Data Security By Using X-BEE

Panem. Charan Arur, M.Sai Chandrasekhar, S.SaiSreeram, K.RamKishore and S.Venu gopal

ABSTRACT:Data Security is primary concern for every communication system. There are many ways to provide security data that is being communicated. However, what if the security is assured irrespective of the hackers are from the noise. This Project describes a design of effective security for data communication by designing standard algorithm for encryption and decryption.

Zigbee is a PAN technology based on the IEEE 802.15.4 standard. Unlike or wireless USB devices, ZigBee devices have the ability to form a mesh network between nodes. Meshing is a type of daisy chaining from one device to another. This technique allows the short range of an individual node to be expanded and multiplied, covering a much larger area.

I.INTRODUCTION

An embedded system is a special-purpose system in which the computer is completely encapsulated by or dedicated to the device or system it controls. Unlike a general-purpose computer, such as a personal computer, an embedded system performs one or a few pre-defined tasks, usually with very specific requirements. Since the system is dedicated to specific tasks, design engineers can optimize it, reducing the size and cost of the product. Embedded systems are often mass-produced, benefiting from economies of scale. Embedded systems are designed to do some specific task, rather than be a general-purpose computer for multiple tasks. Some also have real-time performance constraints that must be met, for reason such as safety and usability; others may
have low or no performance requirements, allowing the system hardware to be simplified to reduce costs.An embedded system is not always a separate

Zigbee or 802.15.4 is a wireless network standard to create a wireless network using low cost, low power consumption & low data rate connectivity devices. It can beat your Wi-Fi networks hands down for certain applications like industrial automation, medical patient monitoring, etc due to its prominent features. Let us find out what they are, in this article.

1) Zigbee/ 802.15.4 Network:

Zigbee is a Wireless Networking standard like Wi-Fi. Zigbee even operates in the same unlicensed frequency spectrum of 2.4 Ghz like Wi-Fi, but the similarity ends there. Zigbee devices form self configuring, self healing wireless networks that use low cost devices (radios, clients) to achieve a limited throughput (250 Kbps). The low bandwidth might surprise you initially, but that is sufficient for many applications.

Zigbee is the name of the alliance formed by independent companies that have some interest in manufacturing inter-operable wireless sensors and radios that can work with Zigbee standard and 802.15.4 is the IEEE Standard for the same. While IEEE 802.15.4 defines the physical and MAC layers, Zigbee itself defines the network and application layers of this wireless network. It means that all Zigbee devices will work with each other, irrespective of the manufacturer.

2) Features of Zigbee/ 802.15.4 Network:

- Transmission distance: 100 meters (Can be lesser in indoor and higher in outdoor conditions)
- Throughput: 250 Kbps at 2.4 Ghz with 16 Channels / 40 Kbps at 915 Mhz with 10 Channels
- Frequency: Uses unlicensed bands, can work anywhere in the world without requiring special permissions
- System resources required: 4-32 Kb
- Battery life: Around 1000 Days, Low power design
- Scalability: Highly scalable network that can accommodate up to 64,000 nodes using a single coordinator
- Relationship with Wi-Fi: Zigbee Networks can interfere with Wi-Fi if both are operating in 2.4 Ghz and they are not designed to inter-operate natively
- Cost: Zigbee Routers and Sensors cost very less (compared to Wi-Fi) and hence are more suitable for bulk deployment
- Network Topology: Uses Mesh Topology, Star Topology and Peer-to-Peer Topology, and can work in any one of them

Panem.Charan Arur, is working as Assistant professor and M.Sai Chandrasekhar, S.SaiSreeram, K.RamKishore and S.Venu gopal are UG Students[B.Tech], all are with Dept. of ECE, Priyadarshini Institute of Technology(PINN),Nellore.

3) Applications of Zigbee/ 802.15.4 Network:

Some applications suitable for Zigbee / 802.15.4 Wireless network include : Industrial automation, Energy automation, Access Control, Heart rate monitor, Home security, Environmental control, Lighting control, Meter reading, HVAC / Heating control, etc.

4) Components of Zigbee/ 802.15.4 Network:

Coordinator: There is one coordinator (generally) in a Zigbee network that stores the network configuration information, security keys and all other important information about the network. This is the control unit of the whole Zigbee network. But in large networks, multiple Coordinators can be linked together. The end points/ sensors can connect directly with the coordinator, if required.

Router: Since the range of the Coordinator is limited, Routers are used to extend the Zigbee networks. They have a range of 100 meters each, and they are kept within the range of other nearby routers so that they can form a mesh network. They connect the end users with the coordinator.

