A Smart Automation of ZigBee through GPRS

Dr. K Rameswaraiah[1], D. Vara Prasad[2] and Mahendradatta[3]

***Abstract*---**The last two decades onwards WSN's it plays a vital role in communication system. Manual operations are replaced by automatic system to perform efficient and effective data transmission. ZigBee has a great magnitude for remote accessing and control. Smart grid could be referred as electric grid for the purpose of enabling bidirectional flow of information and electricity .The purpose of paper is to communicate with GPRS by the ZigBee network and home automation for indentifying defectives and controlling / monitoring the home appliances. The operation and control of the next generation electrical grids will depend on a complex network of computers, software, and communication technologies. Being compromised by a malicious adversary would cause significant dam- age, including extended power outages and destruction of electrical equipment. Moreover, the implementation of the smart grid will include the deployment of many new enabling technologies such as advanced sensors, metering, and the integration of distributed generation resources. Such technologies and various others will require the addition and utilization of multiple communication mechanisms and infrastructures that may suffer from serious cyber vulnerabilities

***Keywords*--** Medium Access Control (MAC), Physical Layer (PHY), WPAN, Open Systems Interconnection (OSI), AES.

I. INTRODUCTION

ZIGBEE is a specification for a suite of high level communication protocols using small, low-power digital radios based on an IEEE 802 standard for personal area networks[5]. ZigBee devices are often used in mesh network form to transmit data over longer distances, passing data through intermediate devices to reach more distant ones. This allows ZigBee networks to be formed ad-hoc, with no centralized control or high-power transmitter/receiver able to reach all of the devices.

Dr. K Rameswaraiah[1] is Professor, Department of CSE.

D.Vara Prasad is Asst.Professor, Department of ECE ST. Peter's Engineering College, Hyderabad, India.

Mahendradatta is a Student, Department of IT ST.Peter's Engineering College, Hyderabad, India

Any ZigBee device can be tasked with running the network. ZigBee is a specification for a communication protocol using small low-power digital radios based on the IEEE 802.15.4 standard. It is more specifically known as low-rate wireless personal area networks (LR-WPANs). Confidentiality of a ZigBee network is established though utilizing the AES algorithm. Moreover, frame integrity is achieved by generating integrity codes. ZigBee devices authenticate by employing predefined keys. Additionally, ZigBee networks provide security countermeasures against message replays by ensuring freshness of transmitted frames.

The 802.15.4[6] protocol is vulnerable to jamming. This threat aims to weaken the availability of system services. Another threat is characterized by message capturing and tampering, which are difficult to avoid in LR-WPANs, since the cost of sufficient physical protection ZigBee is targeted at applications that require a low data rate, long battery life, and secure networking. ZigBee has a defined rate of 250 Kbit/s, best suited for periodic or intermittent data or a single signal transmission from a sensor or input device. Applications include wireless light switches, electrical meters with in-home-displays, traffic management systems, and other consumer and industrial equipment that requires short-range wireless transfer of data at relatively low rates. The technology defined by the ZigBee specification is intended to be simpler and less expensive than other WPANs, such as Bluetooth or Wi-Fi[4].

Fig. 1: Different kinds of Wireless Technologies.

ZigBee is a low-cost, low-power, wireless mesh network standard. The low cost allows the technology to be widely deployed in wireless control and monitoring applications. Low power-usage allows longer life with smaller batteries. Mesh networking provides high reliability and more extensive range. ZigBee chip vendors typically sell integrated

radios and microcontrollers with between 60 KB and 256 KB flash memory. ZigBee operates in the industrial, scientific and medical (ISM) [4] radio bands; 868 MHz in Europe, 915 MHz in the USA and Australia and 2.4 GHz in most jurisdictions worldwide. Data transmission rates vary from 20 to 250 kilobits/second. The ZigBee network layer natively supports both star and tree typical networks, and generic mesh networks. Every network must have one coordinator device, tasked with its creation, the control of its parameters and basic maintenance. Within star networks, the coordinator must be the central node. Both trees and meshes allows the use of ZigBee routers to extend communication at the network level. ZigBee builds upon the physical layer and medium access control defined in IEEE standard 802.15.4 (2003 version) for low-rate WPANs.

