

Wireless Sensor Networks in Agriculture Sector- Implementation and Security Measures

Sandeep Shiravale
Department of Information Technology
MIT Academy of Engineering,
Alandi, Pune, India

S. M. Bhagat
Department of Information Technology
MIT Academy of Engineering,
Alandi, Pune, India

ABSTRACT

Wireless Sensor Network technology is expected to create significant impact on our lives in the coming decade. Various applications of Wireless Sensor Network include environmental monitoring, natural disaster prediction, home appliances covering many domains like agriculture, and health care, clustered databases and so on.

A Sensor Network is a network comprised of sensing as well as computing facilities which helps the administrator in observing and reacting to the events and phenomena in a specified environment.

This paper describes implementation of Wireless Sensor Networks in agriculture sector. The deployment of Wireless Sensor Network for precision agriculture.

General Terms

Wireless Sensor Network, Precision Agriculture, Ipv6, Security, WSN

1. INTRODUCTION

A Wireless Sensor network consists of densely distributed nodes that help in sensing, signal processing, embedded computing as well as connectivity. The sensors are deployed in different arrangements. It can be point to point master-slave combination, short-hop or multi-hop. The design methodologies are needed across a set of disciplines including information processing, network as well as operational management, confidentiality, integrity, availability and in-network or local processing.

The sensor node is an important and integral component of WSN and it is capable of processing, gathering relevant information and communicating with the other nodes which are part of the network. Every node which is part of wireless network is capable to transfer the information and they accomplish this using a wireless link. The Global Positioning System present on the node helps in finding the right location of the nodes present in the specified domain. The design of the sensor nodes uses embedded software for sensor processing, energy management, locationing and so on. The embedded software works on the application layer and it specifies multiple interfaces on a sensor node. Those multiple interfaces help in designing a structured platform according to the specifications and ease down the implementation procedure.

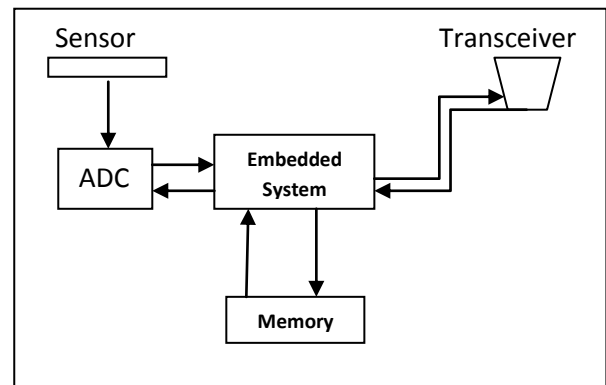


Fig.1 Architecture of Sensor Node

The architecture drawn above explains architecture of a Wireless Sensor node. The embedded system is responsible for acquiring converted signals from sensing device and processing it further. The memory unit holds the data in its buffer and forwards it to the transceiver for uploading. The reverse process occurs while data reception.

2. STANDARDS AND SOFTWARE

2.1 Standards

The standards that are relevant to sensor networks are as follows.

- 1) IEEE 802.11 a/b/g
- 2) IEEE 802.15.1 PAN/Bluetooth
- 3) IEEE 802.15.3 Ultra wideband (UWB)
- 4) IEEE 802.15.4 ZigBee
- 5) IEEE 802.16 WI Max
- 6) IEEE 1451.5 (Wireless Sensor Working Group)
- 7) Mobile IP

2.2 Software

The different open source operating systems designed specifically for Wireless Sensor networks support node operation. Such operating systems typically utilize a component based architecture which enables rapid implementation and innovation while minimizing the code size as required by the memory constraints endemic in sensor networks. TinyOS is one such example. Further, sensor network protocols and algorithms must possess self-organizing capabilities.

3. ROUTING USING IP V6

3.1 Routing

A Wireless Sensor Network usually is formed by numerous wireless sensor devices. Routing is an important mechanism which will help the data to get forwarded to the right destination. Internet Protocol is an important protocol which helps in routing process. Generally the nodes in a Wireless Sensor Network are integrated and routing using IP version 4 is difficult as the address space is limited. IP version 4 uses 32 bit addressing mechanism which is not sufficient to complete the routing process. The other option is the use of Internet Protocol version 6.

