SECURITY SCHEME FOR WIRELESS SENSOR NETWORK

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Technology

In

Communication and Networking

by

Varun Shrivastava

Roll No: 212EC5179

Department of Electronics & Communication Engineering

National Institute of Technology

Rourkela

2014

SECURITY SCHEME FOR WIRELESS SENSOR NETWORK

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Technology

In

Communication and Networking

by

Varun Shrivastava

Roll No: 212EC5179

Under the guidance of

Prof. Poonam Singh

Department of Electronics & Communication Engineering

National Institute of Technology

Rourkela

2014

National Institute Of Technology
Rourkela

CERTIFICATE

This is to certify that the thesis entitled, "**SECURITY SCHEME FOR WIRELESS SENSOR NETWORK**"submitted by VARUN SHRIVASTAVA in partial fulfilment of the requirements for the award of Master of Technology degree in **Electronics and Communication Engineering** with specialization in "**Communication and Networking**" during session 2012-2014 at National Institute of Technology, Rourkela (Deemed University) and is an authentic work by him under my supervision and guidance.

To the best of my knowledge, the matter embodied in the thesis has not been submitted to any other university/institute for the award of any Degree or Diploma.

Date:

Prof. Poonam Singh
Dept. of ECE
National Institute of
Technology
Rourkela-769008
Email: psingh@nitrkl.ac.in

Acknowledgment

I would like to express my gratitude to my thesis guide Prof. Poonam Singh for her guidance, advice and constant support throughout my thesis work. I would like to thank her for being my advisor here at National Institute of Technology, Rourkela.

Next, I want to express my respects to Prof. S.K. Patra, Prof. S. Meher, Prof. K. K. Mahapatra, Prof. S. K. Behera, Prof. S. K. Das, Prof A. K. Sahoo, Prof. S. Maiti, Prof L. P. Roy and Prof A. K. Swain for teaching me and also helping me how to learn. They have been great sources of inspiration to me and I thank them from the bottom of my heart.

I would like to thank all faculty members and staff of the Department of Electronics and Communication Engineering, N.I.T. Rourkela for their generous help in various ways for the completion of this thesis.

I would like to thank all my friends and especially my classmates for all the thoughtful and mind stimulating discussions we had, which prompted us to think beyond the obvious. I've enjoyed their companionship so much during my stay at NIT, Rourkela.

I am especially indebted to my parents for their love, sacrifice, and support. They are my first teachers after I came to this world and have set great examples for me about how to live, study, and work.

VARUN
SHRIVASTAVA

Roll No: 212EC5179

Dept. of ECE

NIT, Rourkela

Abstract

A Wireless Sensor Network (WSN) could be a network created of tiny autonomous sensors (nodes). Its purpose is to watch environmental variable like temperature, pressure, humidity, motion, brightness, etc. These nodes use a radiofrequency system to deliver the knowledge gathered by the sensors to a central process unit (CPU) or base station. The communication between a node and therefore the base station may happen either directly or step by step through completely different nodes among the network. Some WSN can even be controlled from the base station. Each device node typically consists of the subsequent main components: a microcontroller, completely different sensors, a radio transceiver and electric battery or another supply of power. There are many parts that are wont to adequate the electrical signals and therefore the power provide to the necessities of the most components; during this class may fall devices like voltage regulators, amplifiers, resistors, capacitors or generator sources. Secure communications in some wireless device networks square measure vital. The scheme relies on LOCK scheme and staff ID-based secure cluster key management. The scheme has many blessings over the prevailing LOCK theme. This scheme improves the wireless device network system security. It minimizes the amount of key storage demand and therefore the number of the communication messages for rekeying. Additionally, one distinctive advantage is that it doesn't have an effect on the other nodes once evicting compromised node or moving the node from one location to a different. The goal of this thesis is to style and build a WSN node and to program its microcontroller thus it covers a basic practicality, implement the science security and to send the collected knowledge to different network nodes. This goal was achieved. Four nodes were engineered and programmed, and their practicality was tested. Associate Attiny85 microcontroller was used for the WSN node and Atmega328 microcontroller was utilized in base station programmed in C with Arduino. The Attiny85 microcontroller receives the signals from the sensors and converts them to digital; then it stores the digitalized knowledge to finally deliver them to its NRF24l01 trans-receiver radio module wherever they're sent by radio.

Keywords: WSN, NRF24l01, Arduino, Atmega328, Attiny85.

List of figure

List of Tables

Contents

Chapter 1 Introduction

1.1 Introduction

Wireless sensor network comprises of devices which have sensor from which it can sense the environmental condition, apply some processing and finally can send the data to the command center. Using some advanced mesh protocols, these devices extend the reach of Internet out into the physical world. The mesh property of network can find out and use any valid communication route by hopping data from one node to the other to find out its destination. The most important advantage of the wireless sensor networks lies within the ability to deploy giant numbers of small nodes that act together by themselves. The application area of the wireless sensor network is where it becomes important to observe or monitor the environmental condition or to monitor the health of instruments or machine in the industry. Whereas usually said as WSN, they'll conjointly management actuators that stretch management from Internet into the real world. An example can be cited as a manufactory might be simply monitored for leaks by many sensors that mechanically type a wireless sensor network and report if there is any chemical leakage. In contrast to ancient wired systems, readying prices would be bottom. Rather than having to deploy thousands of feet of wire routed through protecting passage, installers merely got to place quarter-sized device at every sensing purpose. The network is scalable, that is, it can be easily extended only by adding additional devices which means no complicated configuration is required. Additionally to drastically reducing the installation prices, WSN have the power to dynamically adapt to dynamic environments. Adaptation mechanisms will reply to changes in network topologies or will cause the network to shift between drastically completely different modes of operation. For instance, identical embedded network acting leak observation in an exceedingly chemical works may be reconfigured into a network designed to localize the supply of a leak and track the diffusion of toxic gases. The network might then direct employees to the safest path for emergency evacuation.

Current wireless systems solely scratch the surface of potentialities rising from the combination of low-power communication, sensing, energy storage, and computation. These things are priced many greenbacks, target specialized applications, and admit the pre-deployment of intensive infrastructure support. In distinction, WSN use tiny, affordable embedded devices for a large vary of applications and don't admit any pre-existing infrastructure.

Unlike ancient wireless devices, WSN don't have to communicate directly with the closest dynamic base station, but only with their neighbors. Instead of looking forward to a pre-deployed infrastructure, every individual sensing element or mechanism becomes a part of

the infrastructure. Point to point networking gives an illusion of a mesh like network to send the data between small embedded devices in an exceedingly multi hop fashion. The versatile mesh architectures can cover a large geographic area and also new nodes can be easily added by just informing the neighboring nodes. To boot, the system will mechanically adapt to compensate for node failures. This is the difference between the mobile network to the wireless sensor network as in mobile network the cell phones are denied of the service once too many phones are present in the area while in the wireless sensor network the service increases as more nodes are present in the network. As long as there's sufficient density, one network of nodes will grow to hide limitless space.

Figure 1.1

An example can be shown using figure 1. This figure shows an agricultural field with hundreds of nodes used to monitor the area. These hundreds of nodes uses routing protocol to transmit the data to a specific point also called base station to collect all data and to store the data for future reference. The application demands low cost, scalable and robust network which is easily met by wireless sensor network. If one node fails, a new topology should be selected so that the network doesn't go down and the base station can still receive the data without any obstruction.

The above example also show the fact that the sensor nodes should not be expensive and can be changed without any difficulty. And the new node should start communicating with the base station without bringing any large change in hardware.

But, wireless sensor network has application in both civil and military level. There are some application where use of secure communication is highly essential. However, these network are prone to many cyber-attack because of presence of wireless connectivity and absence of physical medium. Thus, anybody can send the fake data and can bring the network down. Thus, security in wireless sensor network is highly required.

However, the design of wireless sensor network make the design of security very complicated. The nodes have very less computation as compare to base station and thus security model for wireless sensor network become different from that of existing wireless network. Thus, the existing security model for wireless and wireline communication cannot be applied on wireless sensor network. Hence, resource conscious security protocols become necessary for wireless sensor network.

This thesis focuses on development of the WSN architecture and implementation of cryptographic security for secure data transmission.

1.2 Goal

The goal of this thesis is to design the wireless sensor network using embedded system and to use the security protocol of wireless sensor network to make the communication between the nodes secure.

1.3 Objective

The objective of this thesis is to design a home security system using wireless sensor system and to make the communication between the sensor nodes secure.

1.3.1 To study the architecture of Wireless Sensor Network

The wireless sensor network consist of base station which is the collection point of the data from all the sensor nodes. The base station is embedded system consist of RF module and microcontroller atmega32. The nodes is embedded system consist of RF module, sensor and microcontroller attiny85.

1.3.2 To add cryptographic security protocol in this wireless sensor network

The communication between the sensor nodes is made secure, that is, the data transmission and reception which take place is in encrypted forms. This is done using elliptic curve cryptographic.

1.4 Thesis overview

This thesis consist of 6 chapters that explains the topics introduction, background, working of the system, result, conclusion and further development that can be applied on this project.

Chapter 2: Wireless sensor network and Security will give a brief explanation about wireless sensor network and security protocol to the reader.

Chapter 3: Microcontroller and RF module will give introduction about the architecture of atmega32 and attiny85 microcontroller that is being used in this project and the RF module that will be attached to the nodes of wireless sensor network.

Chapter 4: System Design that shows the step that was used to design the system.

Chapter 5: Results

Chapter 6: Conclusion, shows the conclusion that can be drawn from the project.

Chapter 2 Wireless Sensor Network and Security

2.1 Wireless Sensor Network

The construction of the wireless sensor network can be explained with a simple equation below:

Sensor + intelligent circuit + RF module gives a node which can be used for many powerful applications.

At present we can see that thousands of application can use the wireless sensor network. It can be perceived as combination of different field of modern technology. Although, it is not that easy as it seems. The user should have a thorough knowledge about both the advantage and disadvantage of each and every hardware component used in the network. Also the user should have a thorough knowledge about network technology used in the network and the routing protocol that is used. The nodes should be designed in such a way that after they are placed in the network they must be able to produce primitives that can make the network efficient in terms of size, speed and power consumption. Thus, everything comes down to the limitations of individual nodes as a single node can bring the network down.

2.1.1 Sensor Node application

The 3 application categories we've got selected are: environmental information assortment, security observance, and sensor node pursuit. We have a tendency to believe that the bulk of wireless sensor network deployments can constitute one among these category templates.

2.1.1.1 Security Observance

The second type of application for wireless sensor network is security observance. WSN that observe security of a particular building like bank are placed at fixed positions and observe the one or more sensor to discover any irregularity. The most important difference between security observance and environmental information assortment is that the in this case the nodes are not collecting any type of data. In this case the nodes have to check the status of sensor and then transmit the information to the base station in case of any security breach. The fast and consistent communication of warning is the basic requirement of this system.

Also, it is highly required that the node exists and working properly. If any node is deactivated without the permission of the authorized user, the network will report the situation as security breach and will then turn on the alarm. For security observance network, the network should be made such that all the node are accountable for approving the status of every other node. One way to make this possible is by assigning a central hub which is

connected to every other node and is responsible to report that all the node are working or not. Thus, the topology of security observance network will be star topology than the mesh as in environmental information assortment.

The most accepted standard in security system is that every node is to be examined atleast once every hour.

