Durvesh Pilankar, Tanmay Sawant, Radhika Sule, Shweta Mahadeshwar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.2506-2509

Implementing Agricultural Applications Using Wireless Sensor Network and Securing Them Using Advanced Encryption Standard

Durvesh Pilankar[1], Tanmay Sawant[2], Radhika Sule[3], Shweta Mahadeshwar[4]

[1, 4](Department of Electronics and Telecommunication, Vidyavardhini College of Technology, Maharashtra, India,

[2, 3](Department of Electronics and Telecommunication, St. Francis Institute of Technology, Maharashtra, India,

ABSTRACT

A wireless sensor network (WSN) is a large number of sensor nodes distributed throughout large geographical area of interest. These sensors monitor various conditions by measuring different parameters like temperature, pressure, sound, light intensity, heat, movement, etc. The sensed data is routed to the sink node via intermediate sensor nodes. Thus we get accurate information about the parameters present in that area. Application design can be simplified by providing a set of programming primitives for sensor networks that abstract the details of low-level communication, data sharing, and collective operations. The focus on sensor networks for agriculture has a main topic of low power consumption and efficient implementation of hardware and software for various applications. The security threats involved in wireless technology cannot be ignored. Although difficult to achieve it is inevitable to secure the wireless communication network. For effective utilization of the WSN commercially, a security system for the wireless network is a must. Security aspect of network is achieved using Advanced Encryption Standard(AES) for data and Personal Area Network(PAN) ID for node security. Our goal is to confront an emerging technology with a concrete problem of world-wide dimensions, the sustainability of farming for small land-holders.

I. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. The nodes sense environmental changes and report them to other nodes over flexible network architecture. Sensor nodes are great for deployment in hostile environments or over large geographical areas. Sensors usually communicate with each other using a multi hop approach. The flowing of data ends at special nodes called base stations (sometimes they are also referred to as sinks).A base station links the sensor network to another network (like a gateway) to disseminate the data sensed for further processing. Base stations have enhanced capabilities over simple sensor nodes since they must do complex data processing; this justifies the fact that bases stations have workstation/laptop class processors, and of course enough memory, energy, storage and computational power to perform their tasks well. Usually, the communication between base stations is initiated over high bandwidth links.

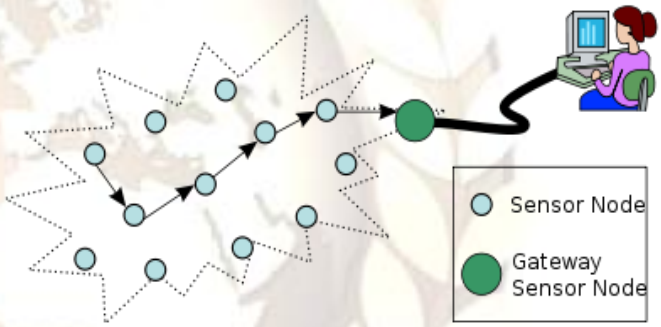


Fig-1: Typical Wireless Sensor Network [9]

The idea of automating the collection of physical data in order to monitor environments is not new.

But recent technological advances have allowed for the networking of a wide variety of sensors, independently from any preexisting infrastructure. Whenever physical conditions change rapidly over space and time, WSNs allow for real-time data processing at a minimal cost. Their capacity to organize spontaneously in a network makes them easy to deploy, expand and maintain, and provides resilience to the failure of individual measurement points.

II. ZIGBEE

Zigbee basically is built from low-power digital radios used to create personal Area Networks. Its based on IEEE 802.15 standard. Zigbee consumes low power for operation which ensures longer battery life for the equipments. Thus, equipments requiring long battery period can be installed with ease. Other notable advantages are low cost and ease of implementation in any area. Zigbee can also be

implemented in cases where high data transfer rate is not a necessity. All these factors make Zigbee highly suitable and convenient for usage in the applications related to agriculture.

