# Certificate

It is hereby certify that work which is being presented in this thesis **"Design and Develop ECC for the Wireless Sensor Networks"**, in partial fulfillment of the requirement for the award of degree of Master of Engineering in Software Engineering submitted in Computer Science and Engineering Department of Thapar University, Patiala is an authentic record of research work carried out under the supervision of **Dr.Maninder Singh** and refers other researcher's work which are duly listed in the reference section. The matter presented in thesis has not been submitted for the award of other degree of this or any other university.

(Vandana Ladha)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr.Maninder Singh)
Associate Professor
Computer Science and Engineering Department
Thapar Unversity
Patiala

**Countersigned by**

**(Dr. Rajesh Bhatia)**
**Head**
**Computer Science & Engg. Deptt.**
**Thapar University,**
**Patiala**

**(Dr.R.K.Sharma)**
**Dean(Academic Affairs)**
**Thapar University,**
**Patiala**

# Acknowledgement

I would like to express sincerest thanks to my thesis supervisor Dr.Maninder Singh, Associate Professor, Computer Science and Engineering Department for his inspiration, guidance, stimulating suggestions, immense help and support throughout the period of this research work. He has provided me with all the necessary resources including motivation and research environment without which it would not have been possible to complete this work. It was a great opportunity for me to do this work under his supervision.

I would like to thank Dr. Rajesh Bhatia, Assistant Professor and Head, Computer Science and Engineering Department for his moral support and the resources he had facilitated for this work.

I would also like to thank all my teachers for their stimulating discussions and invaluable support I received during this period of research. I am thankful to the authors whose work I have consulted and quoted in this work.

Finally, I wish to thank my dearest family and friends especially Yogesh Kumar and Tikka Singh (Computer Science and Engg.) for all their immense love, enthusiastic, encouragement and support throughout my life without which it would not have been possible to complete this work. Last but not the least I would like to thank God who has always been with me in my good and bad times.

Vandana Ladha

(800831025)

# Design and Develop ECC for Wireless Sensor Network

*Thesis submitted in the partial fulfillment of the requirements for the award of degree of*

**Master of Engineering**

**In**

**Software Engineering**

*by*

**Vandana Ladha**

**Roll No 800831025**

**under the supervision of**

**Dr. Maninder Singh**

**(Associate Professor)**



COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

Patiala-147004

July-2010

# Certificate

It is hereby certify that work which is being presented in this thesis **"Design and Develop ECC for the Wireless Sensor Networks"**, in partial fulfillment of the requirement for the award of degree of Master of Engineering in Software Engineering submitted in Computer Science and Engineering Department of Thapar University, Patiala is an authentic record of research work carried out under the supervision of **Dr.Maninder Singh** and refers other researcher's work which are duly listed in the reference section. The matter presented in thesis has not been submitted for the award of other degree of this or any other university.

(Vandana Ladha)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr.Maninder Singh)
Associate Professor
Computer Science and Engineering Department
Thapar Unversity
Patiala



**Countersigned by**

**(Dr. Rajesh Bhatia)**
**Head**
**Computer Science & Engg. Deptt.**
**Thapar University,**
**Patiala**

**(Dr.R.K.Sharma)**
**Dean(Academic Affairs)**
**Thapar University,**
**Patiala**

# Acknowledgement

I would like to express sincerest thanks to my thesis supervisor Dr.Maninder Singh, Associate Professor, Computer Science and Engineering Department for his inspiration, guidance, stimulating suggestions, immense help and support throughout the period of this research work. He has provided me with all the necessary resources including motivation and research environment without which it would not have been possible to complete this work. It was a great opportunity for me to do this work under his supervision.

I would like to thank Dr. Rajesh Bhatia, Assistant Professor and Head, Computer Science and Engineering Department for his moral support and the resources he had facilitated for this work.

I would also like to thank all my teachers for their stimulating discussions and invaluable support I received during this period of research. I am thankful to the authors whose work I have consulted and quoted in this work.

Finally, I wish to thank my dearest family and friends especially Yogesh Kumar and Tikka Singh (Computer Science and Engg.) for all their immense love, enthusiastic, encouragement and support throughout my life without which it would not have been possible to complete this work. Last but not the least I would like to thank God who has always been with me in my good and bad times.

Vandana Ladha

(800831025)

# Abstract

Wireless Sensor Networks consist of sensor nodes and few powerful control mobile laptops performing activities like routing, data aggregation etc over wireless media. These kind of networks are getting popular these days because of small size, ease of handle and installation. Because of this property they are used in environment like military, hospitals, weather forecasting etc. for processing critical information.

However such kind of environment is more prone to *"Man In the Middle Attack"*, where attacker can easily perform malicious activities without interrupting network operation, which can further propagate to other nodes that can alter say routing information and even can degrade the network performance and stability. To overcome such security issues researchers had proposed various techniques like data encryption/decryption, authentication, key generation/distribution. But due to small memory size and battery life of sensors, WSN suffers from resource constraints. Thereby major issue is to design key transmission and management protocol that consumes less resources. Beside this they should be scalable and flexible enough as any number of node at any time can leave and enter the network.

In traditional network systems, Public Key Cryptography and Symmetric key Cryptography are used for providing these security services and protocols and they are used together for secure network implementation. As far as past research is concerned Symmetric key cryptography could not be applied because of resource constraints on sensor nodes particulary because of low battery life. This lead the researchers to develop more solutions based on PKC like hash tables, key cryptography etc. But scientist created a milestone by developing a discrete problem based algorithm and finally they identified ECC as a most optimal and efficient algorithm.

Among the two i.e. RSA and ECC former is resource hungry thereby later is well suited algorithm in such scenario as it generate key of relatively small size and less power is consumed for key management

In this report we have designed ECC algorithm and implemented it over a simulated network created with the help of Java Sun Spot kit, consisting of two sensor devices and a basestation. Here by going through the work done by different researchers where they have compared both RSA and ECC algorithm with the help of automated tool over different factors, it can be concluded that ECC is the most optimal and efficient algorithm for wireless communication. Using Java SunSpot kit a wireless sensor network is formulated and devices are made to communicate with Elliptical Diffi-Hellman Algorithm implemented over it, the packet are then captured and verified using the automated tool.

*Keywords:Wireless Sensor Networks, PKI, Elliptical Curve Cryptography, SunSpot devices*

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

This chapter gives a detailed description of Wireless sensor network and its general architecture. Here, need of security in such environment, major attacks that are possible in such environment and the defensive measures that can be taken to save the critical information to be hacked, is also described.



## 1.1 Background

By the immense effort of researchers in wireless communication, Micro Electro Mechanical System(MEMS) have opened a route to modern civilization which has been densely populated with the low-power, cost-effective and automated devices knows as sensors.

These sensors devices are capable of storing and processing real time data which is helpful in preparation and prevention during the phases of pre-event, responses during the event and post recovery along with the analysis of the event[7]. When networked, sensor networks can not only provide data collection but can also be used for performing and controlling multitude task. Because of it sensor networks are used in various applications like monitoring temperature, humidity, pressure,

soil, vehicle movement, lightening conditions etc.[7]

## 1.2 Wireless Sensor Networks

Wireless Sensor or Wisenet is the network formed by sensor devices that are capable of communicating with each other over wireless media. After the portable devices like PDA, mobiles etc. these devices are emerging at a high speed. Inspite of their small size and memory these sensor device act as a powerful CPU which can be easily portable, installed and handled also known as "Sensor Motes". Due to this they are finding its application in most critical environment like in military, hospitals, weather forecasting, agriculture for purposes of transmitting routing, personal, temperature and pressure information over limited bandwidth and frequency.

Sensor motes consist of microcontroller, transceiver with antenna for receiving and transmitting data, memory having Operating System installed over it. Various companies came into play for developing sensor device like MICA, INTEL and the latest is SunMicrosystems supporting different operating system like TinyOs, JavaSqwak depending upon their performance.