As the breach is found, a security protocols should start and the message is to be commuted to the base station as soon as possible. The time required for the message to reach the base station is a major influence on the performance of the model. Users require that warning to convey as soon as within seconds of security breach. Thus, nodes in the network should react quickly to the request from the other nodes and thus forward the data to the base station as quickly as possible.

In such a network, more stress is given to increase the speed of warning transmission as compare to the energy requirement in transmissions. This is due to the fact that the security breach is a rare event to happen. For example, in fire alarm system, the probability of getting a breach is very low. By increasing the speed of transmission, energy required by the node increases as there is constant monitoring of radio channel to send the data to the base station.

In such a model, energy used to transmit the data to the base station will be less than the energy used to confirm the function of other nodes in order to prepare to forward the message to the base station.

2.1.1.2 Sensor Node Pursuit

Another type of application for Wireless Sensor Network is pursuing of any labelled object in a region observed by the network. There may be circumstances where user is interested to pursue a precious resource or a person. Today's tracking device track an object by documenting the previous checkpoint. But, it is not possible to track down the current location. For example, the courier service pursue the current location of its shipment by scanning the bar code when it passes through its routing center, but this system fails as soon as the object doesn't follow the a route from one checkpoint to the other checkpoint and the object is lost.

In wireless sensor network scenario, the object can be pursue by marking the object with a small sensor node. The sensor node can then give the current location of the object by communicating with the sensor nodes that are present in the environment at known places.

These nodes will actually read the radio messages send by the node marked on the object. Thus, a database can be maintained which shows the location of object when passed through these known location. Thus, we can find out current location of the object and not only the last checkpoint of the object.

In this model, there will be a continuous topology changes in network as the node is always in moving state. The radio link between the stationary nodes will be steady but the radio link between the mobile node and the stationary node will always be changing. Also the nodes will always be leaving the system and new node will always arrive in the system. Thus, it's required that stationary node are able to detect the new mobile node efficiently as soon as they arrive in the network.

2.1.1.3 Hybrid networks

If generalized, an application can have features of all the three type of application. An example can be cited as if a network is made in order to pursue vehicles whenever they pass through a location, the wireless sensor network can shift from being a security observance network to sensor pursue network. If there is no traffic of vehicles, it can act as security observance system. As soon as a vehicle is passed, alarm is generated and whole or part of network is shifted to sensor pursue network and thus send a report to the base station which pursue the vehicle. Thus, it becomes important to make a single architecture that can control all three applications.

2.1.2 System assessment metrics

As we have discussed the application situations, we take down the assessment metrics that will be used to assess the wireless sensor network. In order to do this, we have to mind the required use of the network and also the main advantage of wireless sensor network over the present technology that is being used. The assessment metric for wireless sensor network are lifetime, coverage, cost and ease of deployment, response time, accuracy, security and sample rate.

2.1.2.1 Lifetime

One of the most important aspect to a wireless sensor network is its estimated lifetime. The objective of environmental information assessment and security observance is to place the

nodes in open ignored for a large span of time which can be for months and even years sometimes.

The most important issue for lifetime of nodes in sensor network is its power supply. Every node should be designed keeping in mind that it could supervise its local power supply so that it could maximize the lifetime. Also, it is not the average lifetime of node that is critical but the minimum lifetime of node that comes out to be critical. In case of security observance system, the minimum node lifetime should be high for node as failure of even one node will bring the system down.

There can be a situation where the nodes can be supplied with external power source such as connecting the sensor nodes to the power source of the building. But, the most important aspect of wireless sensor network is its ease of installation. That is it is being small and handy can be placed anywhere in the room or building, but by supplying it with external power supply, this advantage gets cancelled as there are only fixed places in the building where it can now be place. A negotiation can be made by supplying some of the most important nodes in the building with external power supply.

Although given the fact rest of the nodes in the building is to be self-powered. This means that either they should have large power storage or they should convert the environmental energy into usable energy for its own for example solar cell. But the requirement in both the condition is that power wastage should be minimum and consumption by node should also be minimum.

Most of the power supplied to the node is taken by the radio module in the node. However this can be reduced by decreasing the transmission power. However, this effects the other metrics.

2.1.2.2 Coverage

Other important aspect is the coverage for a wireless network. It is ideal to make the network over a larger physical area. The coverage of network here doesn't mean range of radio links. By using techniques like multi-hop communication the coverage of network can be broaden beyond the range of radio links. But, for a fixed range multi-hop communication increases the power utilization of node and thus decreasing the lifetime. Also, they require minimal node density which also increases the implementation cost.

Attached to the range is the network's capability to scale large number of nodes.

Scalability is an important aspect of wireless sensor network. A user can anytime increase the number of sensor in the network in order to increase the size of network without any large

change in the technology used. Thus, collecting more and different data. By increasing the number of node the lifetime of network decreases as more the number of node more will be the data to be transferred and thus more will be the power consumed.

2.1.2.3 Cost and ease of deployment

A positive point for wireless sensor networks is they are easy to deploy. People in field of archeology or biology are not expected to understand the concept of networking and communication that take place inside wireless sensor network. Thus for this reason wireless sensor network must be able to set up itself. There should be possibility that an untrained person may be able to use wireless sensor network easily and efficiently.

The ideal condition is that the nodes will automatically configure themselves wherever they are placed. However, reality is far from ideal, there must be a constraints placed on node placement. There must be a feedback provided to tell when these constraints are disrupted.

The system should adapt as the environmental condition changes. There may be scenario where a large object interfere in communication between nodes, the nodes should automatically adjust to these situation.

The initial setup is only a single step in wireless sensor network lifecycle. In its whole lifetime, the total cost for user increases with its maintenance. Thus, cost of maintenance becomes important factor than cost of setup of network. Whenever require, the network should be able to send a request for hardware maintenance.

2.1.2.4 Response time

In an application scenarios like that of security observance system, response time of alarm becomes an important factor. The alarm must be triggered as soon as intrusion is found. Although being a low power task, node should be able to trigger a high priority messages to base station as soon as possible. Though these events are uncommon or rare, these event may occur without any prior knowledge. Response time is important in environmental assessment system as it is used to control various machines and tools. Wireless sensor networks is an important asset in industries as it can be used to measure the temperature and pressure of various industrial machines without going near to them, any change in measurement should be conveyed quickly to the user. Thus, response time becomes an important factor as performance index in industrial applications as well.

But, by making the response time low, network lifetime also decreases as the frequency of using the radio link increases and thus increasing the use of power supply. Thus, a tradeoff is

maintain to make the response time minimum with maximum network lifetime. Also, the tradeoff is made on the basis of application. If the application requires to decrease the response time to make the performance satisfactory then the same is done on the expense of network lifetime.

Response time can be decreased by using the node which are given power all the time. These nodes are responsible to trigger the alarm and then send the alarm to base station but this decreases the ease of deployment.

2.1.2.5 Temporal accuracy

In some application, samples from different node are cross-correlated in time so as to find out the nature of event that is being measured. The accuracy of correlation will depend on the speed of event which is being calculated. For example in order to find out the temperature of a building samples are correlated within seconds or minutes. But in order to find out the reaction of building to seismic event a time accuracy of millisecond is required.

In order to maintain temporal accuracy in a wireless sensor network, the network must be able to make and keep a time base which then synchronizes with every node in the network so that every samples of data can be correlated with time to find out the measurement required. But in order to achieve this power is consumed more and thus the network lifetime decreases which again requires a tradeoff. Time synchronization between different nodes in the network becomes an important factor. Thus to maintain time synchronization different synchronization messages are send by the time base to the nodes in the network in order to update the time. The time base need to use the radio module more thus require a continuous power supply as its failure can bring the entire time synchronization down. This decreases the ease of deployment as well.

The final conclusion can thus be made that to increase the temporal accuracy the bandwidth requirement increases and also it decreases the network lifetime and ease of deployement.

2.1.2.6 Effective sample rate

In an application scenario where data collection is done, effective sample rate is an important aspect. Effective sample rate can be defined as the rate at which nodes takes the data from the sensor and then transfer the data to the base station. For the application like environmental information assessment demand for data is only 1-2 times per minute. But, along with the

sample rate in case of single sensor there is also the impact of multi hop networking architecture.

One way to increase the effective sample rate above that of the raw communication of network is to manipulate the processing taking place inside the network. There are various type of compression technique that can be used in order to decrease the bandwidth require to transmit the data while maintaining the effective sample rate constant. Use of local server or local station can be used to collect and store the data collected from the nodes for short periods.

Trigger by an event is simplest form of processing that can be done in a network. They are mostly used in security observance system. The data is continuously monitored from the sensor by the nodes and every time a security breach happens alarm gets triggered and the data is then sent to the base station.

2.2 Security

2.2.1 Introduction

In many wireless sensor network application, security of data transmitted between the nodes becomes an important issue. For example in application like military, the wireless sensor network is under constant malicious attacks, as the network is wireless which means there is no physical media involve. Thus, secure data transmission becomes an important aspects in such applications.

But, there is some interesting point that should be consider first. The wireless sensor network architecture is not the same as compare to the current wired or wireless network. The nodes have low computational capability so as to increase the network lifetime. Thus, the design and working of existing security protocol becomes challenging. One option is to use resource conscious security protocol.

The most important part of secure communication is key management. There are many dynamic key management protocol that have been proposed in the past. These protocol are important for network with long lifetime. In these type of system the keys are changed continuously on demand. These protocol make the network scalable that is new nodes can be attached to the wireless sensor network.

ID based symmetric keying [1] is one of the most famous key management protocol. According to this protocol, the wireless sensor network is divided into three part, the base

station, the gateway and the sensor nodes. The base station creates the keys which is then allocated by gateway on demand of sensor nodes. This scheme is not suitable for rekeying as there will be a large number of messages exchanged between sensor nodes for rekeying. The more the number of messages to be sent the less will be the network lifetime and ease of deployment.

Thus, in order to make a balance the number of keys for each node and number of messages to be exchanged, an efficient rekeying solution known as exclusion based systems (EBS) was proposed. Based on this a scheme for secure wireless sensor network was proposed known as LOCK scheme. LOCK scheme has two layer of EBS in order to implement localized rekeying.

The EBS reduces the number of messages exchanged during rekeying but also uses compromised keys for encrypting the message. This is a disadvantage for wireless sensor network that tries to minimize the power consumption in order to increase the network lifetime. The advantage of this scheme is that it reduces the possibility of collusion attack.

2.2.2 Key management scheme

The node uses a symmetric key mechanism known as ID based key management. Thus, every node should be able to store key that it shares with the neighbor nodes and the base station. Because the nodes have limited memory resources and are also vulnerable to attacks, they should be assigned a limited number of keys. In this way memory is saved. Also, when a node is attacked by the adversary, node can be compromised so as to reduce the damage on the network.

The gateway have enough memory resources so that a large number of keys can be assigned to them but they cannot be trusted and thus, are not assigned all the keys.

The base station have no restriction as they are secured and have enough resources and thus can be trusted to assign all the keys of the network.

The keys are stored in the flash memory of sensor node and gateways before they are deployed. They can be deleted when required to. The base station stores all the keys that is also allocated to the sensor nodes and gateways. Thus, the total number of keys in base station becomes $G + S$ where G is gateway keys and S is sensor node keys. The sensor nodes stores two secret session keys one that is used for secure communication with gateways and other that is used for secure communication with the base station.