III. SENSORS

It is a transducer which is used to measure agricultural parameters. In this paper the agricultural parameters discussed are 'Temperature and Water Level Indication' which are measured by using Thermistor and Linear Variable Potentiometer respectively. [1]

IV. SENSOR NODE

The sensors which we discussed above are mounted on the node which contains microcontroller as well as transreceiver module. The microcontroller used here is AtMega328[2].It acts as a buffer and also keeps a check on the frequency in which data is passed to the transceiver module. Now the sensor nodes within the network are making discrete, local measurement of the area wherein they are set up, communicating wirelessly and the collected data is routed back to the user via sink(base station).[3]

The transreceiver module i.e. ZigBee (XBEE 24 S2) [4] will do the communication between the nodes in the wireless sensor network. For interfacing between the microcontroller and Xbee module here 'Xbee SHEILD' is used. Xbee module can be programmed as per the requirement using the 'X-CTU' software. Programming parameters which are of prime importance are Baud Rate, I/O Sampling and Addressing.

V. OPERATION

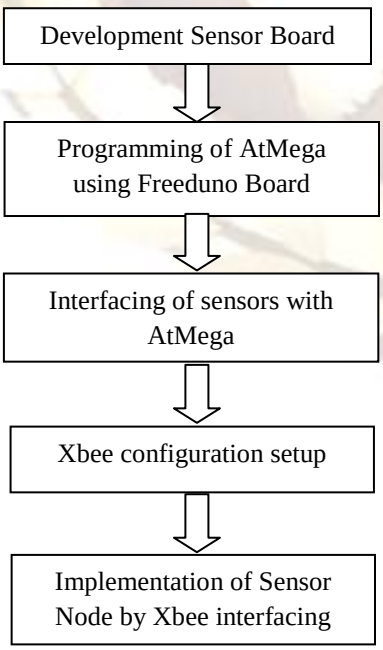


Fig-2: Flow chart of 'Node Development'

A Zigbee network can be used in 3 topologies-star, tree and mesh. Depending upon the need of the experiment these topologies can be used. So here we have used the star topology wherein there is one central node and 2 minor nodes which are connected to central node and info travels via the central node.

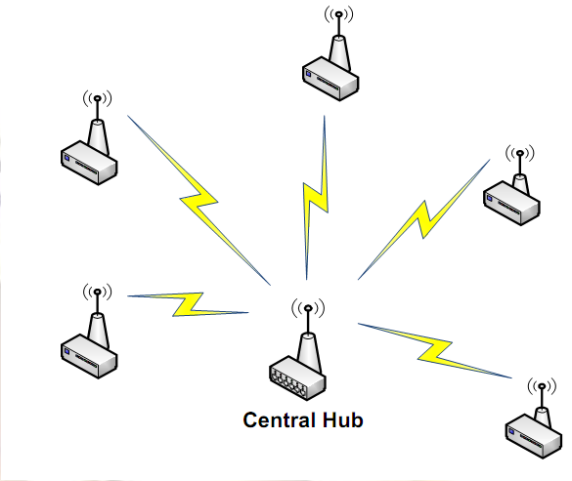


Fig-3: Star Network[10]

Basically, the Sensors mounted on sensor node will pursue the condition and give appropriate output to the respective microcontroller. The AtMega will gauge the conditions and it will send the essential data to the transreceiver module .While doing so AtMega also simultaneously acts an analog to digital convertor (ADC).Using interfacing devices data is passed to the Transceiver module. Xbee module will be used for the communication purpose. As only two nodes are used in our project, we have considered only 2 Xbee modules for on field work i.e for water sensing and for checking temperature of the soil so as to provide water for irrigation. At the base station or the sink another Xbee module is used for data reception from on field nodes. Each Xbee module has unique PAN ID. This helps in determining a unique identity to a particular node. The one connected to the server computer is the Coordinator while the others are Subordinators. Now at the subordinator i.e at the node on field, data will be sensed and further the processed data is transmitted by the transreceiver. In our case the data is directly transmitted to the base station as we have considered only two on field nodes but an actual WSN network consists of hundreds of nodes spread across a vast area. Most of the energy of the battery is consumed while transmitting the data and not while sensing or processing the data. So when data is transmitted from a node which is far away from a base station, a lot of energy of the battery is utilized and if done on a constant basis it will drain off the energy from the battery thus making the node completely useless for further operations. Once the battery dies, node wont sense or transmit the

processed data hence special care must be taken for this problem as energy saving is one of the most important parameter of the WSN.Various protocols have been mentioned over the years to save energy in WSN eg. MECN,LEACH,SPIN etc.By using any of these protocols energy of node can be saved thus improving the performance in any application Coordinator at the base station continuously accepts inputs from the subordinators and it updates its database accordingly. Thus the parameters are sensed and required action will be taken.