II. ZIGBEE ARCHITECTURE

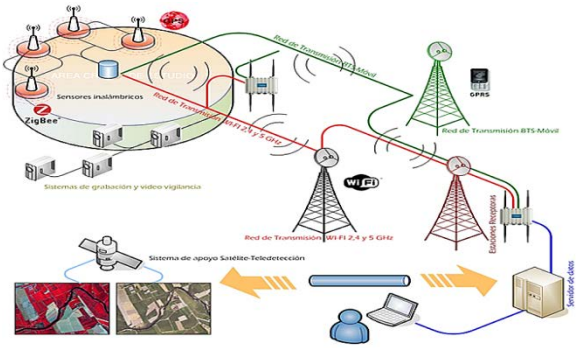

Fig. 2: architecture of ZigBee.

A. *Basic Characteristics Of Zigbee:*

2.4 GHz and 868/915 MHz dual PH modes represents three license free bands :2.4-2.4835 GHz,868-870 MHZ. and 902-928 Mhz. the number of channels allotted to each frequency band is fixed at sixteen (numbered 11-26),one(numbered0) and ten (numbered 1-10) respectively. The higher frequency band is applicable world wide, and lower band in the areas of North America, Europe, Australia and New Zealand. Maximum data rates allowed for each of these frequency bands are fixed as 250 kps @ 2.4 GHz. 40kbps@915MHZ and 20kbps@868 MHZ. High throughout and low latency for low duty-cycle applications (<0.1%) Fully reliable "hand-shaked" data transfer protocol .Different topologies as illustrated below: star, peer-to-peer, mesh [5]

2.2 *Frame structure*

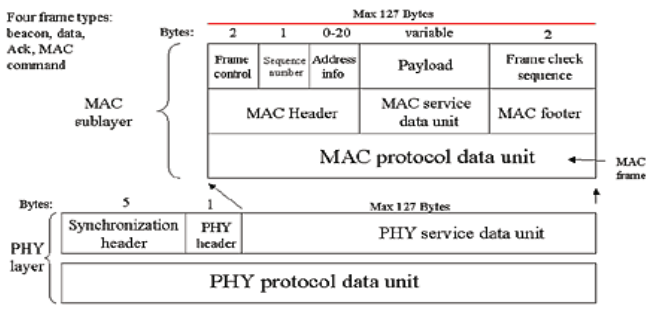

Fig. 3: Frame Structure.

The data frame provides a payload of up to 104 bytes. The frame is numbered to ensure that all the packets are tracked. If a frame check sequence ensures the packet are received without errors. The frame structure improves reliability in difficult conditions that the device takes advantage of "quite time" between frames to send a short packet immediately after the data packets transmission. A MAC command frame provides the mechanism for remote control and configuration of client nodes. A centralized network manager uses MAC configure in stead of clients, command frames no matter how large the network. Finally beacon frame wake up client devices which listens fro their address and go back to stay if they do not receive it. Beacons are important mesh and cluster tree networks to keep all the nodes synchronized without requiring that node to consume precious battery energy by listening for long periods of time.

III. THEORY OF TECHNOLOGIES

A. *Channel accessing and addressing*

Two channel access mechanisms are implemented in 802.15.4 for a known beacon network, and standard Aloha. CSMA-CA [5] (carrier sense medium access with collision avoidance) communicates with the positive acknowledgement for successfully received packets. In a beacon enabled network a super frame structure is used to control channel access. The super frame is setup by the network coordinator to transmit beacons at pre determined intervals and provides 16 equal width time slots between beacons for contention free channel access in each time slot.

The structure guarantees the dedicated bandwidth and low latency. Channel access to each device address employees 16 bit IEEE and optional 16-bit short addressing. The address free within the MAC can contain both source and destination addressing information. This dual address information is used in mesh network to prevent a single point of failure with a network.