The base station can find out which gateways and sensor nodes are affected by the attack from adversary. Thus, the base station renew the keys for gateways and sensor nodes as

continuity of the same keys can lead to the deduction of keys by the adversary. The new keys are then updated to the gateways which then inform the sensor nodes.

During placement, every gateway is given *S/G* keys where *S* is the number of sensor node and *G* is the number of gateway. This key assigning is done at random as the base station doesn't know the exact position of sensor and gateways.

Once the gateways are placed they form clusters using the algorithm known as cluster forming algorithm and thus they acquire the keys of the sensor nodes that are present in there cluster from the other gateways using key exchange protocol. As soon as the keys are exchanged the gateways delete the keys of the sensor nodes that are not present in their cluster from their memory. This step is an important step as if the keys of other cluster are stored in the gateway, they will be available to the attacker.

The sensor nodes also store the ID of their gateway in their memory that contains the key before placement. This ID is the "hello" message that is broadcasted during the placement of sensor nodes. If this ID is not sent the gateway had to do a lot of computation to find out the sensors in their clusters. The sensor nodes send the information about their location and the power used to the gateways using the message that is encrypted using the key that it shares with the gateway. This information is then used by the gateway to form a routing table.

Whenever a new sensor node is added to the network, it will have two keys with it. One that is shared with the gateway of its cluster and the other will be shared with the base station. But the problem is that the nodes are assigned randomly and not in a pre-assigned fashion. Thus the gateway doesn't know the ID of the newly assigned sensor nodes.

The base station comes to play in this situation. It separates the list of newly added sensor nodes into different sets. These list have the sensor IDs and the keys correspondingly that is to be shared with the gateway. At this time the base station transmit this list to any gateway randomly. After the sensor nodes are placed, they broadcast a "hello" message to the gateway. After the hello message is received the gateway assigns the newly added sensor nodes to their cluster using clustering algorithm.

When a sensor node is attacked by an adversary, intrusion detection mechanism runs and tell the base station about the compromised node. The compromised node is then evicted from the cluster of the gateway. This is important as it will not help in deduction of the keys to the adversary. The gateway will then ignore the messages from the sensor node along with all the other sensor nodes present in the cluster.

In case when the gateway is under attack and is compromised, the base station will elect a new gateway as a head of the cluster and the new gateway will be instructed to remove the

compromised gateway from the network. The sensor nodes in that cluster will then be distributed to the new elected gateway.

Single key has capability of encrypting a large amount of data. If the attacker has some information about the data which is sent, it can run a plain text attack and thus can deduct the key used for encryption. Thus, there is a constant demand of renewing the keys used for encryption. But due to this the power consumption increases as the RF module is on always. Thus the gateways are required to renew the keys at some definite time which depends on the amount of traffic and strength of cryptographic properties of the key.

2.2.3 Exclusion Basis System

EBS can be defined as collection Γ of subsets of the set of users. Every subset match to a key and elements of subset let *A* be the user that uses that key. It is assumed that along with the administrative key that lie in Γ set, the base station which act as a key server has a session key which known to all user and for each user there is a private key that is known to the user only.

The session key is needed by the base station for broadcasting or multicasting the encrypted data, whereas the private keys of user are used by user for unicasting encrypted data to the user and also for its authentication.

The dimension of EBS Γ is a situation of secure group where *n* users which can be named from 1 to *n* are present in this group and for each different set in Γ there is separate key.

The malicious users in the user collude to detect messages that they should not. EBS helps in reducing the collusion attacks. For example, let a key management system is formed in the form of tree where users are present at the location of leaves and the node of tree is the place for administrative key. Also, data encryption is represented by the root of the tree. The leaf represent the private keys of user. Every user from this position knows the keys from its location to the root only. These keys are only used to encrypt the rekeying and thus reduces the number of messages to send during rekeying and also reduces the collusion attacks.

2.2.3 Key generation algorithm

The dynamic key management scheme that helps in secure and efficient update of sensor nodes in cluster is done by making a public key that is associated many private keys. The base station set up the system parameters that is used in wireless sensor network lifetime.

The base station has responsibility to select these parameters:

- A large prime number such that $r = 2w + 1$, where w is also a prime number.
- An additive group and a multiplicative group D_1 and D_2 respectively both order r.
- A secret key which is also a master key z which is an integer.
- A random number say R from the additive group D_1.

The base station then calculate the system public key using ID based encryption $R_{pub} = zR$ which is then transmitted to all the gateways that are used in wireless sensor network. The base station also selects two hash function such that $J_1 : \{0,1\}^* \rightarrow D_1$ and $J_2 : D_2 \rightarrow \{0,1\}^*$. The gateway set private key and ID as $L_{ID} = zM_{ID}$ where $M_{ID} = J_1(ID)$.

The algorithm to calculate the key can be divided into three step encryption setup, Encryption and Decryption.

Encryption Setup

For communicating with m gateways, the base station setup the following parameters:

- Select a random integer u
- Calculate $U = uR$.
- Calculate $y_i = \hat{e}(rQ_{ID}, P_{Pub})$, where the function applied is weil pairing mapping.
- Calculate the following function $f(y) = \prod_{i=1}^{m}(y - y_i) \bmod r$.

  Thus we have the equation as follow

  $$\prod_{i=1}^{m}(y - y_i) = \sum_{i=0}^{m} b_i y^i \bmod r.$$

  Hence we can obtain the following constrain

  $$b_0 = \prod_{j=1}^{m}(-y_j) \quad (1)$$

  $$b_1 = \sum_{i=1}^{m} \prod_{j=1, j\neq 1}^{m}(-y_j) \quad (2)$$

  $$b_{m-2} = \sum_{i=1}^{m} \sum_{j=i+1}^{m}(-y_i)(-y_j) \quad (3)$$

  $$b_{m-1} = \sum_{j=1}^{m}(-y_j) \quad (4)$$

  $$b_m = 1 \quad (5)$$

  We can thus use the set $\{b_i\}$ to make the respective exponential functions.

$$\{b_0R, b_1R, b_2R, \ldots, b_nR \} \equiv \{R_0, R_1, R_2, \ldots, R_m\} \quad (6)$$

Encryption

If $C_k \in \{0,1\}^*$ is the session key that is use to encrypt the message then the encryption can be done as follows

- Select a random integer L and a random number I from additive group D_1.
- Calculate $(n + 3)$ tuple

  $K \leftarrow (L, C_k \oplus J_2(I), I + LR_0, LR_1, \ldots, LR_m) = (L, S, S_0, S_1, \ldots, S_m)$
- Broadcast K to gateways.

Decryption

When the gateways receive the K they can decrypt the session keys as follow

$$\hat{e}(L_{ID}, L) = y_i$$

$$S_0 + \sum_{j=1}^{m} y^j S_j = I$$

$$S \oplus H_2(I) = C_k$$

This algorithm has the desired properties which are required for clustered wireless sensor network. First of all most calculations are done in base station and the gateway only do the bilinear pairing, multiplication and logical ex-or. Each gateway stores only one key in its memory for the entire time. The system has a good scalability property.

Chapter 3 Microcontroller and RF module

3.1 AVR family

AVR family of microcontroller was developed by Atmel in 1996 and is based on RISC structure. These are 8-bit microcontrollers. These microcontroller were the first to have an integrated flash memory where program can be stored. Other microcontroller at that time had programmable ROM which can be programmed only once.

Requirement of external memory is thus neglected in most of the applications as flash, EEPROM and SRAM are all present in a single chip. These microcontroller also have parallel external bus. This option can be used to add data memory and other memory-mapped devices. Every microcontroller in this family except the TinyAVR microcontroller have serial interface. These interfaces can be used to interface microcontroller with large serial EEPROM and other flash chips based on the requirement of applications.

The flash memory is the non-volatile memory and can be used to store the program instructions. The register in the microcontroller are of 8 bit but every instruction can use one and sometimes two 16-bit word.

The size of the program memory is shown during the nomenclature of the microcontroller for example the microcontroller ATmega32 have 32 kB of programmable flash integrated in it.

However, provision for off chip programming is absent in these microcontroller that is the codes to be executed by the microcontroller should be present in the flash memory inside the microcontroller.

These microcontroller have register files, SRAM and I/O registers where data and address can be stored.

There are 32 8 bit register present in AVR microcontroller and has RISC architecture. The working register has the memory address from 0000 to 001F in hexadecimal notation that is the first 32 addresses. After the working register there are 64 memory address for I/O register that is from 0020 to 005F in hexadecimal. The SRAM starts from the address 0060 in hexadecimal.

Although the input output register and SRAM have separate addressing scheme for access, they both can be manipulated similarly.

The AVR microcontrollers have different number of PORTs. These ports are controlled by three registers and these are DDRx, PORTx and PINx, where x is the number of port to be controlled.

DDRx is the register that control the direction of the port that is the port is to be made input or output depends on the value present in this register. High represent the corresponding pin to be output pin and low represent the corresponding pin as input pin.

PORTx is the register that is used to assign the value to the corresponding output pin. High represents logic high to be output and low means logic low is to be output. This is used only in the case where the pin is in output mode.

PINx is the register where the input is stored. High means logic high is been written to the input pin and low means logic low is been written to the input pin. The microcontroller reads the value with the help of these registers.

The microcontroller in the AVR family have non-volatile internal memory EEPROM which is used for data storage. This EEPROM cannot be addressed using the addresses as it is not mapped into memory space. This can only be accessed using read-write instruction and also using pointer registers. This makes EEPROM slower than RAM.

The AVR microcontrollers have two stage pipeline structure which is single level. The meaning of the above statement is that while the microcontroller executes the instruction it simultaneously fetch the next instruction. This means that the microcontroller takes maximum two cycles to complete the instructions. This makes the AVR microcontroller fast in accordance with the other 8 bit microcontroller.

3.2.1 AVR CPU core

CPU core of AVR microcontrollers make sure that programs are being executed correctly. The CPU thus be able to grant access to the memory and be able to perform the necessary calculation, control the desired peripherals and run the interrupt service routines whenever there is interrupt to the microcontroller.