IPv6 is the latest version of Internet protocol and it uses 128 bits addressing mechanism. The IETF working group had defined a standard which enable the transmission of IPv6 packets over IEEE 802.15.4 networks (RFC4944). It defines the format for the adaptation between IPv6 and 802.15.4 which is called 6LoWPAN. The advantage of 6LoWPANs is its adaptability to open standard and assuring interoperability with other IP devices.[12]

6LoWPAN layer stack is shown below. A layer called Adaption layer is introduced between the MAC sub layer of Data Link Layer and the Network layer using IPv6 protocol. The Adaption layer helps in transmission of IPv6 data packets over 802.15.4 links. This reduces IP overhead.

| |
|-------------------|
| Application Layer |
| Transport Layer |
| Network Layer |
| Adaptation Layer |
| MAC Sub layer |
| Physical Layer |

Fig. 2 6LoWPAN Layer Stack

3.2 IP Version 6

Internet protocol version 6 is the latest version of Internet protocol. It is the advanced version and provides many benefits as compared to Internet Protocol version 4.

The length of IP version 6 is 128 bits which is four times larger than version 4. The representation is in eight groups of four hexadecimal digits separated by colons. The concept of Network Address Translation (NAT) is eliminated as every device with IP version 6 addresses is on public network. This helps in strengthening secure environment. The IP version 6 packet header is displayed below in Figure 3.

IP version 6 supports various types of network addressing schemes such as unicast, any cast, and multicast.

| | | |
|---------------------|---------------|------------|
| Version | Traffic Class | Flow Label |
| Payload Length | Next Header | Hop Limit |
| Source Address | | |
| Destination Address | | |

Fig. 3 IP version 6 packet Header

The new mechanism called as Anycast helps in finding the "nearest" or "best" destination as viewed by the routing topology. Data is routed using the defined path. These mechanisms are used in 6LoWPAN. [1]

4. SECURITY MEASURES

4.1 Secure Environment

It is essential to provide secure environment while routing data in Wireless Sensor Network. IP version 6 provides necessary security. The length of the address is big and the header format is completely changed. Further, IPSec is part of the protocol suite. A Quality of Service feature can be implemented using the Flow Label field of the IPv6 header. This feature is used to provide priority levels to the data packets. Stateless Address Auto Configuration is a feature that helps version 6 addresses to get configured automatically when the hosts are connected to IP version 6 networks.

IP version 6 supports globally unique addresses with which the activity of every device can be easily tracked. The elimination of NAT reduces complexity and every device using IP version 6 is on the public network. The various transitioning techniques like Dual Stack, Tunneling and Proxying helps in communication between both the versions of IP addresses without increasing any kind of overhead. Considering all the mentioned factors, a proper framework needs to be defined for secure data transmission. [1]

The various services like data encryption, secure routing and secure data aggregation can be enabled. The figure 4 explains the security framework. The framework is basically divided in four categories viz. Cryptography, Routing, Data aggregation and Intrusion detection.

4.2 Cryptography

Cryptography is a science and study of techniques for secure communication. The sender encrypts the information and receiver decrypts the same. Symmetric key cryptography uses same key for encryption as well as decryption where as Asymmetric key cryptography uses different key for the said process. This module is quiet complex in implementation as end-to-end security mechanisms are not suitable for the WSN.

Cryptographic module comprises encryption and key management sub modules. The sub modules provide data confidentiality, authentication and integrity and they enable secure distribution, setup and revocation of cryptographic keys. [1]

4.3 Security Protocols

Security Protocols for Sensor Networks (SPINS) is one of the well known security architecture for the WSN. The architecture comprises of two parts: SNEP (Sensor Network Encryption Protocol) and uTESLA (Micro Timed, Efficient Streaming Loss-tolerant Authentication Protocol). TinyOS operating system is most widely used operating system in WSN. The said operating system helps in building security architecture.

Data routing is an important concept in WSN. Secure routing is an integral part of security framework. The routing module includes following components: route discovery, route maintenance and data forwarding. Route discovery helps in finding the best path from the available paths. After discovering the correct path it is essential to maintain the same path and a secure layer needs to be established. After initialization of this process data is forwarded. These components are directly associated with the cryptographic module.

The base station- connecting certain number of sensor nodes – collects complete information i.e. data. The aggregation process may take place at certain intermediary node so as to save the network resources. It is quite possible that the algorithms used for aggregation process are not that secure and hence the data which is transferred can face vulnerability attack. Further, data aggregation process is performed through several phases in case of large networks. It is therefore necessary to include security concepts. This module needs to be integrated or should be made to work with Cryptographic module as well as routing module.

The last module which is part of secure framework is Intrusion Detection. IP v6 is the latest version and it is necessary to define the module accordingly. These systems must detect intrusions and must be able to communicate with all the neighboring nodes. Every sensor node monitors and records behavior of its neighboring nodes. This information is analyzed and a rule set is established so that the intrusions will be detected and communicated to all the neighboring nodes.