IV. DEVICE TYPES:

These devices have 64-bit IEEE address with optioned to enable to shorter address to reduce packet size, and work in either two addressing modes. Star or peer to peer.
ZigBee network uses three device types

1. The network coordinator: maintains overall network knowledge. It is most sophisticate d and requires the most memory and computing power.
2. The full function device (FFD): supports all 802.15.4 functions and features specified by the standard. it can function as a network coordinator, additional memory and computing power make it ideal for network router function or it could be used in network-edge devices.
3. The reduced function devices {RFD} carries limited functionality to lower costs and complexity .it generally found in network devices.

V. SECURITY:

The zigBee technology provides the high level security with compare to the other technology like Bluetooth and Infrared Security and data integrity of the key benefits of the ZigBee technology .ZigBee leverages the security model of the IEEE 802.15.4 MAC sub layer which specifies four security services.

Access control – the device maintains a list of trusted devices within the network.

Data encryption – This uses symmetric key. 128-bit advanced encryption standards

Frame integrity- to protect data from being modified by parties without cryptographic keys.

Sequential freshness to reject data frames that have been replayed—the network controller compares the freshness value with the last known value from the device.

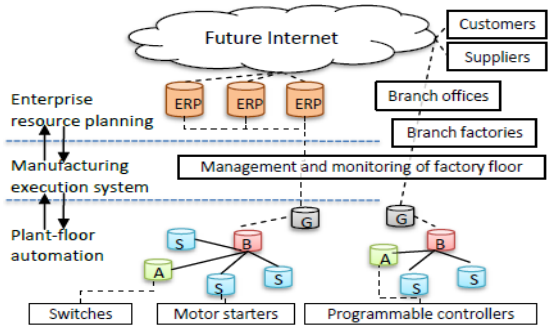

Fig. 4: Network Structure.

VI. THE APPLICATIONS:

- Home Entertainment and Control — Home automation, smart lighting, advanced temperature control, safety and security,
- Wireless sensor networks — Starting with individual sensors like Telosb/Tmote and Iris from Memstic
- Industrial control
- Embedded sensing
- Medical data collection
- Smoke and intruder warning
- Building automation
- Traffic Management
- Agriculture &Military Applications

VII. ZIGBEE DEVICES:

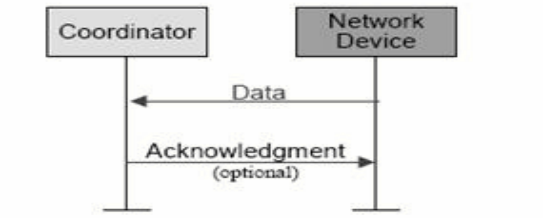

Fig. 5: ZigBee Communication.

- **ZigBee Co-coordinator (ZC):** The most capable device, the coordinator forms the root of the network tree and might bridge to other networks. There is exactly one ZigBee coordinator in each network since it is the device that started the network originally (the ZigBee Light Link specification also allows operation without a ZigBee coordinator, making it more usable for over-the-shelf home products) [7]. It stores information about the network, including acting as the Trust Center & repository for security keys.
- **ZigBee Router (ZR):** As well as running an application function, a Router can act as an intermediate router, passing on data from other devices [6].

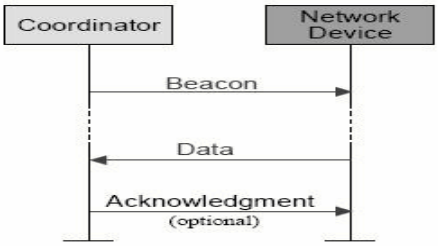

Fig. 6: ZigBee Communication-Response.

- **ZigBee End Device (ZED):** Contains just enough functionality to talk to the parent node (either the Coordinator or a Router); it cannot relay data from other devices. This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life. A ZED requires the least amount of memory, and therefore can be less expensive to manufacture than a ZR or ZC. ZigBee protocols support beacon and non-beacon enabled networks.

