1]Lowest Level Security:There is no authentication performed with this type of security.It must be supported by the Management of Logical Device.
2]Low Level Security-Here,the client must provide a password.The password can be overheard.
3]High Level Security:The highext possible security utilizing algorithms and encryption keys.This type of security is used only in cases when it is not possible to prevent overhearing of the communication channel

VI. THREATS ON SMART METER

Privacy:

Types of attacks on smart meters can be generally classified as physical (external tampering, neutral bypass, missing neutral etc.), electrical (over/under voltage, circuit probing, ESD etc.), and software and data (spy software insertion, cyber attacks). Except for physical tampering of the meter, the majority of these known vulnerabilities are associated with communication media and communication protocols as the grid becomes networked. Solutions for physical tampering include using magnetometer sensors (to detect powerful magnetic fields which affect meter readings in current transformer-based electricity meters), tilt sensors which detect removal or physical tampering of meters from authorized locations, usage of tampering algorithms as part of firmware that helps ensure billing is continued, and anti-tamper switches that can be placed on the casing of the meter to trigger a tamper when the casing is opened. The AMI includes software, hardware, communications, customer-associated systems and meter data management (MDM) software. As meters become smart and networked, meter software must have adequate security against any unauthorized change in software configurations, reading of recorded data, change of calibration data, etc. Secure techniques need be integrated in the solution to secure the communication channels and ensure physical security of assets to make smart grids more secure and reliable.
Key Generation and Storage of Cryptography Algorithms Almost all security passwords and cryptography keys rely on random seed. The use of a pseudo-random number to generate secret keys can result in pseudosecurity. The National Institute of Standards and Technology (NIST) recommends using a FIPS 140-2 compliant random number generator for a high level of security. It is recommended that the random number be generated in hardware instead of software and keys erased in a tamper event.

VII. ZIGBEE SECURED COMMUNICATION NETWORK

Fig.Zigbee module

Zigbee Technology is a bi-directional wireless communication technology of short distance,low complexity,low cost, low power consumption, and low data rate,mainly used in automatic control.It mainly works on 2.4GHz ISM band with 20-250Kbit/s data rate,100m-1.5Km maximum transmission range.and typical; 100m distance.
The technical features include:

[1]Security: Zigbee provides data integrity check and authentication, and uses AES-128 security algorithm.Each application has the flexibility to determine its safety properties.
[2]Reliability: It uses collision avoidance mechanism, and at the same time it reserves a dedicated time slot to require a fixed bandwidth of the communication service, avoid the competition and conflicts when data is sent.MAC layer uses a full confirmation of data transfer mechanisms, and each packet of data sent must wait to recive confirmation.
[3]Low cost: The zigbee modules are very cost effective so they can be deployed in a project and Zigbee protocol is free of royalities.
[4]Power Saving: As the duty cycle is very short ,transmitting and reciveing information has lower power consumption, and using the hibernation mode.Zigbee technology ensures that two N size batteries can support from 6 months to 2

DOI 10.17148/IJIREEICE.2017.5427

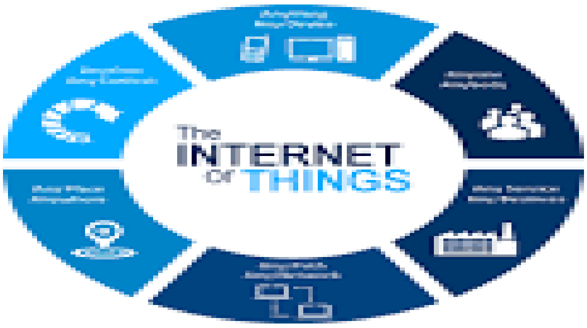
years. Of course, different applications have power different power consumptions.
[5]High Network capacity: A zigbee network can accommodate a maximum of 65536 devices.
[6]Short delays: Enhanced communication delays for delay-sensitive applications.Communication delay and sleep wake up time delay is 15ms and active channel access delay is 15 ms.

Main application of Zigbee are within short range and data transfer rate among the various electronic equipments is not high.The typical transfer data types are periodical data(such as sensor data), intermittent data(such as lightning control), and repetitive low latency data (such as mouse).