II.SYSTEM MODEL

TRANSMISSION SECTION:

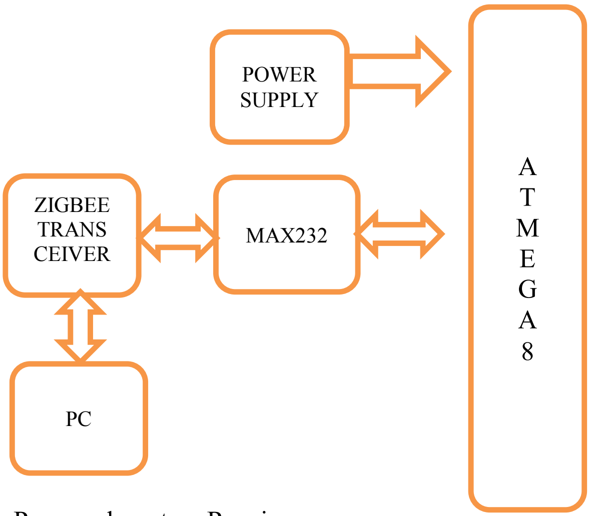


Fig:1 Proposed system Receiver

The Zigbee modules interface to a host device through a logic-level asynchronous serial port.Through its serial port,the module can communicate with any logic and voltage compatible UART or through a level transistor to any serial device (For example : RS-232 or USB interface board).These Zigbee modules are in the form of Zigbee or X-bee or Tharang.

The project is designed in such a way that one ZIGBEE transceiver will be interfaced to the PC through serial communication, so that we can input the data to the controller using the hyper terminal of PC. Here we will use a serial line driver IC MAX232 to interface the PC with controller. The ZIGBEE transceiver is used to encode the data received by the controller and to transmit the data. Hence encoded data will be transmitted by the ZIGBEE transceiver over the wireless medium and the data will be received by another ZIGBEE transceiver which will be interfaced to the PC through serial communication on the receiver side. Now it is responsibility of the controller to transfer the received data to the PC on the receiver side. Hence wireless data transfer between two microcontrollers cen be achieved. By using this project two PCs will communicate each other in both directions.

RECEIVER SECTION:

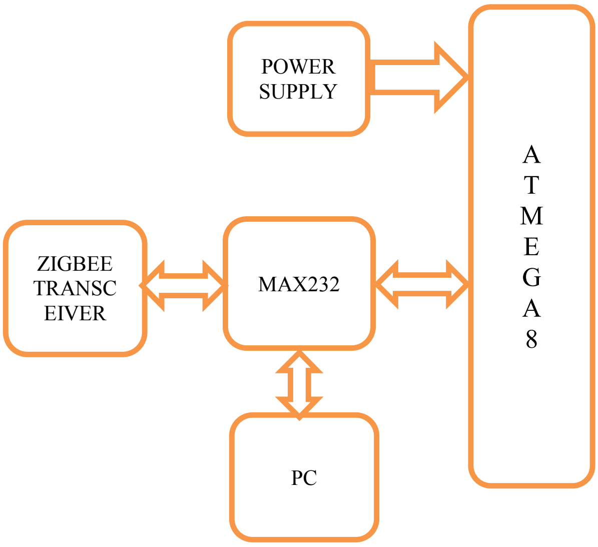


Fig:2 Proposed system transmitter

This project uses regulated 5V,500mA power supply. 7805 three terminal voltage regulator is used for voltage regulation. Full wave bridge rectifier is used to rectify the ac output of secondary 230/12V step down transformer.

III.EFFICIENT COMMUNICATION

Communication models:

An application may consist of communicating objects which cooperate to carry out the desired tasks. The focus of ZigBee is to distribute work among many different devices which reside within individual ZigBee nodes which in turn form a network (said work will typically be largely local to each device, for instance the control of each individual household appliance).

The collection of objects that form the network communicate using the facilities provided by APS, supervised by ZDO interfaces. The application layer data service follows a typical request-confirm/indication-response structure. Within a single device, up to 240 application objects can exist, numbered in the range 1-240. 0 is reserved for the ZDO data interface and 255 for broadcast; the 241-254 range is not currently in use but may be in the future.

Two services are available for application objects to use (in ZigBee 1.0):

The key-value pair *service* (KVP) is meant for configuration purposes. It enables description, request and modification of object attributes through a simple interface based on get/set and event primitives, some allowing a request for response. Configuration uses compressed XML (full XML can be used) to provide an adaptable and elegant solution.

The *message service* is designed to offer a general approach to information treatment, avoiding the necessity to adapt application protocols and potential overhead incurred on by KVP. It allows arbitrary payloads to be transmitted over APS frames.