VIII. NETWORK LAYER

The main functions of the network layer are to enable the correct use of the MAC sub layer and provide a suitable interface for use by the next upper layer, namely the application layer. Its capabilities and structure are those typically associated to such network layers, including routing. On the one hand, the data entity creates and manages network layer data units from the payload of the application layer and performs routing according to the current topology. On the other hand, there is the layer control, which is used to handle configuration of new devices and establish new networks: it can determine whether a neighboring device belongs to the network and discovers new neighbors and routers. The control can also detect the presence of a receiver, which allows direct communication and MAC synchronization. The routing protocol used by the Network layer is AODV. In order to find the destination device, it broadcasts out a route request to all of its neighbors. The neighbors then broadcast the request to their neighbors, etc. until the destination is reached. Once the destination is reached, it sends its route reply via unicast transmission following the lowest cost path back to the source. Once the source receives the reply, it will update its routing table for the destination address with the next hop in the path and the path cost.

IX. Application Layer

The application layer is the highest-level layer defined by the specification, and is the effective interface of the ZigBee system to its end users. It comprises the majority of components added by the ZigBee specification: both ZDO and its management procedures, together with application objects defined by the manufacturer, are considered part of this layer

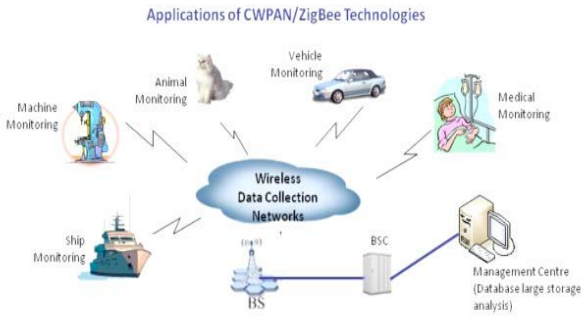

Fig. 7 Applications of CWPAN/ZigBee.

The ZDO is responsible for defining the role of a device as either coordinator or end device, as mentioned above, but also for the discovery of new (one-hop) devices on the network and the identification of their offered services. It may then go on to establish secure links with external devices and reply to binding requests accordingly.

The application support sub layer (APS) is the other main standard component of the layer, and as such it offers a well-defined interface and control services. It works as a bridge between the network layer and the other components of the application layer: it keeps up-to-date binding tables in the form of a database, which can be used to find appropriate devices depending on the services that are needed and those the different devices offer.

A. Communication and device discovery

In order for applications to communicate, their comprising devices must use a common application protocol (types of messages, formats and so on); these sets of conventions are grouped in profiles. Furthermore, binding is decided upon by matching input and output cluster identifiers, unique within the context of a given profile and associated to an incoming or outgoing data flow in a device. Binding tables contain source and destination pairs.

B. Security Services

As one of its defining features ZigBee provides facilities for carrying out secure communication, protecting established and transport of cryptographic keys, ciphering frames and controlling devices. It builds on the basic security frame work defined by IEEE 802.15.4. This is part of the architecture relies on the correct management of symmetric keys and the correct implementation of methods and security policies

X. Basic Security Model

The basic mechanism to ensure confidentiality is the adequate protection of all keying material. Trust must be assumed in the initial installation of the keys, as well as in the processing of security information. In order for an implementation to globally work, its general conformance to specified behaviors is assumed. Keys are the cornerstone of the security architecture; as such their protection is of paramount importance, and keys are never supposed to be transported through an insecure channel. A momentary exception to this rule occurs during the initial phase of the addition to the network of a previously unconfigured device. The ZigBee network model must take particular care of security considerations, as ad hoc networks may be within the protocol stack, different network layers are not cryptographically separated, so access policies are needed and correct design assumed. The open trust model within a device allows for key sharing, which notably decreases potential cost. Nevertheless, the layer which creates a frame is responsible for its security. If malicious devices may exist, every network layer payload must be ciphered, so unauthorized traffic can be immediately cut off. The exception again is the transmission of the network key , which confers a unified security layer to the network key, which confers a unified security layer to the network, to a new connecting devices.