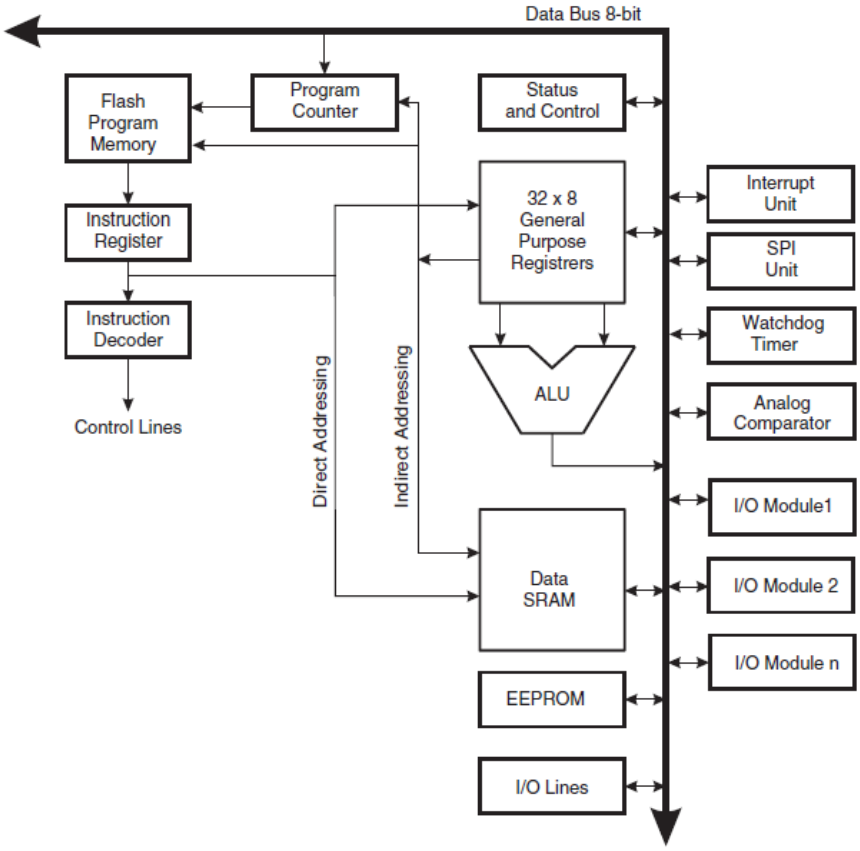


Figure 3.1 Architecture of AVR family

Architecture of AVR is based on Harvard architecture so as to maximize the parallelism and performance index. This means that there is separate memory and bus for both data and program. The program is executed with the help of pipeline structure. This allows the microcontroller to execute one instruction per clock cycle thus making the microcontroller fast.

There are 32 8 bit register which are general purpose which can be accessed within a single clock cycle and hence are fast access registers. This make the ALU operation single cycle. When ALU operation is taking place, two operands are input to the ALU from the register sets, operations are then perform on the operands and the result is output from ALU and is stored back in the register sets.

Out of 32 registers six registers can be used for indirect addressing mode by using them as 16 bit to point the data. This helps in an efficient way of calculating address. One of them can be used to point the lookup table in memory.

3.2 Attiny85

Power management**:**

- Very low power consumption.
  Active mode: 1MHz, 1.8V, 300μA
  Power down Mode: 0.1 μA @ 1.8 V
- A power reduction register gives a method to reduce power consumption.
- Three different sleep modes: idle mode, ADC noise reduction mode, power down mode.
- Idle mode: it enables microcontroller to wake up due to external interrupts and internal interrupts as well.
- ADC noise reduction mode: it improves ADC's noise environment and enables higher resolution for measurements.
- Power down mode: this mode stops all generated clocks and it will allow only asynchronous module operations.

Universal serial Interface (USI) features:

- Synchronous data transfer via two wires.
- Synchronous data transfer via three wires.
- Interrupt on data reception.
- In two wire mode it can wake up from all sleep modes.
- It has start condition detector in two wire mode and with interrupt detection.

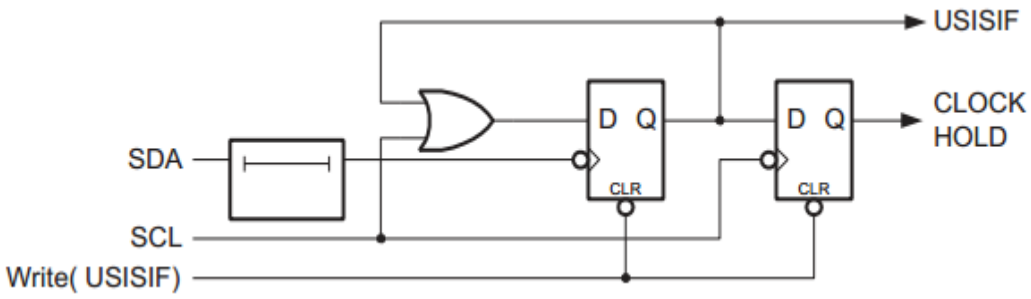


Figure 3.2 Start condition detector logic diagram

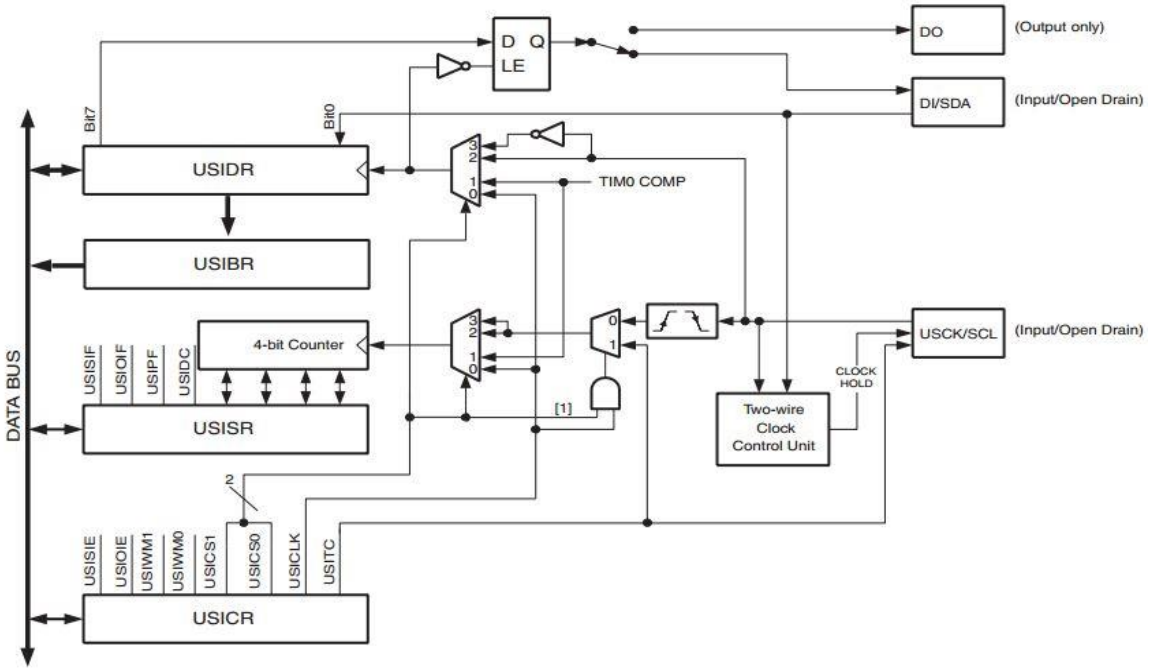


Figure 3.3 USI functional block diagram

- Three wire mode: this mode is useful in SPI mode 0 and 1. But it does not have CSN (chip select not) pin functionality. However the software implementation of this feature is possible. This mode uses pin names as DI, DO, and USCK.

  Figure 4.4 shows two USI units working in three wire mode, one is master and another is slave. The data registers of two USI units are connected in a manner that data between both registers are interchanged after 8 clock pulses (USCK). To detect the completion of a transfer counter overflow flag (USIOIF) can be used.

  The clock is generated by software in master device by toggling the pin USCK with the help of PORTB or by setting 1 to the bit USITC in USICR register.

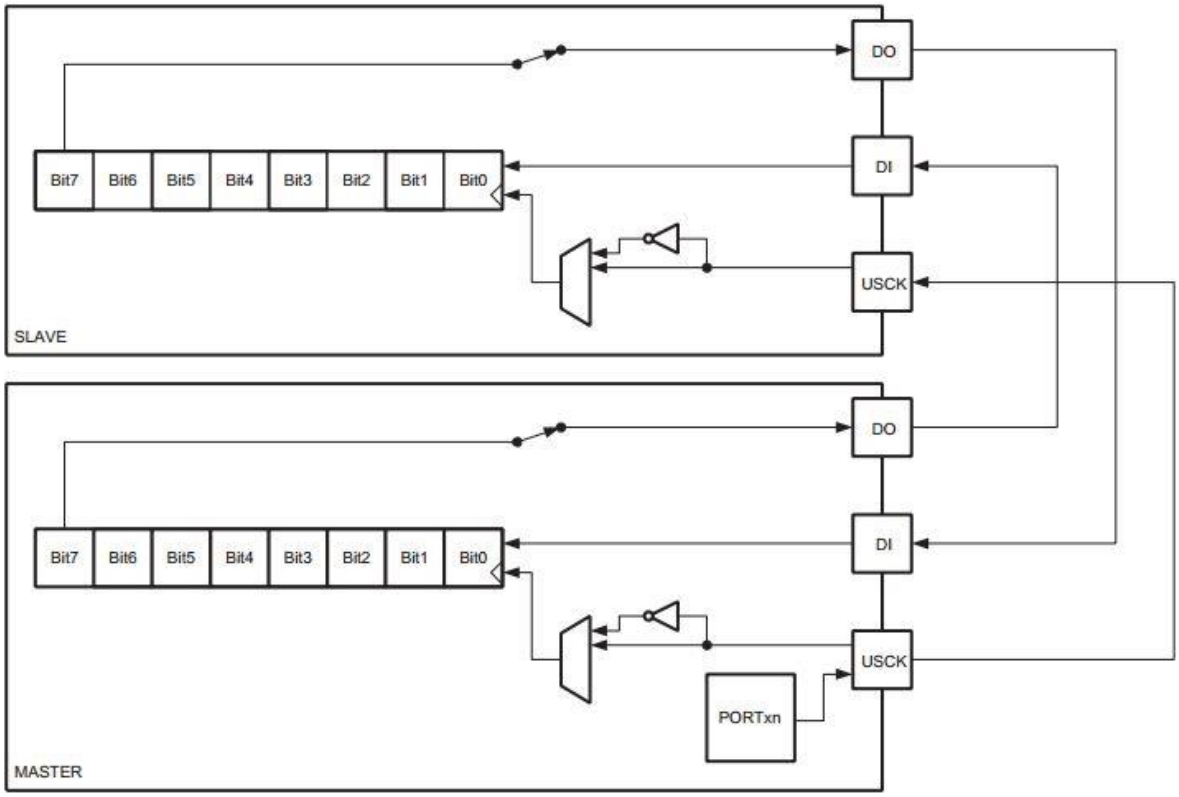


Figure 3.4 Three wire mode operation

Peripheral Features:

- Two PWM channels
- 8 bit timer/counter along with prescaler
- 8-bit high speed timer/counter with separate prescaler
- Output compare registers which are double buffered
- Phase correct pulse width modulator which is glitch free
- Three (TOV0, OCF0A, and OCF0B) independent interrupt source
- Auto reload on compare match (clear time)
- PWM period is variable.
- A programmable watchdog timer/counter with internal oscillator.