VIII. SECURE COMMUNICATION PROTOCOLS

Today, there are several data exchange protocols used between entities within the power grid. Protocols like Transmission Control Protocol (TCP)/Internet Protocol (IP), Hypertext Transfer Protocol (HTTP), and File Transfer Protocol (FTP) are widely used in the global information technology domain. These are not very secure and are vulnerable since the data transferred can easily be eavesdropped by the hacker. For the power grid or smart metering, insecure protocols must be replaced with protocols which offer a high level of security like Internet Protocol Security (IPSec), Secure Socket Layer (SSL), Transport Layer Security (TLS) and Secure Shell (SSH). IPsec uses encryption technology to provide data confidentiality, integrity and authenticity between participating peers in a private network.
High Level Security for Control and Commands: Symmetric key cryptography like AES is good for bulk data but may not offer the highest level of security. Asymmetric key cryptography such as elliptic curve digital signature algorithm (ECDSA) can be used to encrypt any control/commands like remote disconnect/connect real time pricing changes, etc. This ensures a higher level of authentication for the commands to control grid equipments. Key exchanges based on elliptic curve cryptography (ECC) can offer a high level of security. ECC can also be used by wireless networks like Zigbee® to offer digital certificates to exchange information between ZigBee nodes/devices within a smart grid ecosystem.
Secure Debug and Client/Server Authentication: Access should only be allowed with an authentication key. Freescale offers a wide range of 32-bit MCUs and MPUs (the Kinetis family of ARM® Cortex™-M4 core-based MCUs and Power Architecture® based MPUs) that support the security features covered in this article. For ensuring physical security through magnetic field detection and tilt sensing, accelerometers and magnetometers are also available. In some cases, where it is essential to address requirements which call for a separate security device, Freescale partner Inside Secure offers a security chip called VaultIC that features tamper resistance, secure secret keys and certificates storage, on-board
key generation, secure implementation of standards algorithms (i.e. AES, ECC), security functions (mutual authentication, verify/ generate certificate, encryption/decryption, true random number generation), third-party security-level evaluation, and is FIPS140-2 Level 3 and EAL4+ ready. VaultIC, along with the Freescale application processor, makes it possible to implement a highly secure smart electricity meter or an energy gateway. Security through anonymity is no longer an option in today's environment. Implementation of the highest levels of available security helps protect ones physical, data and information assets and ensures customer privacy.

IX. PROTOCOLS USED FOR IOT



Our main motivation was to create an IoT test-bed where to test communications protocols and also innovative applications that could be applied to a gamut of scenarios. While searching for the appropriate application layer protocols to use, we found out that while comparisons can be found between two protocols, there is no paper over viewing all the possible alternatives with pros and cons. The main motivation of this paper is to fill this gap and provide a brief yet accurate description of the key protocols that are being used today to implement the IoT. More specifically,

DOI 10.17148/IJIREEICE.2017.5427

we will discuss on the following list of protocols being used alternatively or jointly to solve different needs of the communication between machines:

1) CoAP: Constrained Application Protocol. 2) MQTT: Message Queue Telemetry Transport.
3) XMPP: Extensible Messaging and Presence Protocol. 4) RESTFUL Services: Representational State Transfer.
5) AMQP: Advanced Message Queuing Protocol 6) Websockets.

2.1CoAP The Constrained Application Protocol (CoAP) is a synchronous request/response application layer protocol that was designed by the Internet Engineering Task Force (IETF) to target constrained-recourse devices. It was designed by using a subset of the HTTP methods making it interoperable with HTTP. CoAP runs over UDP to keep the overall implementation lightweight. It uses the HTTP commands GET, POST, PUT, and DELETE to provide resource-oriented interactions in a client-server architecture. CoAP is a request/response protocol that utilizes both synchronous and asynchronous responses. The reason for designing a UDP-based application layer protocol to manage the resources is to remove the TCP overhead and reduce bandwidth requirements. Additionally, CoAP supports unicast as well as multicast, as opposed to TCP, which is by its nature not multicastoriented. Running on the unreliable UDP, CoAP integrated its own mechanisms for achieving reliability. Two bits in the header of each packet state the type of message and the required Quality of Service (QoS) level. There are 4 message types: 1. Con_rmable: A request message that requires an acknowledgement (ACK). The response can be sent either synchronously (within the ACK) or if it needs more computational time, it can be sent asynchronously with a separate message. 2. Non-Con_rmable: A message that does not need to be acknowledged. 3. Acknowledgment: It confirms the reception of a confirmable message. 4. Reset: It confirms the reception of a message that could not be processed. There is also a simple Stop-and-Wait retransmission mechanism for confirmable message sand a 16-bit header field in each CoAP packet called Message ID which is unique and used for detecting duplicates. CoAPC HTTP Mapping enables CoAP clients to access resources on HTTP servers through a reverse proxy that translates the HTTP Status codes to the Response codes of CoAP. Even though CoAP was created for the IoT and for M2M communications, it does not include any built-in security features. 2.2 Message Queue Telemetry Transport (MQTT): It was released by IBM and targets lightweight M2M communications. It is an asynchronous publish/subscribe protocol that runs on top of the TCP stack. Publish/subscribe protocols meet better the IoT requirements than request/response since clients do not have to request updates thus, the network bandwidth is decreasing and the need for using computational resources is dropping. In MQTT there is a broker (server) that contains topics. Each client can be a publisher that sends information to the broker at a specific topic or/and a subscriber that receives automatic messages every time there is a new update in a topic he is subscribed. The MQTT protocol is designed to use bandwidth and battery usage sparingly, which is why, for example, it is currently used by Facebook Messenger. MQTT ensures reliability by providing the option of three QoS levels:

1. Fire and forget: A message is sent once and no acknowledgement is required. 2. Delivered at least once: A message is sent at least once and an acknowledgement is required. 3. Delivered exactly once: A four-way handshake mechanism is used to ensure the message is delivered exactly one time. Even though MQTT runs on TCP, it is designed to have low overhead compared to other TCPbased application layer protocols. Moreover, the publish/subscribe architecture that it used, is more suitable for the IoT than request/response of CoAP, for example, because messages do need to be responded. This means lower network bandwidth and less message processing that actually extends the lifetime of battery-run devices. To ensure security, MQTT brokers may require username/password authentication which is handled by TLS/SSL (Secure Sockets Layer), i.e., the same security protocols that ensure privacy for HTTP transactions all over the Internet. By comparing MQTT with the aforementioned CoAP, it is possible to see that the UDPbased CoAP has lower overhead than the TCP-based MQTT. However, due to the lack of TCPs retransmission mechanisms, packet loss is more likely to happen when using

2.3 The Extensible Messaging and Presence Protocol (XMPP) It was designed for chatting and message exchanging. It was standardized by the IETF over a decade ago, thus being a well-proven protocol that has been used widely all over the Internet. However, being an old protocol, it falls short to provide the required services for some of the new arising data applications. For this reason, last year, Google stopped supporting the XMPP standard due to the lack of worldwide support. However, lately XMPP has re-gained a lot of attention as a communication protocol suitable for the IoT. XMPP runs over TCP and provides publish/subscribe (asynchronous)and also request/response (synchronous) messaging systems. It is designed for near real-time communications and thus, it supports small 2.3 The Extensible Messaging and Presence Protocol (XMPP) It was designed for chatting and message exchanging. It was standardized by the IETF over a decade ago, thus being a well-proven protocol that has been used widely all over the Internet. However, being an old protocol, it falls short to provide the required services for some of the new arising data applications. For this reason, last year, Google stopped supporting the XMPP standard due to the lack of worldwide

DOI 10.17148/IJIREEICE.2017.5427

support. However, lately XMPP has re-gained a lot of attention as a communication protocol suitable for the IoT. XMPP runs over TCP and provides publish/subscribe (asynchronous)and also request/response (synchronous) messaging systems. It is designed for near real-time communications and thus, it supports small message footprint and low latency message exchange. As the name explicitly states, XMPP is extensible and allows the specification of XMPP Extension Protocols (XEP) that increase its functionality. XMPP has TLS/SSL security built in the core of the specification. However, it does not provide QoS options that make it impractical for M2M communications.

2.4 RESTful Services The Representational State Transfer (REST) is not really a protocol but an architectural style. It was first introduced by Roy Fielding in 2000, and it is being widely used ever since. REST uses the HTTP methods GET, POST, PUT, and DELETE to provide a resource oriented messaging system where all actions can be performed simply by using the synchronous request/response HTTP commands. It uses the built-in accept header of HTTP to indicate the format of the data that it contains. The content type can be XML or JSON (JavaScript Object Notation) and depends on the HTTP server and its configuration. REST is already an important part of the IoT because it is supported by all the commercial M2M cloud platforms. Moreover it can be implemented in smartphone and tablet applications easily because it only requires an HTTP library which is available for all the Operative Systems (OS) distributions. The features of HTTP can be completely utilized in the REST architecture including cashing, authentication, and content typenegotiation. RESTful services use the secure and reliable HTTP which is the proven worldwide Internet language. It can make use of TLS/SSL for security. However, today most commercial M2M platforms do not support HTTPS requests. Instead, they provide unique authentication keys that need to be in the header of each request to achieve some level of security. Even though REST is already used widely in commercial M2M platforms, it is unlikely that it will become a dominant protocol due to not being easily implementable. It uses HTTP which means no compatibility with constrainedcommunication devices. This leaves its use for final applications. Given the current tendency for applications running on smartphones, tablets and pads, the additional overhead associated to request/response protocols affect battery usage, as it also does the continuous polling or long polling for values especially when there are no new updates and the overhead becomes useless. Issues that can be avoided if a publish/subscribe protocol is used such as MQTT or XMPP. CoAP on the other hand, which is the lightweight version of REST, bears the same disadvantages of the request/response architecture. However it is designed to run over UDP making it capable of being used be constrained resource devices, counter to REST. 2.5 Advanced Message Queuing Protocol (AMQP): The Advanced Message Queuing Protocol (AMQP) is a protocol that arose from the financial industry. It can utilize different transport protocols but it assumes an underlying reliable transport protocol such as TCP AMQP provides asynchronous publish/subscribe communication with messaging. Its main advantage is its store-andforward feature that ensures reliability even after network disruptions. It ensures reliability with the following message-delivery guarantees: 1. At most once: means that a message is sent once either if it is delivered or not. 2. At least once: means that a message will be definitely delivered one time, possibly more. 3. Exactly once: means that a message will be delivered only one time. Security is handled with the use of the TLS/SSL protocols over TCP.