VI. ATTACKS ON WSN

There are many small sensor nodes in a sensor network and these are prone to various attacks. But it is difficult to monitor each type of incoming attacks. Physical, link, network, transportation and application layers are basically the different types of layers which gets affected during attacks [5].DOS attacks (Denial Of Service Attacks)[6] are the ones which affect the above mentioned layers.

In addition to DOS Attacks, there are several other attacks on WSN such as Signal/radio jamming, Device tampering Attack, Node Capturing attack, Path Based DOS, Node Outage, Eavesdropping which affects a lot of factors[7]

VII. SECURITY

Security in terms of protecting the information transmitted on wireless networks is of prime concern. The signal can be made difficult to be intercepted or can be encrypted. This can be done by employing easy steps such as reducing the signal power to least possible level so that it is protected but at the same time is able to cover the desired area, turning off the service set identifier (SSID) broadcasting by wireless access point, using directional antennas which will ensure the signal is transmitted only in the desired area.

Another technique is Encryption which is by far the best method to secure the Wireless Sensor Networks. Encrypting the signal increases the signal security by a large amount.

Here the security provision is made available by allotting unique PAN ID.PAN ID stands for personal area network identifier, basically it is a unique name given to each node. For example, Subordinator1 has PAN ID of 2419 while subordinator2 has PAN ID of 2420. PAN ID can consist of numbers, symbols, characters etc. So cracking it by obsolete method is obstinate. Another way of providing security is memory addressing. Thus a twofold security is provided to the system. This gives node security or authentication to the node. The data transmitted in the network is not secure so there is a need of proper encryption technique for data security. So for that Advanced Encryption Standard (AES) is used for encryption. The AES used in our case increases the confidentiality of the message signal and hence protects the information sent over the wireless network

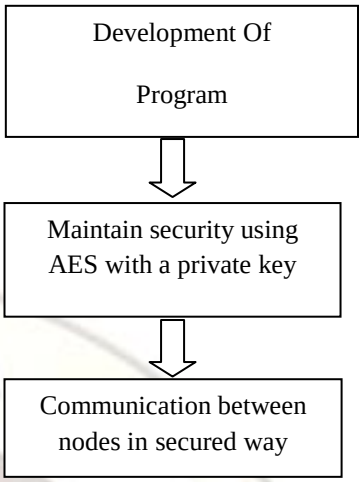


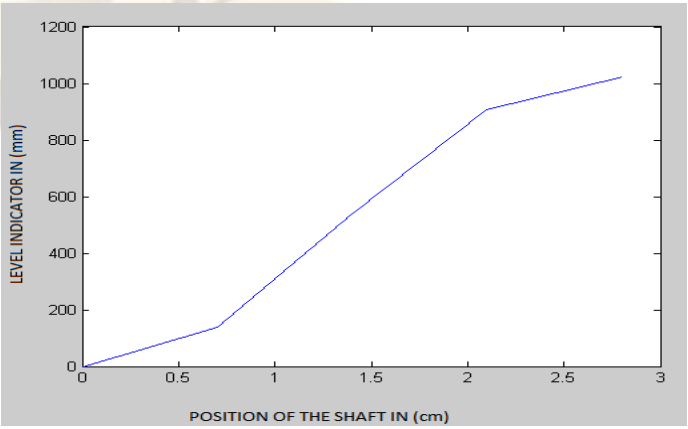
Fig-4: Flow chart of 'Security Management'

7.1 Advanced Encryption Standard

AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES is based on a design principle known as a substitution-permutation network. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. AES operates on a 4×4 column-major order matrix of bytes. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key. Here while setting the configuration of Xbee we can enable the AES i.e. data encryption by using a secret key which is used at receiving end for decryption. Hence data security is carried out.