5. PRECISION AGRICULTURE

Precision Agriculture is a concept or technology implemented in crop management. The variations occurring in crop or soil properties within a field are noted, mapped and then necessary actions are taken. This concept is developed to maximize crop production and to minimize environmental pollution and degradation. Wireless Sensor Networks will be commonly used in agriculture sector. As discussed in the previous section, the security framework is utilized in sensor nodes which will effectively route the data packets and enable multiple transmission. WSN is generally ad hoc in nature and it is not mandatory to have an infrastructure readily available. The basic building block consists of a base station acting as a gateway between sensor nodes and the end user. [13],[14]

There are various factors considered before implementing the system. The soil quality is important. The temperature of the soil, the moisture present as well as micrometeorological parameters like air temperature, air humidity, wind speed and direction, precipitation also needs to be considered while completing the design process.

6. PROPOSED SYSTEM ARCHITECTURE

6.1 Objective in designing

The main objective behind designing the system is research in agriculture sector. The specific design will help the farmers in many areas like collecting weather data from meteorological department, planning for the right crop, communicating with agricultural experts and so on.

India ranks second worldwide in farm output. India is the second largest producer of wheat and rice, world's second or third largest producer of several products. This sector can easily feed the growing population and export wheat and rice. Poor infrastructure and unorganized retail cause India to experience some of the highest food losses in the world. The advanced technology will definitely help in resolving the highlighted issues.

6.2 The design process

The design of WSN includes various disciplines like database, query processing, networking, algorithms and distributed systems. The basic functionality of WSN generally depends on the applications but the following requirements are typical. I) determine the value of required parameter II) Classify the object that has been detected. III) Track an object. [9]

The hardware components of WSN must include the sensing and actuation unit, the processing unit, the communication unit, power unit and other application dependant units. Sensors generally have four basic hardware subsystems. A) Power, B)Computational logic and storage, C) Sensor transducers, D) communication unit. Sensors have five basic software subsystems. I) Operating system microcode(middleware), II) Sensor drivers, III) Communication processors, IV) Communication drivers, V) Data processing mini-apps. Sensor nodes have to deal with certain resource constraints like power consumption, communication, computation, and uncertainty in measured parameters. [5]

The electromagnetic spectrum provides an unguided medium for point to point and /or broadcast radio transmission. A transmission channel is never perfect because it is subjected to noise sources. The following factors are considered while designing a transmission channel. I) Propagation and propagation impairments: The basic physical mechanisms affects radio propagation is reflection, diffraction and scattering. The issues can be overcome by a) radio system design, b) antenna system design, c) signal / waveform design and d) building/environment design. II) Modulation: Spread Spectrum techniques have higher effective signal to noise ratio. Direct Sequence Spread Spectrum technique can be implemented for effective outcome. III) Available wireless technologies: The various standards in Section II can be used to broadly implement WSN.

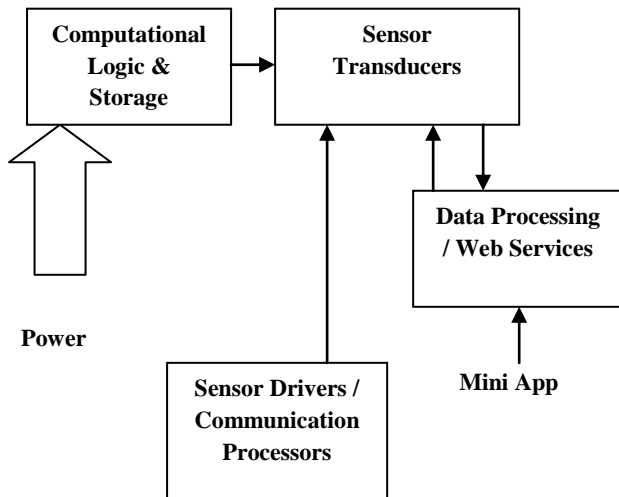


Fig. 4 Proposed System Architecture

Routing is an important concept and the design process is faced with many challenges. Routing algorithms are classified according to the manner in which information is acquired and maintained and the manner in which this information is used to compute paths based on the acquired information. Three different strategies can be identified: proactive, reactive and hybrid. The proactive strategy relies on periodic dissemination of routing information to maintain consistent and accurate routing tables across all the nodes of the network. Reactive routing establishes routes to a limited set of destinations on demand. Hybrid strategies rely on the existence of network structure to achieve stability and scalability in large networks.

After the design, it is necessary to monitor the activities which will help overcome the design issues. The optimization of node distribution is essential so that it can reduce energy consumption. Network fault tolerance includes node failure detection and failure recovery. Integration of a portable GPS device can solve this issue easily but at a higher cost.