### 1.2.1 Architecture of WSN

A general architecture of WSN consist of sensor nodes communicating over wireless media and a base station. Base station collect the information and broadcast it further to the Gateway which then send server and display it over the screen of the web client requesting the particular information. The entire scenario is shown in the Figure 1.1 given below, where the wireless media is shown with the dashed lines. Inspite of the local network one can also have basestation attached to a single

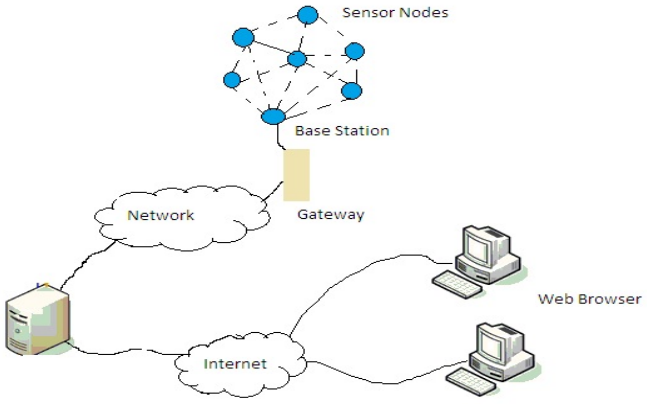


**Figure 1.1** Architecture of WSN network.

machine running a host application for displaying results of the data so collected.

### 1.2.2 Application area of WSN

Wireless Sensor networks are becoming popular because of their small and ease of installation. Thereby used in very sensitive environment, some of them are discussed below:

- **Civil Engineering** :Structure Monitoring is the latest application of sensor networks where they are attached to heavy structures like bridges, building and then analyzed for the strain they gain while passing of the train and their tolerance power.

- **Industry Automation**:It is not always possible to keep on track of maintainable of heavy and large machines and it is not always mandatory also. So in industries these machines are embedded with sensors that keep on diagnosing machines and apprise whenever the maintainable is required.

- **Military environment**:In military environment sensors are used to trans-

mit sensitive information,detecting presence of movements of enemy units on land/sea,identifying chemical and biological threats,targeting systems and controlling command within the army units.

- **Agriculture**:Now a days, Wireless sensor network is helping our farmers a lot in detecting soil moisture,presence of pesticide and Ph level of water and soil that help farmers in detecting which crop to cultivate and which effective measure should be taken to save the crop.

- **Public safety**:For security purpose WSN is playing an effective role, as it usage in airports help in determining presences of weapons, specialized luggage tags, physical location of disaster.

- **Hospitals**:In hospitals sensors are formulated by embedding them into machines, that helps in diagnosis of patient, communication, determining wearing out of machines, in operations for detecting presence of unwanted material in body like stones, doing bypass surgery etc. There are various other application of such networks but discussing all of them is out of scope of this thesis report.



## 1.3 Significance of Wireless Sensor Networks

In the above section various application of WSNs has been described. Now in the following section various features of WSNs that make it eligible to be used in such diversing environment has been discussed:[7]

- Sensing accuracy:Using variety of sensors nodes in the network increase the accuracy level of the data collected as compare to a single node.

- Area coverage:This feature signifies that a efficient network cover a wide geographical area without adding any additional cost to the network.
- Fault tolerance:Due to the redundancy of sensor device as well as the information, the network is capable of functioning even in faulty condition.
- Connectivity:Sensor nodes are connected to the sink node and also the wired connection of the internet.This basically enables them to share only relevant information.
- Minimal Human Interface:Having less interaction of the human with the system make it less prone to error and can continue its work without any interruption.
- Dynamic sensor scheduling:Using some scheduling criteria the sensor network can set the priority for data transmission.



## 1.4 Security in WSN

### 1.4.1 Need of Security in WSN

Wireless sensor networks are becoming more popular in most critical environment as in military, hospitals etc where they have to perform mission-critical tasks. Security is of main concern in such sensor networks because of their resource constraints and of the nature of communication they do i.e wireless. So implementing security in such network is more important than that of wired networks. Without taking security factor into consideration an attacker can easily analyze the packet and breach out the important information being transmitted between the nodes, known as eavesdropping or can easily inject their own packet. Researchers found that in

sensor networks, security should be implemented during design time for ensuring secrecy of sensitive information, privacy of people and safe operation over sensor networks.

### 1.4.2 Major Attacks in WSN

As per the constraints of WSN, major attacks are categorized as *"Man In The Middle Attack"* . The various other attacks included in such scenario are discussed below:

1. **Sniffing:**In this kind of attack, the attacker place the attacking node nearby the sensor grid capture the data by analyzing information transmitted over shared medium and collected at the attacker side, where he can perform any malicious activities using the gathered information. This kind of attack is possible because of the inherit vulnerability of wireless network i.e. unsecured wireless media.

2. **Data Integrity attack:**The attacker here compromise the data traveling within the network by making change in it and falsify the victim's research.This kind of attack is possible because of the weakness of protocol used for route discovery and data transfer.The attacker node here consist of processing ,memory,power capability greater than that of the sensor node. Because of this kind of attack the attacker can alter routing information making it useless that can come with a DoS attack.

3. **Energy Drain Attacks:**This attack is possible because of the fact that the sensor node posses limited battery life and most of the power is consumed in radio transmission. Here the attacker node, radiates large amount of traffic

and force the sensor node to respond. The mandatory requirement of this kind of attack is that the attacker node should posses the greater transmitting radiation strength to split the network and get hold over any of its part.

4. **Black Hole Attack:**Attacker here places the node in such a way to publish it as the shortest route within the network thereby attracting most of the traffic. This malicious act is possible because of the vulnerability of routing protocol. Because of this successful attack the attacker can launch another attack like data integrity and sniffing.

5. **Hello Attack:**In this attack the attacker fools the sensor nodes to be the base station thereby attracting most of the traffic to the attacker node. Here also the attacking node must have higher radio range and transmitting power. This attack helps the attacker to launch other attacks and act as a alternative to the black holes.

6. **Wormhole Attack:**In this attack,the intruder node act as a repeater between two nodes.Thereby the attacker creates the wormhole which forces the sensor nodes to identify it as the neighbor node.The basic goal here is to undermine cryptography used and to confuse the protocols.



### 1.4.3 Security Issues in WSN

Creating a security design for WSN is quite critical as it different from traditional networks as it suffers from various constraints. So for developing a particular security approach one has to understand the constrains some if the are listed below:

- **Very Limited Resource**:Every security approach requires data and code memory and energy to power the sensor. WSN networks consist of very small

devices i.e sensor. Any security policy designed for such network should be less resource hungry. As like the desirable code should be small in size that occupy less memory space over sensor device e.g Tiny OS and Java Sqwak are operating system designed specially for such n/ws. Energy is the another biggest factor that governs the design of any security policy designed for such networks, as sensor once deployed proved to be costly. Therfore battery life taken to the field must be conserved to extend the life of individual sensors and entire network. Before implementing any cryptographic policy its energy impact should be taken into consideration as they consume energy for various functions like encryption, decryption, key management etc.

- **Unreliable Communication :**This kind of constraints is due to the inherit nature of WSN networks as Wireless sensor network has connectionless media of transfer so any attacker can by creating certain program can analyze the data and can sniff out the secure data transmitted between the sensor nodes. Even if the media is reliable the another constraint here is *Conflict*. This is due to the nature broadcasting messages nature of sensor network.So when the congestion is high packets carrying valuable data destroyed easily and will never reach it destination. *Latency* is the yet another constraints due to the congestion and multi-hop routing because of which synchronization is achieved between sensor nodes, which is very critical requirement for various security functions like key distribution, reports etc.

- **Unattended operation**:Due to some reason the sensorial go unattended which can face three caveats like *Physical Attacks*, in sensor network, a node is more prone to physical attack as compared to PC placed remotely in secure networks. *No Central Management*, sensor networks should be distributed de-

sign for secure mechanism. Moreover, more the nodes are unattended, more the chances nodes are compromised by sensor nodes.

### 1.4.4 Security requirement of WSN

After having deep knowledge about WSN and its constraints we can underline major security requirement of WSN. They have been listed below:

- **Data Confidentiality** : Because of the inherited vulnerability of WSN, data confidentiality should be made the major ingredient of Security policy created for such networks where sensor nodes are capable of sending the data securely to the neighbor nodes, especially in military environment. Apart from this other kind of sensitive data like public and private key should be made secure from traffic analysis.

- **Data Integrity**: Adding confidentiality doesn't mean that entire security is achieved. An attacker after sniffing data can alter the alter it and again can inject within the network that after reaching the node can initiate some malicious activity which can give wrong results or even can crash the entire network. So Data Integrity is yet another requirement of such networks.

- **Data Freshness**: Sensors should made sure that data send over the network should be fresh i.e no old messages should be replayed over network. This is basically used in case of shared keys that keep on changing and if this requirement is not considered the attacker once sniffing the key would replay with it again and again. For this counter must be used that can determine freshness of data.