VIII. EXPERIMENTAL RESULTS

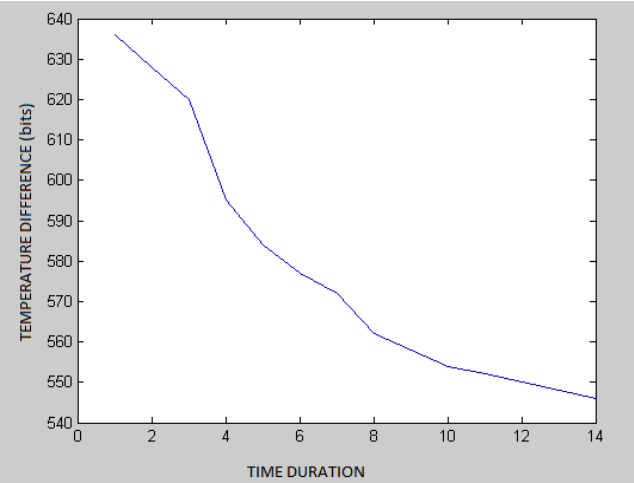
8.1 LEVEL INDICATOR



Graph-1: Graphical Analysis of Water Level Indicator

The graph shown above indicates the level of water in a reservoir. When the reading is maximum value it indicates that the water in the reservoir is at its peak and required action should be taken (for e.g. the pumping can be continued).Now if the reading drops to a low value then pumping should be stopped so as to save water.

8.2 THERMISTOR



Graph-2: Graphical Analysis of 'Thermistor'

The graph explained above is that of cooling thermistor .Here two sensors are used .One of which is buried in the soil and the other one is exposed to sunlight .The graph shows that when the outer temperature is high compared to soil temperature max reading is displayed and it shows the need of irrigation.

IX. CONCLUSION

Wireless sensor networks have many applications in our day to day life and it can be used to play an important role for a number of agricultural purposes such as soil moisture, water level and flow detection for irrigational purposes. The results obtained in the project are in accordance with the facts .The prototype of two sensor nodes used in our project can be modified and applied on a large scale in farms .The temperature variations, flow control and a variety of other parameters can be explored. Security achieved by using AES encryption and PAN ID paved way for the data transmitted to remain secure. Power consumption and cost efficiency is another aspect that is taken under consideration as the nodes even operate in a power saver mode .Thus the project helps a modern day farmer to combine technology and agricultural expertise to yield large profits and better product quality.

REFERENCES

[1]. Chee-Yee Chong, Srikanta P. Kumar, " Sensor Networks: Evolution, Opportunities, and Challenges", pp.1247-1254, Proceedings of the IEEE, Vol. 91, No. 8, August 2003.

[2]. http://www.atmel.in/devices/ATMEGA328.aspx?

[3]. Yazeed Al-Obaisat, Robin Braun,"On Wireless Sensor Networks: Architectures, Protocols, Applications, and Management", University of Technology, Sydney, Australia.

[4]. Shahin Farahani ,"ZigBee Wireless Networks and Transceivers", Newnes publications www.books.elsevier.com

[5]. Xiaojiang Du, Hsiao-Hwa Chen, 'Security in Wireless Sensor Networks, Proceedings Of IEEE, Vol.15, No. 4, Aug. 2008

[6]. A. D. Wood , J. A. Stankovic, "Denial of Service in Sensor Networks", Computer, vol. 35, no. 10, Oct.2002, pp. 54–62

[7]. Rina Bhattacharya,"A Comparative Study Of Physical Attacks On Wireless Sensor Networks", International Journal Of Research in Engineering And Technology, Vol.2,No.1,Jan 2013

[8]. Xing Zhang, Jingsha He and Qian,"Security Considerations on Node Mobility in Wireless Sensor Networks", 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology, pp. 1143-1146.

[9]. http://en.wikipedia.org/wiki/Wireless_sensor_network

[10] Steven Kosmerchock," Wireless Sensor Network Topologies"