2.6 WEBSOCKET: The Websocket protocol was developed as part of the HTML 5 initiative to facilitate communications channels over TCP. Websocket is neither a request/response nor publish/subscribe protocol. In Websocket a client initializes a handshake with a server to establish aWebsocket session. The handshake itself is similar to HTTP so that web servers can handle Websocket sessions as well as HTTP connections through the same port. However, what comes after the handshake does not conform to the HTTP rules. The session can be terminated when it is no longer needed from either the server or the client side. Websocket was created to reduce the Internet communication overhead while providing real-time fullduplex communications. There is also a Websocket subprotocol called Websocket Application Messaging Protocol (WAMP) that provides publish/subscribe messaging systems.

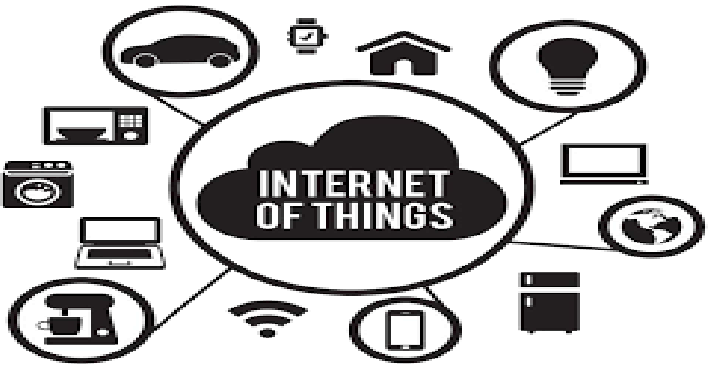


Fig- IoT communication

DOI 10.17148/IJIREEICE.2017.5427

Websocket runs over the reliable TCP and implements no reliability mechanisms by its own. If needed, the sessions can be secured using the Websocket over TLS/SSL. During the session, Websocket messages have only 2 bytes of overhead. As reported by relevant studies, the HTTP polling (in REST) repeats header information when the data transmission rate increases, thus increasing latency. Websocket is estimated to provide a three-to-one reduction in latency against the half-duplex HTTP polling. Websocket is not designed for resource constrained devices as the previous protocols and its client/server based architecture does not suit IoT applications. However it is designed for real-time communication, it is secure, it minimizes overhead and with the use of WAMP it can provide efficient messaging systems. Thus, it can compete any other protocol running over TCP.

X. CONCLUSION

In this paper, we have discussed various issues which can create hurdles in proper data management with IoT based Smart and Multi-functional Energy meter. How, to overcome the hurdles which are created for proper data management between meters.

ACKNOWLEDGMENT

We express our sincere gratitude to **Prof. Yogesh Bhute**, HOD, Department of IT, Abha-Gaikwad Patil College of Engineering, Nagpur for extending his valuable insight for completion of work.

REFERENCES

[1] D.Mohanapriya, T.Shanthi “Embedded Based Optimization Power Consumption in Smart Grid” International Journal of Emerging Technology and Advanced Engineering.

[2] S.W.Lee,C.S.Wu,W.M.S. Chiou and K.T.Wu “Design of an Automatic Meter Reading System”

[3] Bharath P,Ananth N,Vijeta S,Jyoti Prakash K.V.,”Wireless automated digital Energy Meter” , ICSET 2008

[4] Yin-Kang,L.Xiang-yang and X.Jing, “the Hardware Design of Concentrator for Wireless Intelligent Meter Reading System”, Element and IC,no. 1 ,pp 37-39,2005

[5] G.Song,F.Ding.W.Zhang and A.Song, “ A Wireless Power Outlet System for Smart Homes”, IEEE Trans Consumer Electronics,vol.54, no. 4,Nov 2008

[6] Li Kaicheng,Liu Jiafong, yue Conyuam and Zhang Ming, “Remote Power Measurement and Meter-Reading System Based on ARM Microprocessor”, Proc .IEEE Conference on Precision Electromagnetic Measurements Digest, Pp 219-217 June 2008

BIOGRAPHY

Mr. Lalit Laxman Ajit received B.E. Degree in Electronics and Communication Engineering from Manoharbhai Patel Institute of Engineering and Technology (MIET), Gondia in 2007. Currently, he is pursuing M.E. in Wireless Communication and Computing from Abha-Gaikwad Patil College of Engineering, Nagpur.

DOI 10.17148/IJIREEICE.2017.5427