- **Authentication**: An attacker inspite of modifying the data packet can inject

stream of packet by itself so the receiver must ensure that the is originated from the intended source. Also this feature is necessary for performing various administrative task required for managing sensor networks.

- **Self-Organization**: Wireless networks are typical ad-hoc networks so the sensor node are flexible and independent enough for self organizing themselves as no infrastructure has been proposed yet for such dynamic network. For implementing various cryptographic algorithms and its functions like key distribution the sensor nodes must be capable of self organizing themselves, otherwise the network is prone to hazardous attack.

### 1.4.5 Defensive measure

Eavesdropping is the major threats within WSN where attacker can sniff the packet and even change it. Effective measure should be taken to save the data from the malicious attack that effect the secrecy of data. One of the solution given by researchers is in the modulating the data in a unreadable human form that ensures secrecy and authorization of data. In the following section it has been discussed that how it can be achieved:



### 1.4.6 Cryptography

Cryptography is a science and art for encrypting sensitive information in a unreadable human format while communicating over unsecured media so that it is transmitted and processed by intended receiver. It basically involve two core mechanism *Encryption* and *Decryption*. Figure 1.2 gives a brief description of entire cryptographic mechanism.

Initially the messages is encoded into human unreadable format known as *Encryption* from the sender side and then released over the network,on receiving the message is decoded at the receiver side using the same algorithm known as *Decryption.*Here the algorithm used for encryption and decryption is known as cryptophytes and the encoded message is cipher text and decoded message is known as decipher text.The algorithm or key used in cryptosystem are very complex as they consist of mathematical formulae and concept. This reveals the fact that the strength of any ciphered message depends upon the difficulty level of understanding the algorithm.Cracking such algorithm can be possible but it consumes a large amount of resources in terms of time, power and money. Basic purpose of doing cryptography is to achieve three things

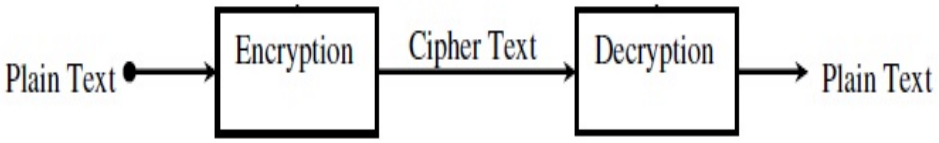


**Figure 1.2** Cryptographic Method

- Confidentialety:It means the secrecy of message should be maintained.
- Authentication: Only the intended receiver should receive the message.
- Non repudiation: It refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

The basic cryptographic algorithm are divided into two kind i.e Symmetric and Asymmetric Cryptographic algorithm. They can be discussed briefly as in following section:

### Symmetric Algorithm

As the name specifies in Symmetric Algorithm same key is given to both sender and the receiver and because they are kept private so it is also knows as private key algorithm. The entire mechanism has been shown in the Figure 1.3:

Here the sender encrypts the message using the secret key and the reciter decrypts

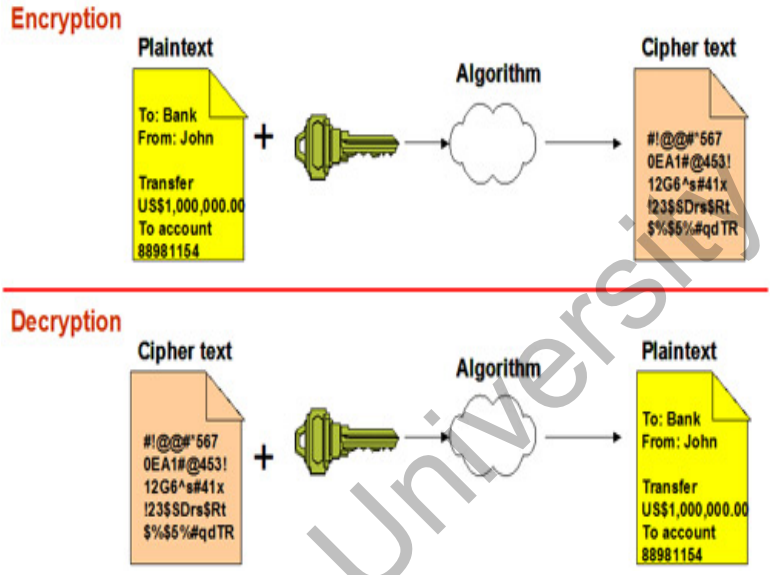


**Figure 1.3** Symmetric Key Mechanism

it using the same key. Number of Algorithm are their that follows symmetric key algorithm as basic principle like DES, RSA etc and many more are there.

Various issues are associated with the symmetric algorithms are:

- **Scalability** :As the number of communicating node increases over the network the performance degraded as they have to maintain a separate key for each and every node.So every time a node want to communicate with other, some processing has to cover the overhead of generating the key and storing and managing the key, this will automatically have effect on the performance of the individual system.

- **Key distribution**: As the communicating nodes same keys and they uses the media for transferring keys. Here an intruder if get over the hand over key he can then easily decrypt the encrypted messages.

- **Limited Security:**Symmetric algorithms can only provide confidentiality but no authentication and non-repudiation.

Another solution has determined to achieve the three basic security elements while communicating over the network i.e. confidentiality, integrity and availability.

**Asymmetric key Cryptography**

Asymmetric key cryptography is so called as here both sender and receiver are allocated different set of keys i.e public key and private key. Here public key is known to all the users over the network want to communicate with the owner and the private key is only known to the owner. Here the algorithm generate a set of pair for every system, but they are not mathematically related i.e. if any intruder get hold of any of the key the another cannot be obtained. However the messages encrypted with a private key can only be decrypted using the corresponding public key.
A general scenario of public key cryptography has been shown in the Figure 1.4: Here the sender will encrypt the message with receivers public key in secure message format this can as only be decrypted using receivers private key so ensures the confidentiality and authenticity. Now when to have secure and signed message format the sender will encrypt the data its private key and then again encrypt it with receiver private key, this covers the concept of digital signature. So the main advantage of asymmetric key over symmetric key are :

- **Highly scalable** :Every machine require one pair of private and public key

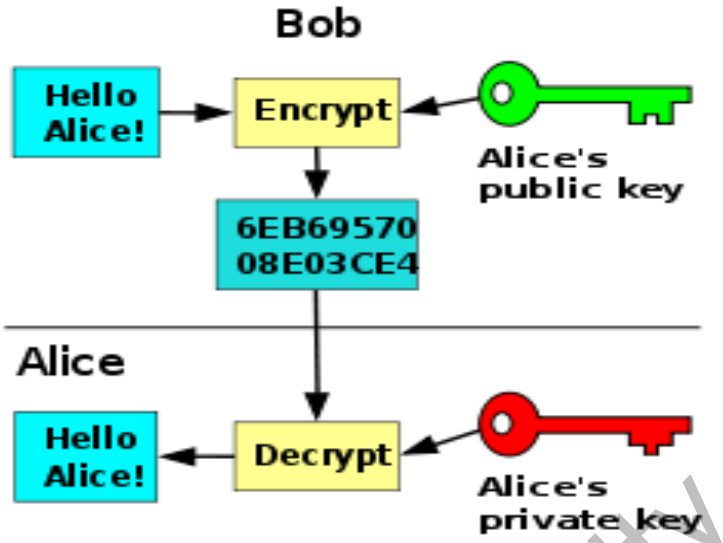


**Figure 1.4** Asymmetric Key Mechanism

for secure data communication.

- **Proper Key distribution**:Private key remain with the owner so it is never hacked.
- **Security elements:**The three elements of security are achieved here.