Addressing is also part of the application layer. A network node consists of an 802.15.4-conformant radio transceiver and one or more device descriptions (basically collections of attributes which can be polled or set, or which can be monitored through events). The transceiver is the base for addressing, and devices within a node are specified by an *endpoint identifier* in the range 1-240.

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.

Depending on the available information, device discovery may follow different methods. When the network address is known, the IEEE address can be requested using unicastcommunication. When it is not, petitions are broadcast (the IEEE address being part of the response payload). End devices will simply respond with the requested address, while a network coordinator or a router will also send the addresses of all the devices associated with it.

This extended discovery protocol permits external devices to find out about devices in a network and the services that they offer, which endpoints can report when queried by the discovering device (which has previously obtained their addresses). Matching services can also be used.

The use of cluster identifiers enforces the binding of complementary entities by means of the binding tables, which are maintained by ZigBee coordinators, as the table must be always available within a network and coordinators are most likely to have a permanent power supply. Backups, managed by higher-level layers, may be needed by some applications. Binding requires an established communication link; after it exists, whether to add a new node to the network is decided, according to the application and security policies.

Communication can happen right after the association. Direct addressing uses both radio address and endpoint identifier, whereas indirect addressing uses every relevant field (address, endpoint, cluster and attribute) and requires that they be sent to the network coordinator, which maintains associations and translates requests for communication.Indirect addressing is particularly useful to keep some devices very simple and minimize their need for storage. Besides these two methods, *broadcast* to all endpoints in a device is available, and group addressing is used to communicate with groups of endpoints belonging to a set of devices.

.

IV.SECURITY

ZigBee provides facilities for carrying out secure communications, protecting establishment and transport of cryptographic keys, cyphering frames and controlling devices. It builds on the basic security framework defined in IEEE 802.15.4. This part of the architecture relies on the correct management of symmetric keys and the correct implementation of methods and security policies.

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 physically accessible to external devices and the particular working environment cannot be foretold; likewise, different applications running concurrently and using the same transceiver to communicate are supposed to be mutually trustworthy: for cost reasons the model does not assume a firewall exists between application-level entities.

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, to a new connecting device.

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 sublayer, 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. Different services use different one-way variations of the link key in order to avoid leaks and security risks.

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 momentary vulnerability 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 (through the initially insecure channel) to communicate.

Thus, the trust center maintains both the network key and provides point-to-point security. 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:

The MAC sublayer is capable of single-hop reliable communications. As a rule, the security level it is to use is specified by the upper layers.

The network layer manages routing, processing received messages and being capable of broadcasting requests. Outgoing frames will use the adequate link key according to the routing, if it is available; otherwise, the network key will be used to protect the payload from external devices.

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 within it, which may originate in the devices themselves (for instance, a simple status change) or in the trust manager (which may inform the network that a certain device is to be eliminated from it). It also routes requests from devices to the trust center and network key renewals from the trust center to all devices. Besides this, the ZDO maintains the security policies of the device.

The security levels infrastructure is based on CCM*, which adds encryption- and integrity-only features to CCM.

V.CONCLUSION

In this paper, we have analyzed the performance of different network topologies of XBee ZB module based wireless sensor network. We considered scenarios with direct transmission from the End Device to the Coordinator and with the presence of Routers for relaying messages. For multi-hop transmission with Routers, our results show that the performance of the network is highly degrading in terms of network throughput and packet delay. Therefore, to improve the system perfor- mance, the number of transmitting nodes should be mini- mized. It was also observed that the throughput varies with the packet size. A maximum throughput of 5.4 kbps was achieved which is much lower than the theoretical value of 250 kbps. Mesh routing recovery time was found to be be- tween 90ms and 130ms for a simple route of two hops and it is expected that this recovery time will increase with the number of hops in the route. Furthermore, power consumption of ZigBee End Devices using the cyclic sleep mode can be re- duced effectively, which will improve the lifetime of the entire network.

Overall, the performance analysis shows that the XBee ZB module is more suitable for low data rate applications not having very high reliability and real-time deadlines.

.

References

[1] D. I. Inc. (2013, accessed on 6 October, 2012). ZigBee Wireless Standard. Available: http://www.digi.com/technology/rf-articles/wireless- zigbee

[2] Z. Alliance. (2012, accessed on 6 October). ZigBee Specification. Available: http://www.zigbee.org,

[3] Based on Zigbee Technology," Wireless Sensor Network, vol. 4, pp. 25-30, 2012. [

[4] Z. Zou, K.-J. Li, R. Li, and S. Wu, "Smart Home System Based on IPV6 and ZIGBEE Technology," Procedia Engineering, vol. 15, pp.International Journal of Scientific & Engineering Research, Volume 4, Issue 4, April-2013 ISSN 2229-5518

[5] A. Cano, J. L. Añón, C. Reig, C. Millán-Scheiding, and E. López- Baeza, "Automated Soil Moisture Monitoring Wireless Sensor Network for Long-Term Cal/Val Applications," Wireless Sensor Network, vol. 4, pp. 202-209, 2012.