High Performance CPU:

- Advanced RISC architecture with a rich instruction set.
- 32 general purpose registers combined with the instruction set.
- Two independent registers can be accessed in the execution of single instruction in single clock cycle.
- ATtiny85 provides 8K bytes of In system programmable flash.
- 512 bytes of EEPROM and 256 bytes of SRAM.
- 6 general purpose I/O lines.
- Designed with volatile memory technology with high density.
- DebugWire on chip debug system

- Supply voltage 2.7-5.5 V
- On chip oscillator

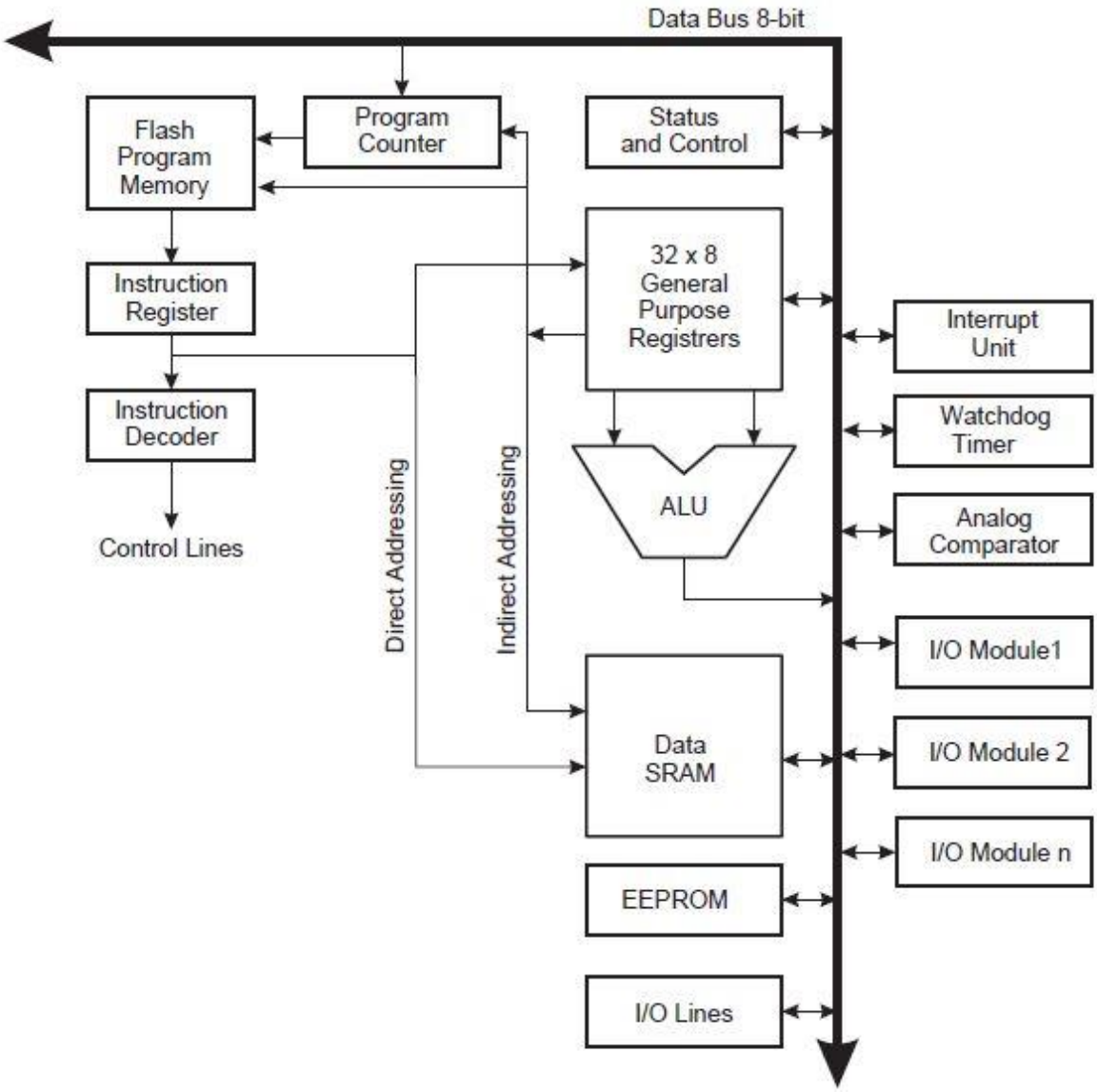


Figure 3.5 Block diagram of AVR architecture

Analog features:

- 4 single ended channel 10-bit analog to digital convertor
- 2 differential ADC channels having programmable gain.
- On chip Analog comparator.

Instruction Set for AVR:

Mnemonics	Operands	Description	Operation	Flags	Clock Note
ADD	Rd, Rr	Add without Carry	Rd ← Rd + Rr	Z,C,N,V,S,H	1
ADC	Rd, Rr	Add with Carry	Rd ← Rd + Rr + C	Z,C,N,V,S,H	1
ADIW	Rd, K	Add Immediate to Word	Rd+1:Rd ← Rd+1:Rd + K	Z,C,N,V,S	2 (1)
SUB	Rd, Rr	Subtract without Carry	Rd ← Rd - Rr	Z,C,N,V,S,H	1
SUBI	Rd, K	Subtract Immediate	Rd ← Rd - K	Z,C,N,V,S,H	1
SBC	Rd, Rr	Subtract with Carry	Rd ← Rd - Rr - C	Z,C,N,V,S,H	1
SBCI	Rd, K	Subtract Immediate with Carry	Rd ← Rd - K - C	Z,C,N,V,S,H	1
SBIW	Rd, K	Subtract Immediate from Word	Rd+1:Rd ← Rd+1:Rd - K	Z,C,N,V,S	2 (1)
AND	Rd, Rr	Logical AND	Rd ← Rd • Rr	Z,N,V,S	1
ANDI	Rd, K	Logical AND with Immediate	Rd ← Rd • K	Z,N,V,S	1
OR	Rd, Rr	Logical OR	Rd ← Rd v Rr	Z,N,V,S	1
ORI	Rd, K	Logical OR with Immediate	Rd ← Rd v K	Z,N,V,S	1
EOR	Rd, Rr	Exclusive OR	Rd ← Rd ⊕ Rr	Z,N,V,S	1
COM	Rd	One's Complement	Rd ← $FF - Rd	Z,C,N,V,S	1
NEG	Rd	Two's Complement	Rd ← $00 - Rd	Z,C,N,V,S,H	1
SBR	Rd,K	Set Bit(s) in Register	Rd ← Rd v K	Z,N,V,S	1
CBR	Rd,K	Clear Bit(s) in Register	Rd ← Rd • ($FFh - K)	Z,N,V,S	1
INC	Rd	Increment	Rd ← Rd + 1	Z,N,V,S	1
DEC	Rd	Decrement	Rd ← Rd - 1	Z,N,V,S	1
TST	Rd	Test for Zero or Minus	Rd ← Rd • Rd	Z,N,V,S	1
CLR	Rd	Clear Register	Rd ← Rd ⊕ Rd	Z,N,V,S	1
SER	Rd	Set Register	Rd ← $FF	None	1
MUL	Rd,Rr	Multiply Unsigned	R1:R0 ← Rd × Rr (UU)	Z,C	2 (1)
MULS	Rd,Rr	Multiply Signed	R1:R0 ← Rd × Rr (SS)	Z,C	2 (1)
MULSU	Rd,Rr	Multiply Signed with Unsigned	R1:R0 ← Rd × Rr (SU)	Z,C	2 (1)
FMUL	Rd,Rr	Fractional Multiply Unsigned	R1:R0 ← (Rd × Rr)<<1 (UU)	Z,C	2 (1)
FMULS	Rd,Rr	Fractional Multiply Signed	R1:R0 ← (Rd × Rr)<<1 (SS)	Z,C	2 (1)
FMULSU	Rd,Rr	Fractional Multiply Signed with Unsigned	R1:R0 ← (Rd × Rr)<<1 (SU)	Z,C	2 (1)
Branch Instructions					
RJMP	k	Relative Jump	PC ← PC + k + 1	None	2
IJMP		Indirect Jump to (Z)	PC(15:0) ← Z, PC(21:16) ← 0	None	2 (1)

Table 1

Connection Diagram: This connection is recommended in ATtiny85 datasheet. Also this is connection for In-system-programming of microcontroller through ISP.

The remaining connections which includes the pins (I/O) and peripherals are described in other sections of this thesis.

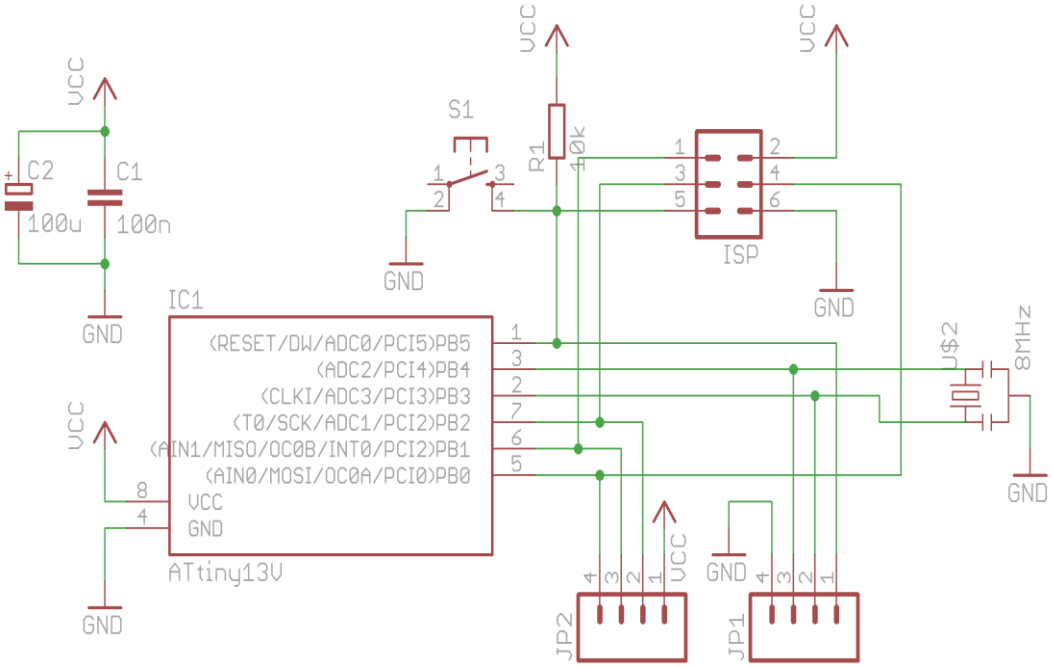


Figure 3.6 ATtiny85 connection diagram

3.3 Atmega328

Atmega328 is 8 bit microcontroller in AVR family. This is based on RISC architecture. It can have throughput as high as 1 MIPS per MHz. This is done by completing the instruction in single clock. This allow the designer to optimize speed and power.