Researchers and scientist have worked over various issues that still remain uncovered and they come up with different algorithm with Public Key Infrastructure(PKI) our main area of concern is ECC that is discussed below:

### Elliptical Curve Cryptography

Elliptical Curve Cryptography or ECC is found to be the best solution until now as RSA was subsided because it doesn't fully satisfies the resource constraints. According to ECC based on Deffi-Hellman Algorithm is depicted in Figure1.5 where a point G is selected from Elliptical curve E. For Alice(A) and Bob(B) communicating, A

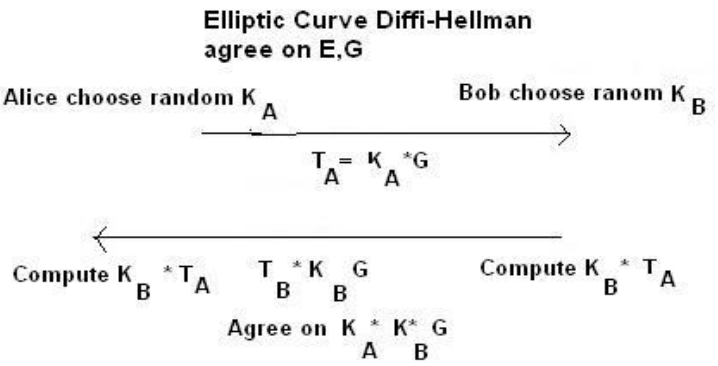


**Figure 1.5** Elliptical Curve Cryptography Mechanism

generates private key $K_a$ and the public key is generated as $T_A$ as $T_a = K_a * G$ and B generates the $K_b$ as private key and public key as $T_b = K_b * G$. Here they generates their shared key as $K_a * T_b = K_a * K_b * G$ and Bob computes the shared key as $K_b * T_a = K_b * K_a * G$. Because $K_a * T_B = K_b * T_b$, now Alice and bob now shares a secret key. This thesis work is an attempt to implement ECC on WSN and showcase its usefulness over other techniques.

The next chapter, literature survey, discuss in detail work done by other authors, followed by chapter on implementation of ECC on SunSpot.

# Chapter 2

# Literature Survey



Wireless Sensor Network has been discussed in very brief in the previous chapter. However going through literature one can identify that researchers has put their heart and soul in understanding the concept in depth, identifying the issues and stating out their solutions. The following sections describe the research till date in brief by different authors that helped me a lot in underlining this research work:

Smart environment is an evolutionary step in various fields like industry, home, hospital, military etc for automating entire system. However such smart environment rely upon sensory data that come from the real world. Sensors are the devices used for collecting such information that are located distributed geographic locations. However for accuracy of data, decision making, monitoring and analyzing data, to have meaningful information, Wireless sensor network came into scenario[1]. F.L Lewis, Head of the Department of Sensors MEMS Group has described the complex scenario of the usage of sensors.

### Wireless Sensor Networks

Sensors are found to be of small size, low-power, low-cost devices that are capable of collecting and even processing sensory information from its surrounding. The radio antenna embedded over the device, flexibility and portability make it capable to be used in wireless environment. Such a network of sensors communicating over wireless media is known as Wireless sensor network[2]. The three author of this paper has done a survey over wireless network and published this paper in year 2001, it helped a lot in understanding the concept. Wireless Sensor networks are also defined as the set of independent node communicating over a limited frequency and bandwidth[4]. According to the authors F.Amin, A.H. Jahangir and H Raisefard, *Wireless Sensor networks consist of small nodes that sense the environment, process the data and communicate through the wireless links.*

A general Architecture of Wireless Sensor network has been described in a presentation[3] given by Rabi Mahapatra. This architecture has been shown in Figure 2.1, describing the scenario of a Wireless Sensor Network connected to outside world via Internet. The Figure 2.1 consist of sensor devices analyzing the environment events, capturing data and transmitting it to the intermediary node known as *forwarding node* and finally the data reaches to base station also known as *sink node* i.e responsible of processing the data. Finally through the gateway data is transmitted to the outside world.

### Application of Wireless Sensor Networks

Sensor posses very unique characteristics of analyzing environment conditions like room temperature, pressure, humidity and even presence of intruder, along with it they are capable of processing data and analyzing it. In a survey done on wireless sensor network, number of applications are discussed[2]. The Figure 2.2 depicts a

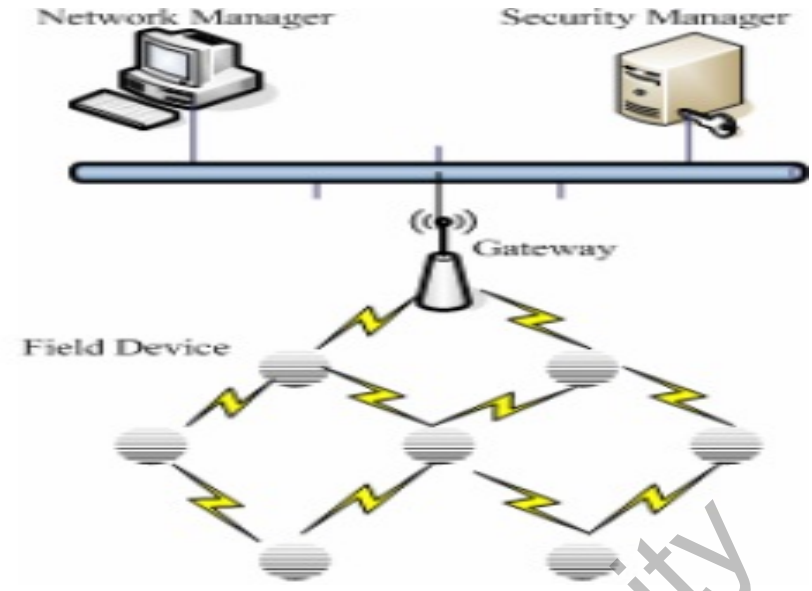


**Figure 2.1** WSN Architecture [29]

scenario where WSN is applied to different fields: This paper describes different area applications of wireless sensor network.

1. **Health applications:**In hospitals, integrated wireless sensor network used for diagnostic patient, drugs administration and movement of unwanted animals like flies in the hospital environment, maintenance of machines etc.

2. **Environmental applications**: Sensors are capable of sensing environment conditions like temperature, humidity, pressure so they are used in flood detection, weather forecasting, forest fire detection, movement of birds and animals that can effect the crop.

3. **Vehicle Monitoring** :Identifying vehicle theft and keep information about its condition is now been done by wireless sensor network. In case of threat one can easily trace out the vehicle as the sensor device is embedded in the machine and also the vendor can easily track out when the machines need maintainable so as to provide better service to its customer .

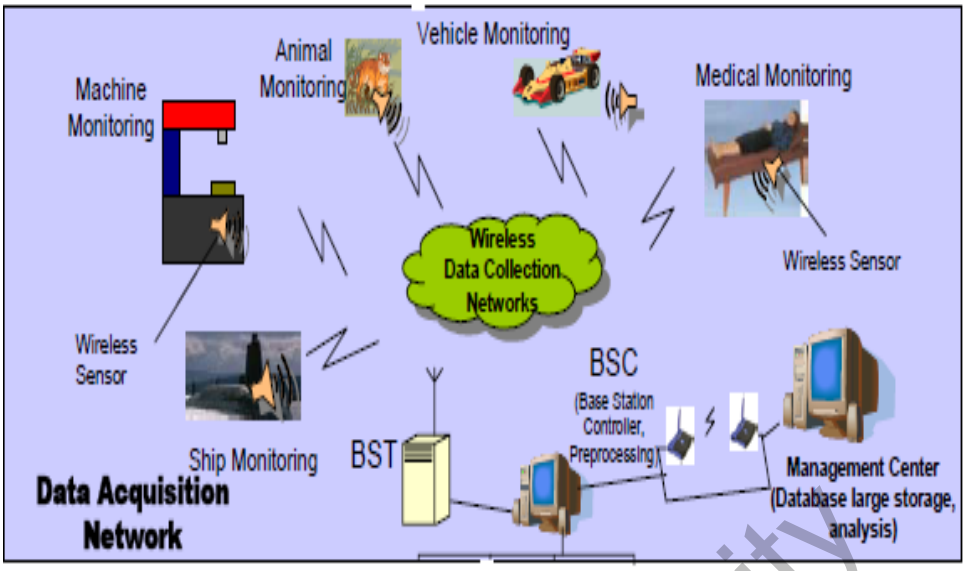


**Figure 2.2** Application Scenario of WSN in various fields[2]

4. **Structural Monitoring:**Wireless sensor networks are becoming more popular in mechanical engineering and civil engineers where mechanics embedded sensors in machines and can easily identify its wear and tear out condition. Similarly civil engineers embed these sensors into buildings and bridges and detect when they want maintainable.

5. **Military applications**:WSN are very popular in military area for identifying presence of an intruder and for communicating private information.

6. **Home applications** :Sensor devices are capable of making household work automated where they are embedded with in the home appliances like VCR, vacuum tubes,grinder etc and are able to communicate with each other by forming a sensor network so that one can perform all the functions remotely.