XI. Security Architecture

ZigBee uses 128-bit keys to implement its security mechanisms. A key can be associated either to a network, being usable by both ZigBee layers and the MAC sub layer, or to a link, acquired through pre-installation, agreement or transport. Establishment of link keys is based on a master key which controls link key correspondence. Ultimately, at least the initial master key must be obtained through a secure medium (transport or pre-installation), as the security of the whole network depends on it. Link and master keys are only visible to the application layer. Key distribution is one of the most important security functions of the network. A secure network will designate one special device which other devices trust for the distribution of security keys: the trust center. Ideally, devices will have the trust center address and initial master key preloaded; if a is allowed, it will be sent as described above. Typical applications without special security needs will use a network key provided by the trust center to communicate. Devices will only accept communications originating from a key provided by the trust center, except for the initial master key. The security architecture is distributed among the network layers as follows:

1. The MAC sub layer is capable of single –hop reliable communications. As a rule, the security level it is to use is specified by upper layer.
2. The network layer manages routing, processing received messages and being capable of broadcasting requests .Outgoing frames will use the adequate link key according to routing, if it is available;

3. The application layer offers key establishment and transport services to both ZDO and applications. It is also responsible for the propagation across the network of changes in devices.

A. Simulation of ZigBee networks

Network simulators, like OPNET, NetSim and NS2, can be used to simulate IEEE 802.15.4 ZigBee networks. These simulators come with open source C or C++ libraries for users to modify. These way users can check out the validity of new algorithms prior to hardware implementation.

Subsequent methodology: First, we point the most applicable and utilized communication mechanisms that could be adopted or that sub- part of the grid by introducing their technology and use. Second, we discuss their security objectives including confidentiality, integrity, authentication, and authorization. Third, we elaborate on their threats and vulnerabilities. Finally, we discuss their feasibility in the context of their implementation and security on smart grid HANs and NANs.

XII. HAN COMMUNICATION MECHANISMS

The AMI is the key element in smart grid HANs It is dubbed the convergence of the power grid, the communication infrastructure, and the supporting information architecture. It refers to the systems that measure, collect, and analyze energy usage from advanced smart devices, including in-home devices as well as electric vehicle charging, through various communication media, for the purpose of forwarding the data to the grid. Thus, this critical communication infra- structure ought to be discussed and investigated.

Wireless LAN — 802.11 is a set of standards developed for wireless local area networks (WLANs). It specifies an interface between a wireless device and a base station (access point) or between two wireless devices (peer-to-peer).

802.11 provide confidentiality by implementing the advanced encryption standard (AES). Integrity is achieved through the AES-CBC- MAC algorithm while authentication is implemented using the Wi-Fi Protected Access standards. IEEE 802.11 by default does not offer authorization mechanisms.

The protocol suffers from significant security threats. It is vulnerable to traffic analysis, a technique that allows the attacker to determine the load on the communication medium by monitoring and analyzing the number and size of packets being transmitted. It is also susceptible to passive and active eavesdropping where an attacker can listen to the wireless connection as well as actively inject messages into the communication medium. Moreover, 802.11 is vulnerable to man-in-the-middle, session hijacking, and replay attacks.

XIII. NAN COMMUNICATIONS MECHANISMS

The NAN is the HAN complementary network that completes the distribution subpart of the smart grid. A NAN is the next immediate tier, and its infrastructure is critical since it interrelates and connects multiple HANs collectively for the purpose of accumulating energy consumption information from households (the HANs) in the neighborhood and delivering the data to the utility company. Thus, the communication infrastructure responsible for such tasks is very significant to address.

WiMAX — The IEEE 802.16[5] standard, referred to as Worldwide Interoperability for Microwave Access (WiMAX), defines the air interface and medium access control protocol for a wireless metropolitan area network (WMAN).

XIV. SECURITY FRAMEWORK DISCUSSION

The present network structure, there is a lack of adequate work in Security schemes and frameworks for AMI, especially in authentication methods. To the best of our knowledge, there are very limited realistic approaches to solving the scalability problem of smart meter authentications, regardless of which communication technology is utilized. Cryptographic methods such as digital certificates require a momentous overhead in comparison with data packet processing. In addition, cryptographic operations contribute to extensive computational cost. In the context of the smart grid, a smart meter routinely sends a meter reading message within a period of 500 ms .Nowadays, for PKI-based scheme generating a digital signature every 500 ms is not an issue using a commodity computer. Conversely, for a legacy power grid that interconnects numerous buildings, the number of meter reading messages that require verification by the NAN gateway might be noticeably larger than its capacity. Although digital signing and message verification can certainly achieve secure communications, we believe that conventional cryptographic operations make such security frameworks neither scalable nor affordable.