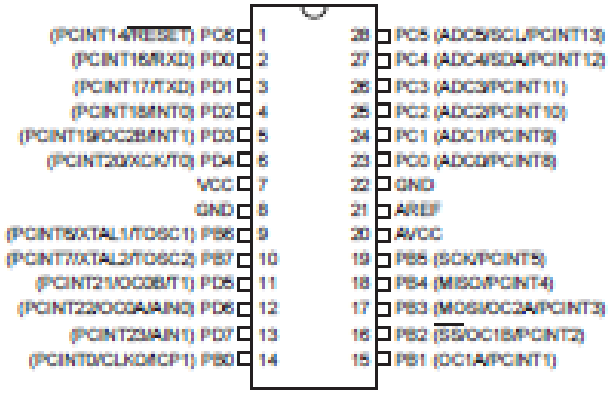


Figure 3.7 Pin diagram of Atmega328

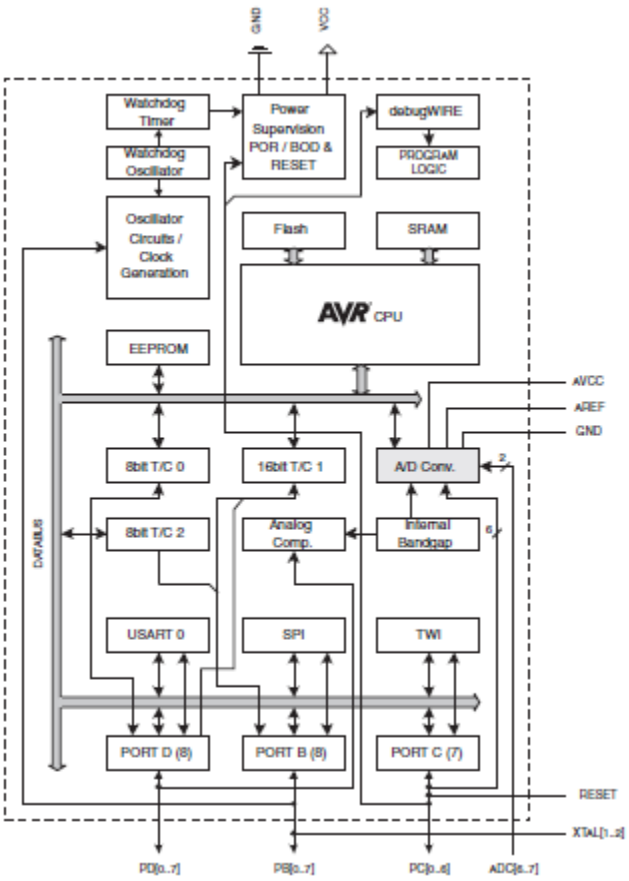


Figure 3.8 Block diagram of Atmega328

The features of Atmega328 microcontroller are as follow

- It has 8K bytes of programmable flash memory with the capability of both reading from and writing to the memory.
- It has 1K bytes of EEPROM
- It has 2K bytes of SRAM.
- It has 23 input output line that is general purpose.
- It has 32 working register that is general purpose.
- It has three timer or counter.
- Programmable USART.
- SPI serial port.
- 10 bit ADC.
- Watchdog timer which can be programmed and has internal oscillator.

3.4 Arduino board with Atmega328

Arduino Uno board is based on ATmega328 microcontroller. It consists of 14 digital I/O pins out of which 6 can be used as PWM channels.

It has 16 MHz ceramic oscillator, an ICSP header, a power jack, USB connection, and a reset button. It has everything that is needed to support a microcontroller. Its feature summary is given as following:

- Operating voltage is 5 V.
- DC current per I/O pin is 40mA.
- DC current for 3.3.V pin is 50mA.
- ATmega328 has 32KB of flash memory out of which 0.5KB will be used by boot loader.
- 2 KB of SRAM.
- 1KB of EEPROM.
- Recommended input voltage is 7-12V.
- USB Overcurrent protection for more than 500mA.

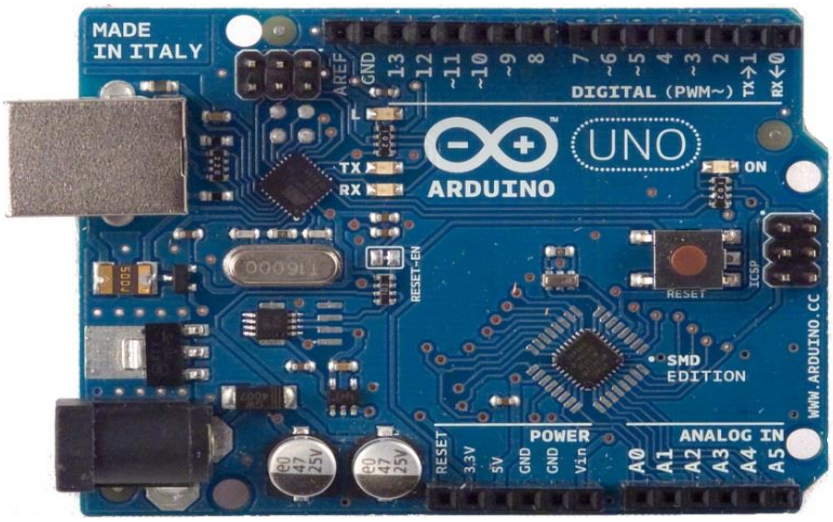


Figure 3.9 Arduino UNO with SMD

3.5 NRF24l01

The module is nothing but RF transceiver which operate at frequency 2.4GHz. This is manufactured at Nordic Semiconductor. The application of this module is basically for ultra low power wireless communication. It is connected to the microcontroller using SPI serial interface.

It sends acknowledge back to the microcontroller as soon it receive. Microcontroller send the command and data after processing it and is to be transmitted. The module uses GFSK passband modulation to transmit the baseband data. It has its own baseband protocol engine which is called enhanced shockburst.

It has 8 pin which when connected with microcontroller can be used as wireless module. In order to connect it with microcontroller and operate it, it must be interfaced with microcontroller using SPI interface. The configuration register of the nrf24l01 are contained within the register map and thus can be accessed by SPI interface. The register map can be accessed by microcontroller in any mode of the module.

Enhanced shockburst which is the embedded baseband protocol engine is based upon the packet communication. It maintains the modes of module for advance autonomous protocol operations. The data is exchanged between the module and the microcontroller is done using a FIFO queue. The enhanced shockburst handles all the operation that is to take place at high speed layer which reduce the cost of the system.

GFSK modulation is used to transmit and receive the data by the module. The air data rate, frequency to be used and power are all configured by the user. The data rate option for the module are 250Kbps, 1Mbps and 2Mbps. The configurable power by the user helps to make the communication optimize for the power and thus can be used for ultra low power applications like the wireless sensor networks.

3.6 LM35: temperature sensor

The LM35 is a temperature sensor whose output voltage is in direct proportion to the temperature. Thus, to obtain the temperature in conventional centigrade the user doesn't have to subtract or normalize the value of the voltage. This makes it advantageous over the kelvin scale temperature sensors.

Its features are as follows

- It is calibrated to centigrade scale as 10mV/C.
- It has an accuracy of 0.5C calculated at 25C.
- Its range is from -55C to 150C.
- It has operating voltage from 4V to 30V.
- It has a very low self heating, 0.08C at 25C in still air.
- It has a output impedance of 0.1 ohm.

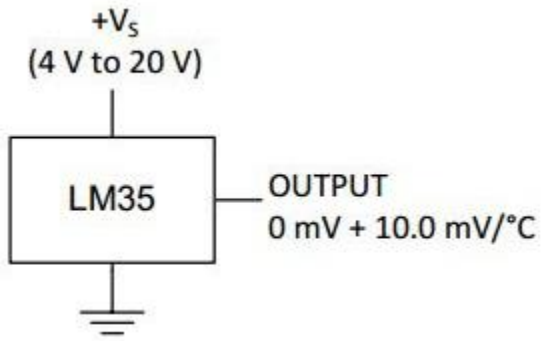


Figure 3.10 temperature sensor from 2C to 150C

3.6 PIR sensor

These sensors are used to sense the motion. Within its range it can detect the presence of humans. They are low power and easy to use. They are cheap and has long life. Thus they are very popular in all type of personal and business applications. They are also called IR motion sensor and passive infrared sensors.

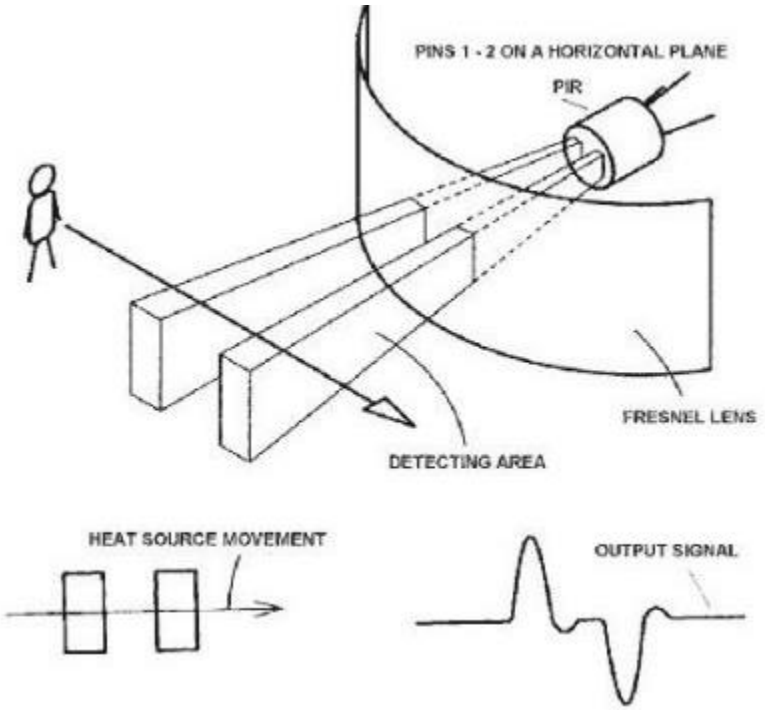


Figure 3.11 working PIR

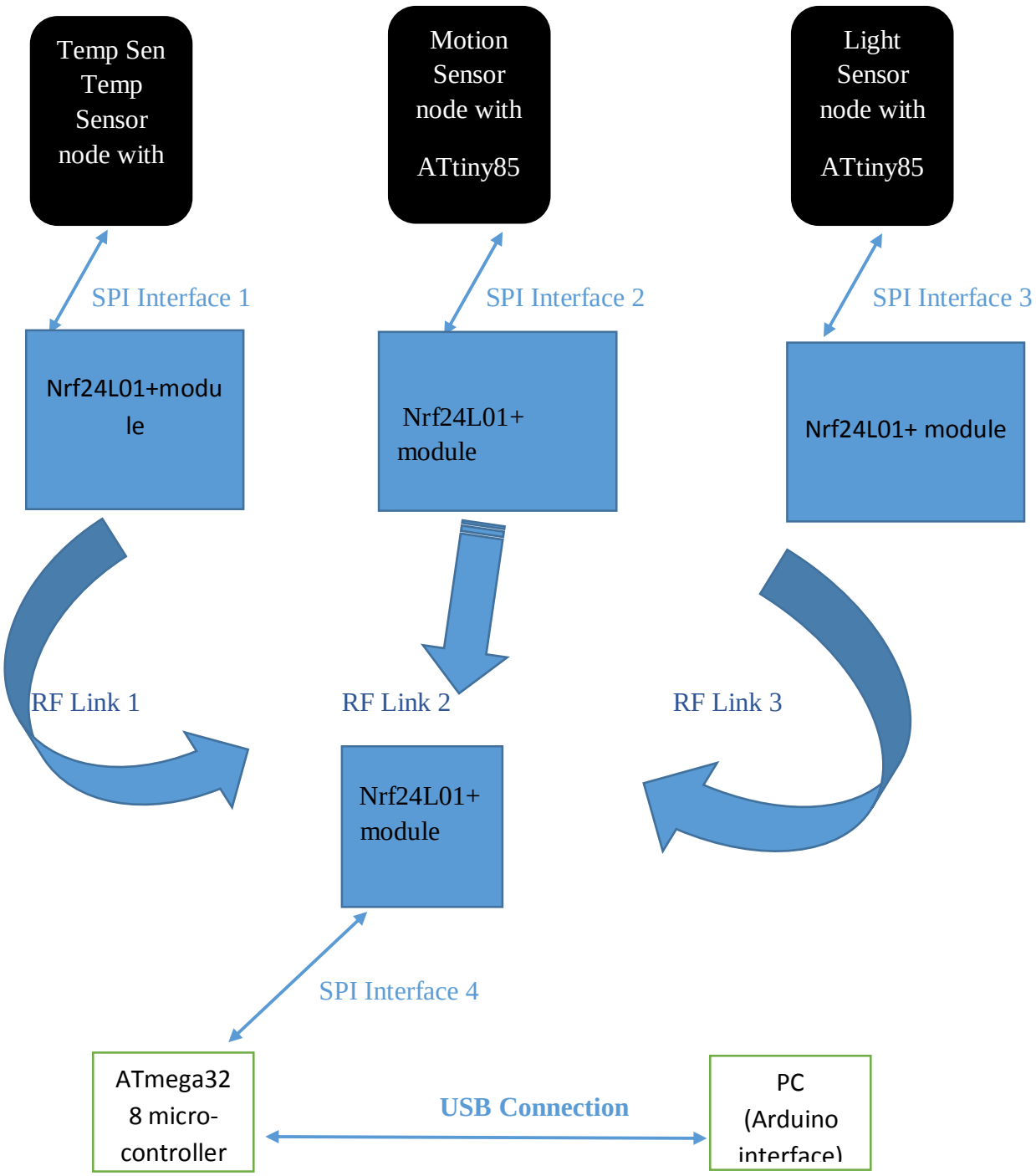
Chapter 4 System Design

4.1 System design

This section explains the implementation of the Wireless sensor networks. The system design of the WSN can be divided into two parts: hardware design and software design.