**Practical application of WSN networks**: In the paper *Smartening the Environment using Wireless Sensor Networks in a Developing Country* written by the joint effort of three author a practical application of Wireless Sensor Networks have

been defined. WSN setup is done for the country Bangladesh which is considered to highly susceptible to the environment calamities like flood, cyclones, tsunami etc. So researchers thought of a system which can give an alarming warning to them with which they can take better action to take the event in control. Hence the development of wireless sensor network to assist meteorologist has a great importance in coastal areas as specifically discussed in the paper[7]

**Flood and water level Monitoring System**:It is considered as the matter of courage to confront the situation when natural disaster such as earthquakes, floods tsunami etc are concerned. The problem of flooding was not solved even when lot of cost was spent over the remote sensing system, satellite and mobile communication. Finally the with the global information and communication infrastructure development there is a new technological achievement in form of WSN. However it is a matter of fact great effort and cost was involved for setting up a sensor network for flooding system in tropical region like Bangladesh[7].

The *flood monitoring system* here consist of three levels i.e. *Data Collection* and *Data Distribution* and *Data analysis*. In data collection one is deal with setting up of the sensor network at the riverbanks and collection up the data as according to the local environment. The data distribution phase one deal with setting up of the base station for communicating data at local as well as the district level. In the data analysis phase one deal with the decision making and analysis of data at central monitoring system.and then again the cycle starts from the first phase. There are various other situation where WSN is applied in Bangladesh like in *traffic control system*, *weather forecasting* but discussing all of them is of scope of this thesis.

**Security requirement in WSN:**

Wireless Sensor network is an emerging technology and is used in various real time and critical sceneries like in military, industries, home, traffic monitoring, health monitoring etc and explained above. One of the major challenge that the Wireless Sensor Networks are facing today is *Security*. Any vulnerability in such scenario if ignored can cause a disaster specially to the scenarios which are highly critical where any mistake can be proved as a *blunder*[10].

Now before discussing it should be known what are the kind of security required in WSN so that we can narrow down our scope for discussing loopholes in different application area. According to F.Amin, A.H.Jahangir and H. Rasifard the security in WSN can be classified in two types:

- **Operational Security** :This kind of security is needed when the we want a network to b continue function even when any of its component is attacked.
- **Information Security** :This kind of security is needed when the critical information is to be saved from the attacker. Basic three principles required to be achieved these are:
  - *Confidentiality*-to maintain the secrecy of data.
  - *Integrity*-to send the data to the receiver without doing any change.
  - *Authenticity*:sending data to intended receiver.

Table 2.1[5] shows what are the threats possible if any loop hole is left undetected while creating an WSN in different application scenario and how the above three properties are effected. *Security elements in WSN*

In the above section we have discussed the basic requirement of security in wireless

**Table 2.1** Possible security threats, grouped according to Application Domain. Here C=Confidentiality I=Integrity and A=Authentication.[5]

| Application domain | Potential Security Threats | Properties Violated |
|---|---|---|
| Military | Denial of Service Attack<br>Supply of misleading information<br>Eavesdropping of classified information | I<br>C<br>A |
| Environmental Monitoring | Suppose government-endorsed environmental sensors are installed near factory to minitor air/water quality to make sure the factory's emission lies beneath the pollution threshold, however by feeding the sensors with worng information, the factory allows itself to escape detectiion and let its polluting emission go unchecked. | I |
| Health/Medical | Providing wrong physiological measurements of a patient to the career or doctor, a miscreant may cause potentially fatal diagnosis and treatement to be performed on the patient | I,A |
| Industry | Eavesdropping of commercial secrets by business rivals. | C |
| | Intentional disruption of manufacturing processes as a result of misleading sensor readings caused by disgruntled employees or business spies | I |

sensor network here we are going to elaborate what are the main security elements required in sensor networks and in what scenario:

1. Confidentiality:Confidentiality basically means keeping the data secret from the unauthorized parties. A sensor should not leak sensor readings to the neighboring networks.

   The confidentiality objective is required in sensor environment to protect the information traveling between the sensor nodes of the network or between the sensors and the appropriate equipment may eavesdrop on the communication.By eavedropping ,the attacker could overhear critical information such as sensing data and routing information[7].

2. Authentication :In a sensor network, an adversary can easily inject messages, so the receiver needs to make sure that the data used in decision making process originates from the correct source. As in conventional systems, au-

thentication techniques verify the identity of the participate in a communication,distinguishing in this way legitimate users from the intruders. In the case of sensor network, it is the responsible of each sensor node and base station to verify that the data sent by the trusted sender an d not by the an adversary that tricked legitimate user nodes into accepting false data.

3. Integrity:Data Integrity ensures the receiver that the received data is not altered in transfixt by an adversary. Lack of integrity could result in many problems since the consequences of could result in many problems since the consequence of using inaccurate information could be disastrous as explained in the above table.

4. Freshness:One of the many attacks launched against sensor networks is the message replay attack where an adversary may capture messages exchanged between nodes and replay them later to cause confusion to the network. Data freshness implies that data is recent and it ensures that an attacker has not repayed old message.

5. Availability:Availability ensures that the service and information can be accessed at the time they are required. In sensor networks they are many risks that could results in loss of availability such as sensor node capturing and denial of attacks.

**Survey of security issues in ad-hoc and sensor networks**

In order to determine how to secure a WSN networks one should know the possible attacks in such scenario. Though WSN suffers from a large number security threats most of them can be categorized as Denial of Service attacks[9]. The following table describes the DoS attacks at each layer of OSI model and the defense that can be possible in each of them[8].

**Table 2.2** DoS Attacks in Sensor Networks wrt OSI Network Model[9]

| OSI Layers | Possible DOS attack |
|---|---|
| **Physical Layer Attack** | Jamming<br>Tampering |
| **Link Layer Attack** | Collision<br>Exhaustion<br>Unfairness |
| **Network and Routing Layer Attack** | Neglect and Greed<br>Homming<br>Misdirection<br>Black Holes |
| **Transport Layer Attack** | Flooding<br>Desynchroniztion |

**Physical Layer Attacks:** Nodes in a sensor network use wireless sensor network as for an ad-hoc network this is the most possible and beneficent way of communicating. However base station and other nodes use wired or satellite communication, but limitation on their mobility and energy make them more scarce. According to the above table the following possible attack possible here are :

- Jamming:Jamming is a well known attack in wireless communication, jamming interferes with the radio frequencies a network nodes are using an adversary can disrupt the entire network with k randomly distributed jamming nodes, putting N nodes out of service, where k is much less than N. For single frequency networks, this attack is simple and effective.[10]

- Tampering:An attacker can also tamper with nodes physically and interrogate and compromise them. This happens because one cannot expect to control access to thousands nodes spread over several kilometers. Here an attacker can damage or replace sensor and computation hardware or can extract sensitive materials such as cryptographic keys to gain unrestricted access to higher level of communication.[10]

**LinkLayer Attacks:** The link or media control layer provide channel arbitration for neighbor to neighbor communication. The attacks possible here are:

- Collision:The adversary here only needs to induce a collision to disrupt an entire packet. Any change in data require a checksum at the receiver side. So any corrupted message would then send corrupted ACK control message in some MAC protocols. The energy the attacker needs, beyond that required to listen for transmissions in minute.

- Exhaustion:Such kind of Link layer attack may attempt in retransmission repeatedly even when triggered by an unusably late collision. This repetition of asking of frames results in exhaustion of battery resources in nearby nodes.

- Unfairness:This is a weaker part of DoS attack where the threat may not entirely prevent legitimate access to the channel but it can degrade the service.

**Network and Routing Layer** Network layer security should provide most reliable transmission stream as compared to other higher layer. As a sensor network does not posses a proper infrastructure so all the nodes act as a router for through traffic. Now as most of the sensor node act as router so it is vulnerable to attack through the internet. The possible attacks possible here are:

- *Neglect and greed*:One simple kind of DoS attack the node as router vulnerability by arbitrarily neglecting to route some message, such a node is called neglectful. And a greedy attack occurs when a node gives priority to its own node messages. The main protocol that is effected here is DSR i.e Dynamic source routing. Here as the same route is used for communicating to destination thereby causing traffic to that route, for example, a base station.

- *Homming*:In the homing attacks or eavesdropping the attacker analyze the traffic, learning the presence of critical resources. Once found these node can be attacked by mobile adversaries using other active means. For hiding important information nodes provide confidentiality for both messages headers and their content. The effective way of hiding this information cryptographic key is required for the encryption, this can be discussed in detail in further section.[10]

- *Misdirection*:A more active attack,misdirection.forwards messages along wrong paths,perhaps by fabrication malicious route advertisement. In such kind of DoS attack thee adversary attack the sender thereby targeting the traffic flow in one direction.