We assert that the security framework required to enable the discussed communication techniques to be employed for smart grid applications should be based on the following design Objectives:

- **Device authentication:** The identity and Legality of the smart meters and their associated consumers should be verified as receiving the proper utility services.
- **Data confidentiality:** The smart meter readings and management control messages

Should be confidential to conceal both consumers' and utilities' privacy.

- **Message integrity:** The smart grid should be able to verify that any meter messages are delivered unaltered in an AMI.
- **Prevent potential cyber attacks**: Smart meters should be guaranteed to obtain secure communication with the AMI net- work, even if an individual smart meter is compromised.
- **Facilitating communication overhead:** The proposed framework should be efficient in terms of communication overhead and processing latency.

XV. SYSTEM IMPLEMENTATION

The hardware description of the proposed system .The main controller that is responsible for handling the command from user terminal or the data from the ZigBee network and timely processing is the core component of the entire system. When dealing with complex tasks, the μC/OS-II embedded real-time multitasking operating system performs a high .Efficiency manager. However, multi-tasking environment will In the proposed system, the ZigBee end device of bring about problem that serial port communication may loss temperature sensor sent the collected data to the coordinator every second.

XVI. CONCLUSION

In this paper, we have investigated applicable communication mechanisms that could be adopted on smart automation on distribution networks. To tackle the cyber security of such infrastructures, we have pinpointed their security objectives and threats. We have further elaborated on their practical feasibility in terms of their technical implementation, possible obstacles, and core security issues, and attacks on smart grid HANs and NANs. We believe it is critical to continue discussing, designing, and implementing solutions for such mechanisms for the purpose of enhancing the cyber

REFERENCES

[1] Communication Security For Smart Grid Distribution Networks – Eliasbou-Harb,Lcaude Fachkha,MAKan Pourzandi,Mourad Debbabi

[2] Smart Home Design based on Zigbee wireless ,sensor Network – Chunlongzang,Minzhang,Yongshangsu,WeilianWan-Yunnan University, Kuming.

[3] Design of remote automatic meter reading system based on ZigBee and GPRS- Li Quan-Xi, Li Gang.

[4] Li-Chien Huang, Hong-Chan Chang, Cheng-Chung Chen, Cheng-Chien Kuo,A ZigBee-based monitoring and protection system for building electrical safety,Wen-Zhong Li,Chao-Yu Duan,ZigBee 2007/PRO protocolstack

[5] Behrouz A Forouzan, “Data communication” 3e, Tata Mc Graw Hill Pub, 2008 pp 19-110.

[6] P.Kinney, ZigBee technology: Wireless control that simply works, white paper dated on October 2008.

[7] Jacob Munk-Stander, Implementing a ZigBee Protocol Stack and light sensor in Tiny OS.

[8] Sheng –Fu Su, The design and implementation of the zigbee protocol Driver in Linux, White Paper dated on July 2011.

Dr.K.Rameshwaraiah obtained his B.Tech graduation from JNTUH in 2001, M.S degree from UK in 2004 and Ph.D from SBU, UK in 2011. Having more than 12 years of teaching experience working as a Professor in CSE Department. Presented more than dozen international and national papers at various journals and attended more than 20 conferences and workshops across the globe. Interested areas of research Software engineering, cyber terrorism, Network Security, Data mining and Ware housing and MANETS.

D.Vara Prasad obtained his B.Tech (E.C.E) from AITS Affiliated to JNTU in 2006 and also completed M.Tech (VLSI-SD) from NITS Affiliated to JNTUK in 2011, having more than 5 years of Teaching, industrial experience. Now working as Assistant Professor in ECE department at St.Peters Engineering College, Maisammaguda, Hyderabad, AP-India, Specialised in communications & wireless sensor networks. EMAILID: vara222 @gmail.com

Mahendra Sri Datta CH, B-Tech, Department of IT at St.Peters Engineering College, Maissamaguda, Hyderabad, AP-India. Attended half a dozen National Workshops, one International Workshop Published Four National Paper Publications .Emai l:: mahendra sridattacheekati @gmail .com