4.2 Hardware design

Figure 4.1overview of the model



4.2.1 Sensor nodes

The sensor nodes have a sensor that detect the condition which is being monitored. In our case the sensor used are PIR sensor for motion detection, temperature sensor for temperature measurement and light sensor for light intensity detection. The sensor sends the data to the microcontroller. The microcontroller used here is the attiny85. The microcontroller uses the ADC which is inbuilt in them to convert the analog data from the sensor to the digital data. The digital data is then processed by the microcontroller.

4.2.2 Power supply branch

The power supply branch consist of a 9V battery and a XC6203X332 voltage regulator. The voltage regulator converts the 9V power to 5V power. After conversion is done it supply the 5V power to the components.

4.2.3 RF module

The RF module used is the NRF24l01. This is a transreceiver that works at 2.4GHz. This module is ideal for ultra low power RF transmission and reception. The microcontroller is connected to the RF module using SPI interface. The RF module has three mode in which it works, receiving mode, transmitter mode and standby mode.

The microcontroller control the RF module by selecting the mode according to requirement. When it want to transmit the data, it set the module to the transmitter mode. When it want to listen, it set the module to the receiving mode. When the microcontroller is ideal it set the module to the standby mode. As the RF section is the most power consuming section, presence of standby mode is important as it can save power which is already in limit. The nrf24l01 uses FSK modulation at passband and have Gaussian filter as the pulse shaping filter. Thus, it can also be said that nrf24l01 uses GFSK passband modulation.

4.2.4 SPI interface

SPI or serial peripheral interface was first used by Motorola. This interface is based on the master slave interaction. It is a full duplex mode as there is separate data lines for both direction of data. The master slave interaction can have many slave and single master but here only one master and one slave is used. It has four serial data bus. Each one for clock, transmitting data, receiving data, and chip select. It is also called synchronous serial interface sometimes.

4.2.5 Construction

The hardware consist of three sensor nodes each of which has attiny85 microcontroller which controls them. They have nrf24l01 module for RF communication.

The topology formed by these nodes is the tree topology. The parent node of this topology is the base station and the sensor nodes are the child node of the topology. The base station controls the child node or the sensor nodes. The sensor nodes transmit the data to the base station as soon as they sense the environment.

The base station is the Arduino Uno board which have Atmega328 microcontroller. It is connected to the laptop or a computer using a USB cable. The data is collected by the base station using the RF module and is then displayed on the screen of laptop by using the GUI of Arduino Uno.

4.2.6 Working

There are four sensor nodes that form the wireless network using the tree topology. These nodes together can be used for smart home system as they can provide security, temperature monitoring and light controlling. All the sensor nodes remain in standby mode until the base station triggers activation signal to the node.

Base station

It will check the lock password that the user will enter before entering the room. In case of wrong password the base station will ask the user for three more attempt after which the lock will be blocked and the password will be reset to any random digits. The alarm will be triggered and the new password will be sent to the user through telnet. In case the user enters the correct password in the first place, the motion sensor will turn off and the light and temperature sensor will be turned on.

```
while user enters password do
    read password;
    if entered password is correct then
        Turnoff PIR sensor ;
        Turnon Light sensor;
    else
        attempt++;
        show(enter correct password);
        if attemp ≥ 3 then
            send alert message to use;
        end
    end
end
```

PIR motion sensor

When the user locks the room, the base station turn this sensor in on state. In case of any intrusion entry, the node will detect the motion of the intrusion and will send an alert message to the user according to the frequency of motion. When user enters the room by unlocking the door, the base station turns it off.

Light sensor

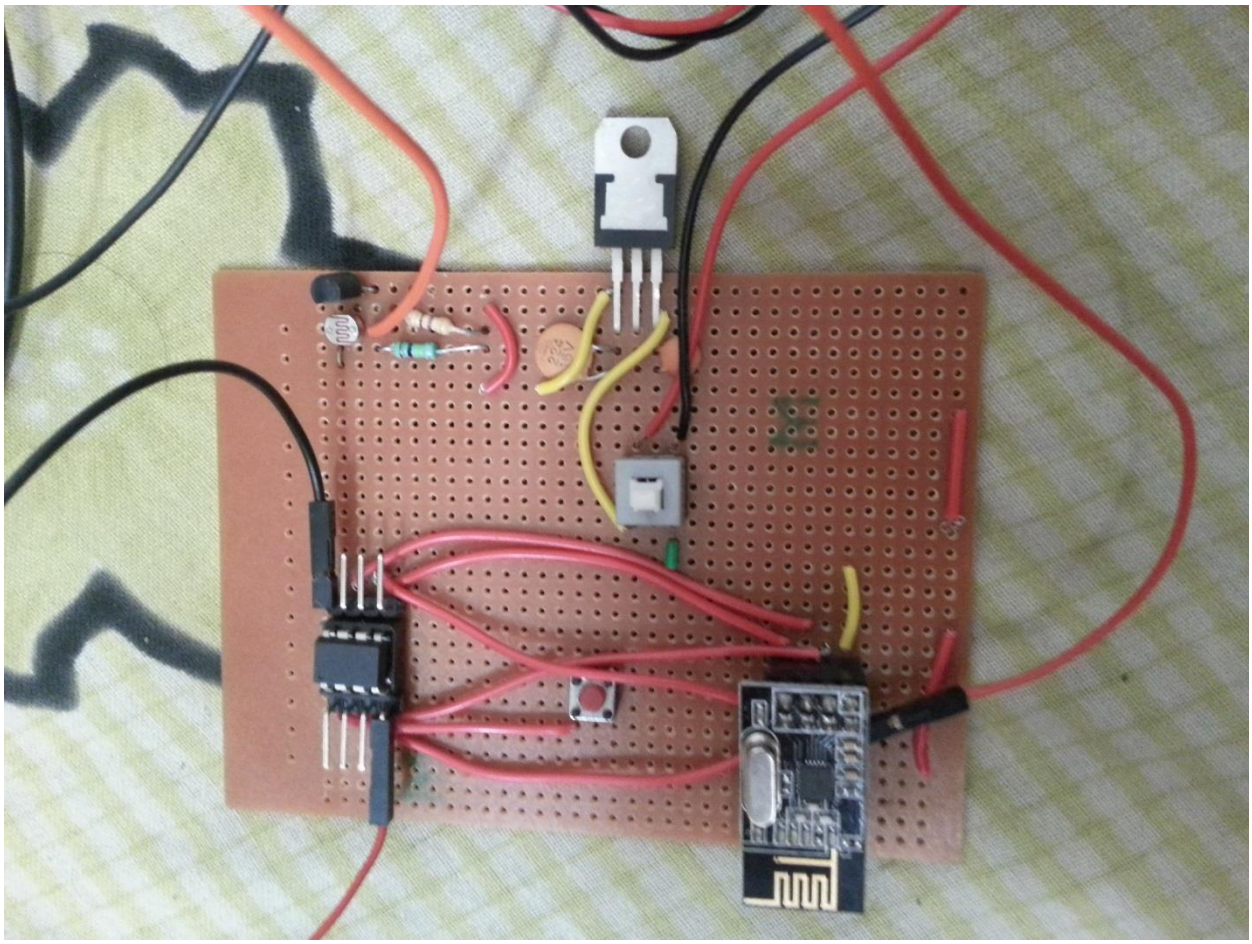
When the user leave the room, the base station tells the light sensor to turn itself off and thus turning off all the lighting system. But when the user is in the room in the first place, the sensor node remain in ON state and continuously monitor the intensity of light in the room according to which it control the lighting in the room.

Chapter 5 Result

The work done in this thesis consist of implementation on sensor nodes that can be used for security and light control. For this, attiny85 microcontroller was used to design the sensor nodes and Arduino uno board with atmega328 was used as base station. The wireless RF module was NRF24l01+ which was used as a transceiver. The base station was connected to the computer or laptop using a USB cable. The data was sent to the base station by the sensor nodes and was seen on the screen of computer.

For security and integrity of data, a security scheme based on elliptic curve cryptography was used. The sensor nodes and the base station were able to encrypt the data using the key which was sent by the base station for each session of communication. The key was sent in a secure form so that only the valid node was able to find out the key. The following pictures show the sensor nodes which was implemented and the data which was encrypted and decrypted using the key sent by the base station.