- Black Holes:This kind of attack is possible due to the vulnerability in Distance-vector based protocol.Node here advertise zero cost route to al the node forming routing black holes within the network. In order to disrupt the message delivery. This cause intense resource contention around the malicious node as neighbors compete for limited bandwidth. [10]

**Transport layer Attacks**: This layer manages the end to end connections. The service that this layer provides can be simple as an unreliable area-to -area, or as complex and costly as reliable sequenced multicast bytestream.Sensor network tends to use simple protocols to minimize the communication overhead of acknowledgement and retransmissions. Protocol that provide sequencing share many DoS vulnerabilities with the internet transmission control protocol.

- Flooding:Protocol that has to maintain state at either end are vulnerable to memory exhaustion through flooding. As in the classic TCP SYN flood, an

adversary sends many connection establishment request to the victim. Each request causes the victim to allocate resources to maintain state for that connection.[10]

- Desynchronization:An existing connection between two end points can be disrupted by desynchronization. In this attack the adversary repeatedly forges the messages to one or both end points. These messages carry sequence number or control flags that cause the end points to retransmission of missed frames. If the adversary can maintain proper timing,it can prevent the end points from the exchanging any useful information, causing them to waste energy in an end lees synchronization recovery protocol.[10]

**Challenges in Wireless Sensor Networks :**

Wireless sensor network is an emerging technology both in new tier of technology and rich domain of active research involving hardware and system design.[12]. Security is a major requirement because of their area of application. However developing a security design is a major issue as or any things have to be take care before creating any security policy and service. Following are the major constraints in Wireless Sensor Network[12]. In a paper "A Study in Wireless Sensor Networks" by M.J. Camel Mary Belinda and C.Suresh Gnana Dhas :

- Deployment : Sensor nodes may be attached to or carried by mobile entities. Here an attacker can easily do physical attacks of being replaced, affecting node location, density and overall topology.

- Mobility:Sensor node may attached to or carried by mobile entities. Mobility may be either an incidental side effects, or it may be a desired property of the system(e.g to move node to interesting physical locations), in which case

mobility may be either active (i.e automatize) or passive (e.g. attached to a moving object not under the control of a sensor node).

- Infrastructure:The various communication modalities can be used in different ways to construct a communication network. Two common forms are so-called infrastructure based network and ad-hoc networks. In infrastructure networks sensors only communicate with base stations. The number of basestation depends on the communication range and the area covered by the sensor node. In ad hoc network every node can communicate with every other node. Thereby acting as a router forwarding messages to every other hop. Here it make it susceptible to various attacks above discuss like black hole, eavesdropping etc.

- Network Topology:One Important property of WSN is its diameter, that is the maximum number of hops between any two nodes in h e network. Sensor node are very small device so their radio frequency is also very less, thereby for meeting the purpose more sensor device has to be used which increases the overall production cost .

- Connectivity:Sensor nodes and base station uses a wireless medium for their connection and data transmission which is highly prone to eavesdropping i.e attacker analyzing network traffic can easily capture out the sent critical data.

- Lifetime:Sensor nodes posses very low battery period that ranges to very few hours.So any security policy implemented should take care off energy consumption that results to minimizing of energy expenditure.

- Storage Capability:Sensor nodes are very small device and its memory range is very few MB. Thereby if any security policy designed the code size should be taken into consideration and it should be minimum as it can be. All the

above constraint of sensor networks make it easy to be captured by intrusion,interception, modification and fabrication and traditional security techniques[12].

**Counter Measure to Homing or Eavesdropping**

In the above section we have discussed number of attacks possible in a WSN scenario. Now let us focus our scope to the major one i.e. Eavesdropping and identify its countermeasure. Sensor network mainly operate in public and uncontrolled areas over inherently insecure wireless channels. It is therefore a very easy for an attacker to eavesdrop and can easily inject a packet. The traditional solution to this problem has been espouse techniques such as message and authentication codes, symmetric keys, encryption keys and cryptography. However the motes are constraints in terms of memory, power and other resources so these techniques has to be applied in an efficient way without sacrificing their strength[14].

**Background**

In this section, work done by different researchers has been discussed in detail along with solutions given by them. So as to reach out a particular decision which algorithm or mechanism is optimum, so as to implement the effective security policy for the same.

Cryptography is considered as a science of hiding information.[16] More specifically according to Pyrgelis Apostologos " Cryptography is the study of mathematical techniques related to aspects information security such as confidentiality, data integrity, entity authentication and data origin authentication".[15]. Initially Cryptography was considered to be solely consist of two main method

Encryption and Decryption. Conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely the key needed for decryption of that message). Encryption was used to (attempt to) ensure secrecy in communications, such as those of spies, military leaders, and diplomats whereas decryption is the reverse process[16].

However in In recent decades, the field has expanded beyond confidentiality concerns to include techniques for message integrity checking, sender/receiver identity authentication, digital signatures, interactive proofs and secure computation, among others. Throughout history, however, there has been one central problem limiting widespread use of cryptography. That problem is key management. In cryptographic systems, the term key refers to a numerical value used by an algorithmic alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information. Consequently, the term key management refers to the secure administration of keys to provide them to everywhere and when they are required[17]. Depending upon the key the cryptographic Technique has been classifies in two forms i.e.Private key Cryptography and Public Key Cryptography.



**Public key Cryptography**

In Symmetric key cryptography both sender and receiver shares posses same key. The main drawback of this cryptographic technique is the way of sharing key between two parties which if done over a non-secure medium can easily be compromised. The authors of [18] and [19] has discussed various approaches of distributing key secretely. Though Kerberoes is very popular protocol for

secret key distribution but when internet and wireless networks are concerned lack a secure channel to secret keys. In 1976, Diffie and Hellman [20] proposed a new type cryptography known as asymmetric or public key cryptography. Public key cryptography uses two keys instead of one, one of these keys is used by sender known as *public key* and the another one is used by receiver of the message decryption, called as *private key*. Public key cryptography is considered to be more secure as the mathematical function used is based upon factorization of the product of large prime numbers, which is very difficult. Therefore most of the public key cryptosystem base their security on the difficulty of solving mathematical problem,finite field discrete logarithm problem and the elliptic curve discrete algorithm.[21]. The another important aspect of public key cryptography is that give a solution for key management and distribution over insecure channel and the two communicating parties need not require to exchange their keys in advance before initiating the communication, such a solution is Deffie-Hellman key-exchange protocol.

**Comparison of RSA and ECC**

A public key cryptosystem is considered to be more secure as here public key is used for communication per discussion in above section of literature survey. There are number of algorithm that has been discussed in this concern like RSA and ECC.One that is adopted in WSN scenario depends upon the consumption of resources like memory, battery, power resources etc. Apart from mathematical part let us discuss how ECC is better than the RSA. RSA algorithm is based upon factorizing method where main principle is to choose big number as a key i.e hard to factorize whereas ECC, as already mentioned above,based upon elliptic curve discrete logarithmic problem of finite field,that

take millions of years to break it.Following graph Fig 2.3 shows a comparison with the key size generated with two algorithm and the time to break each of them.

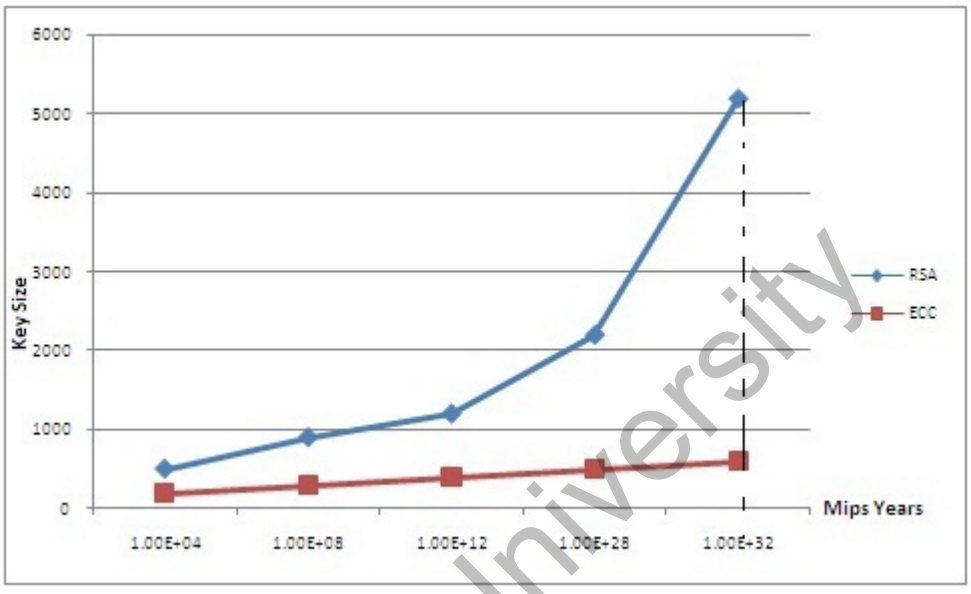


**Figure 2.3** Comparison of Security level ECC vs RSA[5]

With the above graph we conclude that ECC with small size provide equal security level and comparatively take hard to break which is a positive side of ECC algorithm when implemented in WSN scenario. The another aspects where we can compare the two algorithm is in the terms of time and power consumption for performing verification,signature generation and key exchanged operation.This can be shown by the help of following two table: Here the results are shown corresponding to two key size RSA-1024,2048 and ECC-160,224.