[6] Gowrishankar.S, T.G.Basavaraju, M. D.H, and S. K. Sarkar, "Issues in Wireless Sensor Networks," in World Congress on Engineering, London, U.K, 2008

[7] F. Cuomo, S. D. Luna, U. Monaco, and T. Melodia, "Routing in ZigBee: benefits from exploiting the IEEE802.15.4 association tree," in IEEE ICC Glasgow, Scotland, pp. 3271-3276.

[8] A. Wheeler. (2007, April 2007) Commercial Applications of Wireless Sensor Networks Using ZigBee. IEEE Communications Magazine. 70- 77.

[9] B. Latré, P. D. Mil, I. Moerman, B. Dhoedt, and P. Demeester, "Throughput and Delay Analysis of Unslotted IEEE 802.15.4," JOURNAL OF NETWORKS, vol. 1, pp. 20-28, May 2006 2006.

[10] J. Zheng and M. J. Lee, "A comprehensive performance study of IEEE 802.15. 4," Sensor network operations, pp. 218-237, 2004.

[11] B. Mihajlov and M. Bogdanoski, "Overview and Analysis of the Performances of ZigBeebased Wireless Sensor Networks," International Journal of Computer Applications, vol. 29, pp. 28-35, 2011.

[12] O. Hyncica, P. Kacz, P. Fiedler, Z. Bradac, P. Kucera, and R. Vrba, "The Zigbee experience," in Proceedings of the 2nd International Symposium on Communications, Control, and Signal Processing, 2006.

[13] M. P. Shopov, G. I. Petrova, and G. V. Spasov, "Evaluation of Zigbee- based Body Sensor Networks," ANNUAL JOURNAL OF ELECTRONICS, 2011.

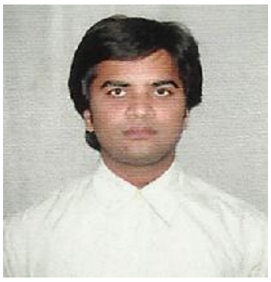
[14] G. Ferrari, P. Medagliani, S. Di Piazza, and M. Martalo, "Wireless Sensor Networks: Performance Analysis in Indoor Scenarios," EURASIP Journal on Wireless Communications and Networking, vol. 2007, p. 081864, 2007.

[15] B. E. Bilgin and V. C. Gungor, "Performance evaluations of ZigBee in different smart grid environments," Computer Networks, vol. 56, pp. 2196-2205, 2012.

[16] E. D. Pinedo-Frausto and J. A. Garcia-Macias, "An experimental analysis of Zigbee networks," in 33rd IEEE Conference on Local Computer Networks, 2008, pp. 723-729.

[17] D. International, "XBee User Manual," ed: Digi International, 2012, pp. 1-155.

[18] W. Dargie and C. Poellabauer. (2010, July 2010). Fundamentals of Wireless Sensor Networks: Theory and Practice



Panem Charan Arur. He did M.Tech (VLSI System Design) and B.Tech (ECE). Now working as a Assistant Professor in ECE department at Priyadarshini Institute of Technology (PINN), SPSR Nellore, AP, India. Doing Research Work on Low Power VLSI. Published Three International Journal, Attended one International conference and Three national level conference and two national level technical seminars, two national level workshops. Professional Association member ships IAENG,CSIT,IACSIT. He has a review committee member in three International Journals. Now he doing research on advanced technologies in VLSI and Embedded systems. Email:panem.charan@gmail.com.

M.Sai Chandra Sekhar Studying B.Tech (ECE) at Priyadarshini Institute Of Technology (PINN), SPSR Nellore, AP, and doing project work on data transmition using zigbee/x-bee. Email: saichandrasekhar@outlook.com

S,Sai Sreeram Studying B.Tech (ECE) at Priyadarshini Institute Of Technology (PINN), SPSR Nellore, AP, and doing project work on data transmition using zigbee/x-bee. Email: srichiru.ram1@gmail.com

K.Ramkishore Studying B.Tech (ECE) at Priyadarshini Institute Of Technology (PINN), SPSR Nellore, AP, and doing project work on data transmition using zigbee/x-bee. Email: kalahastriramkishore@gmail.com

S.Venugopal Studying B.Tech (ECE) at Priyadarshini Institute Of Technology (PINN), SPSR Nellore, AP, and doing project work on data transmition using zigbee/x-bee. Email: venugopal.s117@gmail.com