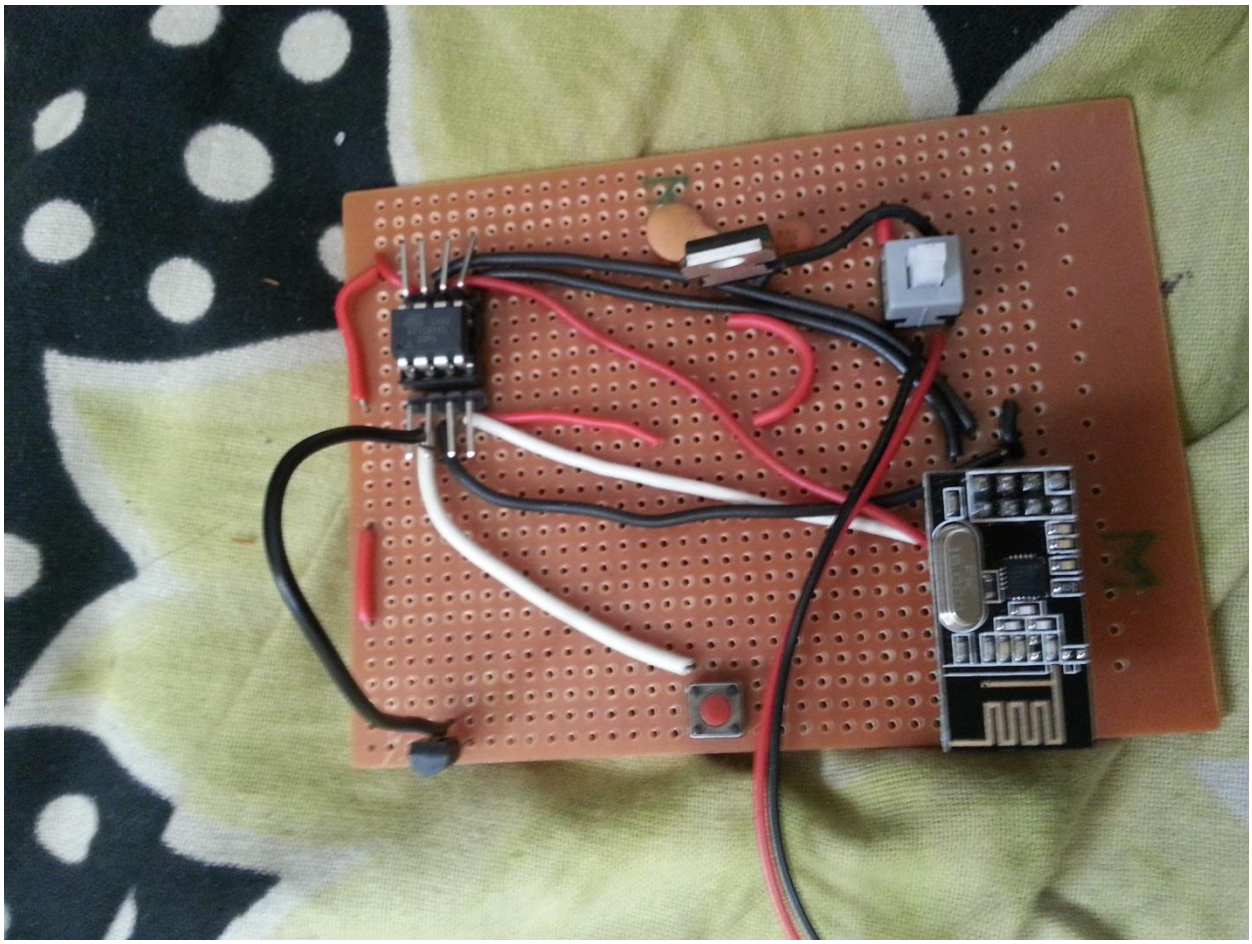
Figure 5.1 Light Sensor



This figure show the light sensor which has LDR where the potential drop changes as the light intensity changes. The output of LDR is fed to the microcontroller which after

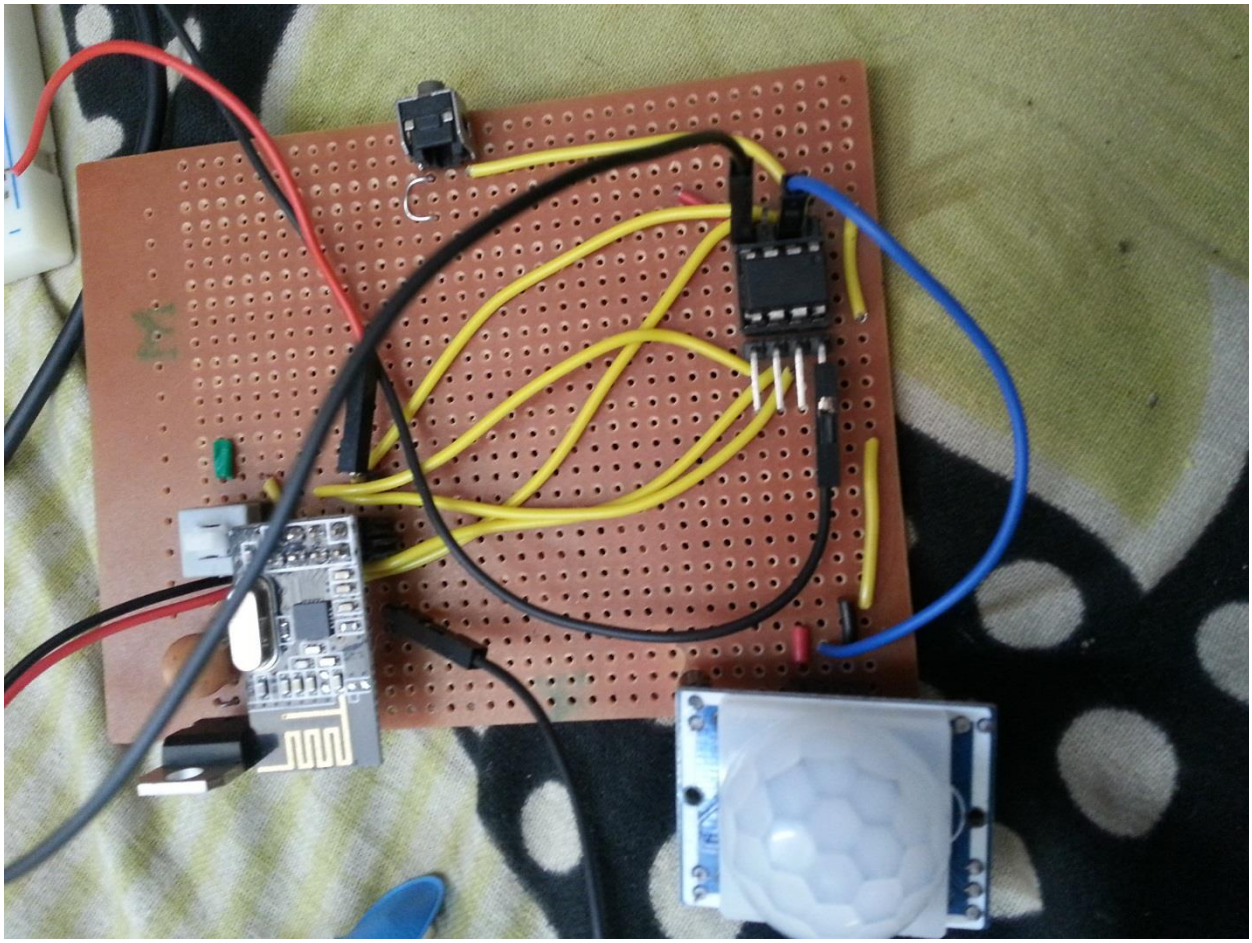
converting the analog value to the digital value sends the data to the base station through RF module shown in figure.

Figure 5.2 Temperature sensor



This figure shows the temperature sensor node. The temperature is sensed using the lm35 temperature sensor. The temperature sensor senses the temperature and then send the raw analog data to the microcontroller. The microcontroller processes the data to make it suitable for data viewing and then send the data to the base station using RF module as shown in figure.

Figure 5.3 Motion Sensor



This figure shows the motion sensor. The motion sensor used here is the PIR sensor. The PIR sensor when sense the motion of human, it sends a low to high pulse transition to the microcontroller attiny85. The microcontroller after finding this transition send an alarm to the base station using the RF module as shown in figure.

Figure 5.4 Security result

```
data =

    31


encr1 =

33E7073E02864


Sk13 =

DE7073E02864


data1 =

    31
```

The above figure is snapshot to show the data send by temperature sensor and is encrypted using key Sk13. The key is sent using the algorithm described in the above section. The data is then decrypted using the key at base station. After the session was over and no data was flowing the key was expired and a new key was generated at the time of new session.

Chapter 6 Conclusion

Conclusion

A group of sensor nodes are designed using nRF24l01+ RF module. Home security prototype is developed by using PIR motion sensor, Light sensor and temperature sensor. All these nodes are controlled by base station. The prototype consumption power is less and cheaper than the existing work. NRF24l01+ can be used for small network, as it doesn't support true mesh topology. Security scheme based on elliptic curve cryptography is deployed on each node. IDs of the sensor nodes is their physical address. This scheme protects the wireless sensor network from malicious traffic. Future goals are: To increase number of node, deploying routing protocol, comparing the sensor node with Zig-bee nodes.

Bibliography

1. Woo, A. and D. Culler, Evaluation of Efficient Link Reliability Estimators for Low-Power Wireless Networks, 2002: Technical Report, UC Berkeley.
2. Cerpa, A., et al, Habitat monitoring: Application driver for wireless communications technology. ACM SIGCOMM Workshop on Data Communications in Latin America and the Caribbean 2001.
3. Mainwaring, A. et al., Wireless Sensor Networks for Habitat Monitoring, in Acm International Workshop on Wireless sensor networks and applications 2002.
4. Xu, Y., J. Heidemann and D. Estrin, Geography-informed energy conservation for AD Hoc routing 2001, ACM Press: SIGMOBILE: ACM special interest group on mobility of systems, users, data and computing.
5. Yarvis, M.D., et al, Real world experiences with an interactive ad hoc sensor network 2002: International Conference on Parallel processing workshops.
6. Combinatorial Optimization of Group Key Management by Mohamed Eltoweissy, M. Hossain Heydari, Linda Morales an I. Hal Sudborough
7. (W. Fumy an P. Landrock, “Principles of key management” IEEE Journal of Selected Areas in Communications, vol, 11, pp, 785-793, June 1993)
8. (Combinatorial Optimization of Group Key Management by Mohamed Eltoweissy, M. Hossain Heydari, Linda Morales an I. Hal Sudborough)
9. (Y. Mu and W. Susilo, “Identity based instantaneous broadcast system in mobile ad-hoc networks” in the 2004 international workshop on mobile systems, e-commerce and agent technology, USA, 2004)
10. (D. Boneh and M. Franklin, “Identity based encryption from the weil pairing” Advance in cryptology-crypto vol 2139 LNCS, 2001)
11. (S. Marinkovic, C. Spagnol, and E. Popovici, Energy-e_cient tdma-based mac protocol for wireless body area networks," in Sensor Technologies and Applications, 2009. SENSORCOMM'09. Third International Conference on, pp. 604{609, IEEE, 2009.)
12. (Alemdar and C. Ersoy, Wireless sensor networks for healthcare: A survey," Computer Networks, vol. 54, no. 15, pp. 2688{2710, 2010.)
13. Junqi Zhang. "A New Security Scheme for Wireless Sensor Networks", IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference, 11/2008

14. Marnane, W, S Faul, C Bleakley, R Conway, E Jones, E Popovici, M de la Guia Solaz, F Morgan, and K Patel. "Energy efficient onsensor processing in Body Sensor Networks", 2010 Annual International Conference of the IEEE Engineering in Medicine and Biology, 2010.
15. Zhang, J. "Wireless sensor network key management survey and taxonomy", Journal of Network and Computer Applications, 201003
16. S. Moon. "CRMS: A Collusion-Resistant Matrix System for Group Key Management in Wireless Networks", 2008 IEEE International Conference on Communications, 05/2008
17. Kubisch, Martin. "Heterogeneous Energy- Constrained Wireless Sensor Networks: Selected Hardware Aspects", Technische Universität Berlin, 2008.
18. He, Xiaobing, Michael Niedermeier, and Hermann de Meer. "Dynamic key management in wireless sensor networks: A survey", Journal of Network and Computer Applications, 2013.
19. Gupta, Megha, Mohammad S. Obaidat, and Sanjay K. Dhurandher. "Energy-Efficient Sensor Networks", Handbook of Green Information and Communication Systems, 2013.
20. M. Essaaid. "Towards an operative land surface temperature in-situ measurements system for remote sensing models validations", Proceedings 2005 IEEE International Geoscience and Remote Sensing Symposium 2005 IGARSS 05, 2005
21. "8-bit AVR Microcontroller with 2K Bytes In- System Programmable Flash", Radioengineering, 2011.