From the above results we conclude that *ECC is an optimum algorithm that we can implement in WSN scenario.*

**Table 2.3** Time Consumption vs Algorithm and Key Size[5]

| Algorithm | Key Size (bit) | Key Exchange | | Signature | |
|---|---|---|---|---|---|
| | | Client (s) | Server(s) | Sign(s) | Verify(s) |
| RSA | 1024 | 1.12 | 22.03 | 22.03 | 0.86 |
| | 2048 | 4.14 | 166.85 | 166.85 | 3.89 |
| ECC | 160 | 1.62 | 1.62 | 1.65 | 3.27 |
| | 224 | 4.38 | 4.38 | 4.46 | 8.84 |

**Table 2.4** The estimated Power Consumption in WSN[5]

| Algorithm | Key Size (bit) | Key Exchange | | Signature | |
|---|---|---|---|---|---|
| | | Client (s) | Server(s) | Sign(s) | Verify(s) |
| RSA | 1024 | 39.96 | 726.99 | 726.99 | 28.38 |
| | 2048 | 136.62 | 5506.05 | 5506.05 | 128.37 |
| ECC | 160 | 53.46 | 53.46 | 54.45 | 107.91 |
| | 224 | 144.54 | 144.54 | 147.18 | 291.72 |

In the next section we are going to discuss basic principle of ECC, mathematical operations and all operations required for for encrypting data.

**Deffie-Helman Key Exchange:**

Deffie-Helman key exchange protocol uses a set of multiplicative set of integer module p, $< Z_{p*}, x >$ where p is a large prime number of the order 300 decimal digits(1024 bits). This group is represented by $G =< Z_{p*}, x >$. The basic Deffi-Hellman Protocol applied when Alice and Bob are communicating with each other can be described in the following way:

1. Alice and Bob both agree on a cyclic group G, its generator g and a prime p.
2. Alice and Bob each secretely chooses a random number a and b such that $0 < a,b < p - 1$.
3. Alice calculates $R_a$=$g_a$ mod p while Bob calculates $R_b = g_b$ mod p.

4. Alice sends Ra to Bob and Bob sends $R_b$ to Alice.
5. Alice calculates $K = (R_b)$ a mod p while $o_b$ calculates $K = (R_a)_b$ mod p.
6. Both get the same value for key. here gEG such that ¡g¿=[21]

*Security in Deffie-Hellman:* The security of Deffie-Hellman algorithm key-exchange protocol is that it relies on the presumed hardness of the Discrete logarithm problem(DLP) in group of large order, i.e computing the Deffie-Hellman secret key is considered computationally impossible given the public parameters. At the end of the protocol, the values $g_a$ and $g_b$ have become public while the value $o_g$ $g_{ab}$ remains private. Thus the Diffie-Hellman Problem(DHP) is to compute gab from $g_a$ and $g_b$. This is widely believed to be difficulty as long as the discrete logarithm problem has not been solved in G[18].

The major shortcoming of Deffie Hellman Protocol is the *Man-in-the-Middle* attack. In this kind of attack an eaves-dropper intercepts all message between Alice and Bob and makes independent connection with them. Here eavesdropper can then replay the message to Alice and Bob, making them believe that they are talking directly to each other over a private network connection when in fact the entire communication is controlled by eavesdropper. To provide security from such kind of attack Deffie Hellman adds new flavor of authentications form of digital signature with public key certificates to establish a secure session between Alice and Bob.

A more recent method used in public key cryptography to generate key is to use elliptic curve and is describe in next section.

**Elliptic curve Cryptography**

Elliptical curve Cryptography (ECC) is ana approach to public key cryptogra-

phy based on the algebraic structure of elliptic curves over finite fields.In 1985, Neap Koblitz[14] independently proposed the use of elliptic curve in cryptography. ECC is emerging as an attractive public key cryptosystem for wireless networks. It provide an alternative to established public-key system such as the DSA(Digital Signature Algorithm and RSA (Rivest-Shamir- Adleman) algorithms. Though these algorithm also provide a better solution when used in wireless networks ECC (Elliptical Curve Cryptography) provides the optimum and efficient solution for the key management and the distribution purpose as far as resource consumption is concerned this has been discussed in [21].

**Mathematical Foundation of ECC:**

Much of the following discussions in this section is based on the material presented in Lawrence C.Washington's book "Elliptic Curves, Number Theory and Cryptography" and "Elliptic Curve Cryptography an Implementation Guide.

The mathematical operations of ECC are defined over a special class of elliptic curve of the form:

$$y^2 = x^3 + Ax + Bmodp - - - - - -(2.1) \tag{2.1}$$

where $A, BZ_p$ are constants satisfying the condition $4A^3 + 27B^2 \neq 0modp$. This condition ensures that the equation(2.1) has no repeated roots(non singular). The modulo p is a prime with $p \geq 3$. The theory can be adopted to deals only with the field of characteristics not equal to 2 or 3.

Let $E_p(A, B)$ denotes the set of points $(x, y)$ that satisfy equation(2.1), i.e. $E_p(A, B) = (x, y)|(x, y)\epsilon Z_p$ and $y^2 = x^3 + Ax + Bmodp$. We define the set

$E(Z_p) as follows$ :

$E(Z_p) = E_p(A, B) \cup \{O\}$

The elements of the $E(Z_p)$ are called the points on the elliptic curve E defined by equation(2.1) together with an extra point O which is called the point of infinity. The specific properties of a nonsingular elliptic curve allows us to define a binary operation, called ädditions" (denoted by +?), on the points of $E(Z_p)$.The operation is the addition of two points on the curve to get another point on the curve.

$R = P + Q$ where $P = (x_1, y_1), Q = (x_2, y_2), R = (x_3, y_3)$.

The point O is defined as an (additive) identity i.e. for all

$P \epsilon E() Z_p, P + O = O + P = P$.

It can be shown that every line intersecting the curve E intersects the curve in exactly three points, where:

1. a point P is counted twice if the line is tangent to the curve at $\boldsymbol{P}$, and
2. the point at infinity is also counted (when the line is vertical).

**ECC Arithmetic**:

The rules for negation, addition and point doubling are described below. However, to conceptualize the basic arithmetic behind $E(Z_p)$ we will first give a graphical explanation of elliptic curve over the reals i.e. the equation $y^2 = x^3 + Ax + Bmodp$ without reduction modulo p.This is because; in modular arithmetic the points on the curve do not make nice graphs. Nevertheless, the concept remains the same.

**Negation**

A negative of a point is the reflection of that point with respect to x-axis. Given a point P, in negation is the point for which $P + (-P) = O$. The line connecting two points intersects the curve O .We can think of the "point of Infinity" O as sitting at the top of the y-axis and lying on every vertical line. As shown in Fig2.4(b), -P is simply the reflection of P in the x-axis, that is if $P = (x_1, y_1)$ then $-P = (x_1, -y_1)$.