7. CONCLUSION

This paper has described the design and implementation of a wireless sensor network for monitoring agricultural environment. The nodes in this system always work under different environmental conditions and it is a real challenge in establishing a WSN. Securing this network is also an uphill task as it is necessary to establish routing and routed protocols concerned. The security framework discussed here is helpful in designing the system architecture. There are various issues and challenges while designing the architecture. Certain issues are discussed in this paper. The future challenge lies in overcoming the stated issues. The new technology should be able to harness several possibilities in managing the farm sector precisely. In the near future, agriculture sector can face multiple challenges. The recent trends should address them and should help in successfully building the prototypes.

The agriculture sector in Indian context is still using age old technique and it is important to upgrade the entire system. The present day technology will help in getting the right crop, analyzing different parameters like weather, soil temperature, and moisture in air and it will help the farmer to maximize their benefits.

8. REFERENCES

- [1] Kresimir Grgic, Drago Zagar, Visnja Krizanovic "Security in IPv6-based Wireless Sensor Network – Precision Agriculture Example" ISBN: 978-953-184-180-1, June 26-28, 2013, Zagreb, Croatia
- [2] YIN Shouyi, LIU Leibo, ZHOU Renyan, SUN Zhongfu, WEI Shaojun "Design of Wireless Multi-media Sensor Network for Precision Agriculture" China Communications • February 2013
- [3] Ioanna Mampentzidou, Eirini Karapistoli, Anastasios A. Economides "Basic Guidelines for Deploying Wireless Sensor Networks in Agriculture" 978-1-4673-2015-3/12/\$31.00 ©2012 IEEE
- [4] Ajay Mittal, Chetan K. P. , Srinivasan Jayaraman, Bhushan G. Jagyasi, Arun Pande, Balamuralidhar "mKRISHI Wireless Sensor Network Platform for Precision Agriculture" 978-1-4673-2248-5/12/\$31.00 ©2012 IEEE
- [5] Jianfa Xia, Zhenzhou Tang, Xiaoqiu Shi, Lei Fan, Huaizhong Li "An environment monitoring system for precise agriculture based on wireless sensor networks" 978-0-7695-4610-0/11 \$26.00 © 2011 IEEE
- [6] T.Kalaivani, Aallirani, P.Priya "A Survey on Zigbee Based Wireless Sensor Networks in Agriculture" 978-1-4673-0132-9/11/\$26.00©2011 IEEE
- [7] Ying Zhang "Design of the node system of wireless sensor network and its application in digital agriculture" 978-0-7695-4350-5/11 \$26.00 © 2011 IEEE
- [8] Prakashgoud Patil, Vidya H, Shreedevi Patil, Umakant Kulkarni "Wireless Sensor Network for Precision Agriculture" 978-0-7695-4587-5/11 \$26.00 © 2011 IEEE
- [9] Lei Xiao, Lejiang Guo "The Realization of Precision Agriculture Monitoring System Based on Wireless Sensor Network" 978-1-4244-6947-5/10/\$26.00 ©2010 IEEE
- [10] Herman Sahota, Ratnesh Kumar, Ahmed Kamal, Jing Huang "An Energy-efficient Wireless Sensor Network for Precision Agriculture" 978-1-4244-7755-5/10/\$26.00 ©2010 IEEE
- [11] ZHANG Xuyuan "Model Design of Wireless Sensor Network based on Scale-Free Network Theory" 978-1-4244-3693-4/09/\$25.00 ©2009 IEEE
- [12] Ansar Jamil, Sharifah H. S. Ariffin, Adel Ali Abdullah, Norsheila Fisal, Kashif Saleem and Sharifah K. Syed-Yusof "Optimal Forwarding Routing Protocol in IPv6-based Wireless Sensor Networks" 978-1-4244-5532-4/09/\$26.00 ©2009 IEEE
- [13] Anurag D, Siuli Roy and Somprakash Bandyopadhyay "AGRO-SENSE: PRECISION AGRICULTURE USING SENSOR-BASED WIRELESS MESH NETWORKS" 92-61-12441-0/CFP0838E © 2008 ITU
- [14] Jzau-Sheng Lin, Chun-Zu Liu "A Monitoring System Based on Wireless Sensor Network and an SoC Platform in Precision Agriculture" 978-1-4244-2251-7/08/\$25.00 ©2008 IEEE
- [15] Srdjan Krco, Mattias Johansson, Vlasios Tsiatsis, Ivica Cubic, Katarina Matusikova "Mobile Network Supported

Wireless Sensor Network Services” 1-4244-1455-5 07
\$25.00 ©2007 IEEE

- [16] Zhenyu Liao, Sheng Dai and Chong Shen “Precision Agriculture Monitoring System based on Wireless Sensor Networks”

- [17] Kazem Sohraby, Daniel Minoli, Taieb Znati “ Wireless Sensor networks: Technology, Protocols, and Applications” Wiley India Pvt. Ltd. ISBN No. 978-81-265-2730-4