**Point Addition**:

For an elliptic curve E, take two arbitrary points $P, Q \neq O$. Point addition in the process of adding these points to obtain another point R on the same elliptic curve. If $Q \neq -P$, as in Figure2.4(a), then the line drawn through the point p and Q will intersect the elliptic curve at exactly one or more points, $-R$. If $P = Q$, the draw the line tangent to E at P(see point doubling). Graphically, $P + Q$ can be found by reflecting the point $-R$ with respect to x-axis. In $E(Z_p)$ we use the same addition operation but the calculation are

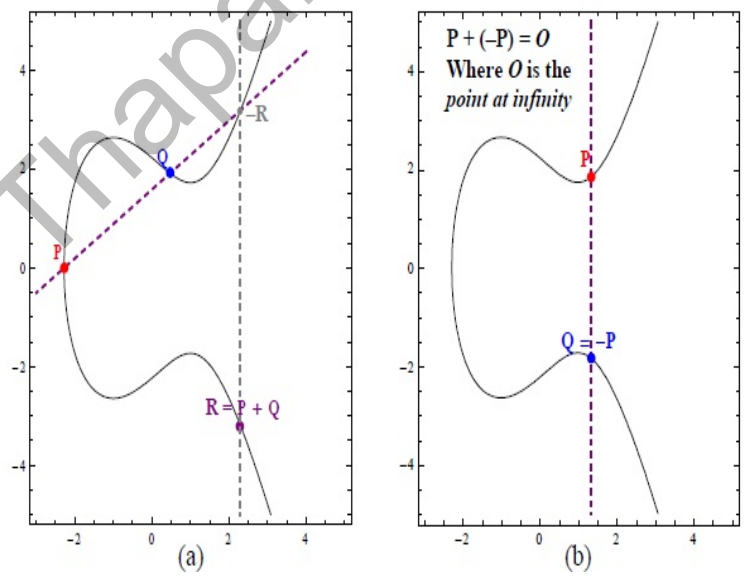


**Figure 2.4** Point addition in Elliptical Curve Algorithm[14]

done modulo p. So let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points in $E(Z_p)$ with $P, Q \neq O$.we first consider the case P and Q have different x and y co-ordinates ($x_1 \neq x_2$ and $y_1 \neq y$ . Then the coordinates of the point $R$,$x_3$ and $y_3$ can be found by first finding the slope of the line m, through P and Q and then calculating the values of $x_3$ and $y_3$ as shown below:

$m = \frac{y_2 - y_1}{x_2 - x_1} mod p$

$x_3 = m^2 - x_1 - x_2 mod p \; y_3 = m(x_1 - x_3) - y_1 mod p$

Our assumption, that $x_1 \neq x_2$ means that $x_1 - x_2 \neq 0 mod p$. This implies that the inverse of $x_2 - x_1$ modulo p exists. However, if $Q = -P\,(x_1 = x_2 and y_1 = -y_2)$, as shown in Figure2.4(b), then two points are additive inverse of each other.

**Point Doubling**

For an elliptic curve E, take an arbitrary point $P \neq O$. Point doubling is the process of adding the point P to itself to obtain another point R on the same elliptic curve. If the y-coordinate of the point P is not zero as in Figure2.5(a), then the tangent line drawn at P will intersect the elliptic curve at exactly one point, -R. Graphically, 2P can be found by reflecting the pint $-R$ with respect to x-axis.

Consider a point $P = (x_1, y_1)$ be in $E(Z_p)$ with $P - neq O$. We first consider the case where y-cordinate of P is not zero $y_1 - neq 0$. In this case, the slope of the line and the coordinates of the point R, $x_3$ and $y_3$ can be found as shown below:

$m = m = \frac{3x_1 - A}{2y_1 mod p}$

$x_3 = m^2 - 2x_1 mod p$

$y_3 = m(x_1 - x_3) - y_1 mod p$

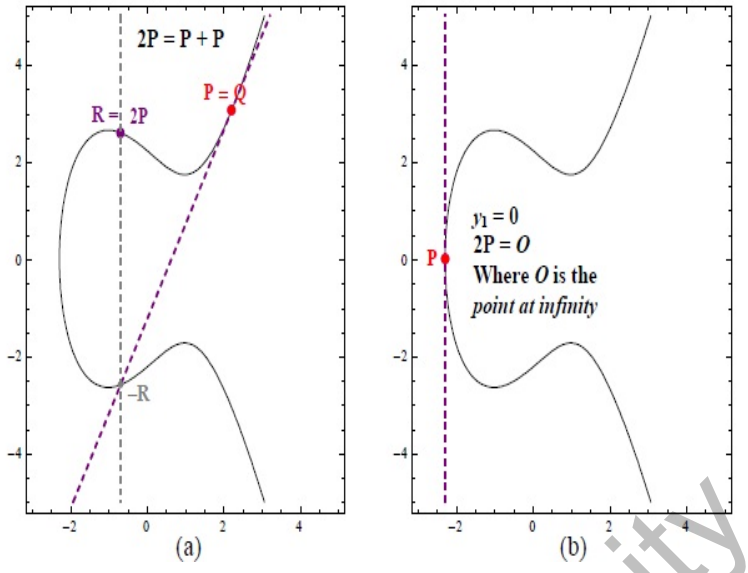


**Figure 2.5** Point Doubling operation in ECC[14]

if the y-cordinate of the point P is zero as shown in Fig2.5(b), then the tangent at this point intersects the curve at O, So $2P = O$.

*Properties of Elliptical curve*

It is shown in [23],[22] that the sets of point $E(Z_p)$ along with the addition rule defined above form an albelian group:

- Closure:Adding two points on the curve creates another point on the curve.
- Associatively:$(P + Q) + R = P + (Q + R)$.
- Commutatively:$P + Q = Q + P$.
- Identity:The p̈oint at infinity" O is additive identity. In other words $P = P + O = O + P$

Scaler Point Multiplication:

Scaler point multiplication is the core of elliptic curve aruthmetic.It is the most essential part of secure elliptic curve cryptosystem.For an elliptic curve E,take

an arbitary point $P - neqO$.Scaler multiplication is the process of adding the point P to itself k times to another point Q on the same elliptic curve.

$Q = kP = P + P + .....P$ here $P + P..... + P = k$

Where $k < |EZ_p|$ is a scaler. Scaler multiplication of a point on E can be performed througha combination of point addition and point doubling e.g $11P = 2\,(((2P)) + P) + P$.

The above mentioned is called the ¨double and add" algorithm for scaler point multiplication.

**Elliptical Curve Discrete Logarithm Problem**

Much of today's ECC is based on the elliptic curve discrete logarithmic problem (ECDLP). Recall from the last section that the scaler multiplication is the core of elliptic curve arithmetic. When the elliptic curve group is described using additive notation, the elliptic curve discrete logarithmic problem is defined as follows:

*"Given the point kP and Q in the group, find the value of k such that $kP = Q$"*

The problem is considered computationally difficult unless the curve is "weak". Several classes of curve are weak and must be avoided e.g if $|EZ_p| = p$, then the curve is vulnerable.

**ECC Domain Parameters**

To use ECC all parties involved in the communication must agree on all the elements defines the elliptic curve E i.e domain parameters for the elliptic curve $EZ_p$ are p,A,B,G,n and h.Following is a brief description of each:

- p is a prime such that $p > 3$.

- A and B are the parameters defining the elliptical curve equation.
- G is a called the base point or the *generator* point. Each curve has a specially designed point,G, choosen such that a large function of elliptic curve points are multiplies of it. We call ¡G¿ the cyclic subgroup generated by G.Scaler point multiplication can be used for finding the multiplies of G. The scaler for point multiplications chosen such that it is a number between 0 and $n-1$.
- n is the order of G, i.e the smallest non-negative integer n such that $nG = O$.
- h is called the *cofactor* where $h = \frac{|EZ_p}{n}$. Since n is the size of the cyclic subgroup generated by G, it follows from Langrange's theorem that the order of the subgroup must divide the order of the group. So h is an integer. For cryptography application h must be small ($h \leq 4$).

In this chapter the various solutions for securing communication WSN has been discussed and compared to conclude which one is best and optimum. In the next chapter actual problem and objectives of the thesis are listed that confines its scope .

# Chapter 3

# Problem Statement

Sending data over wireless network has always been criticized for security concerns. Over the years many efforts have been put to secure wireless data channels, some successful implementations had also been devised. We wish to further this design and development process to explore use of ECC for Sun Spot WSN devices.

**Objectives:** Following are the objectives that are aimed to be achieved during the entire thesis:

- To study and explore various algorithms for secure data transmission over WSNs.
- Design and Develop ECC for WSN devices.
- Demonstrate the use using Sun Spot WSN device.

# Chapter 4

# Implementation Details and Results



From the previous chapters it can be concluded that Elliptic curve DiffieHellman based upon ECC discrete algorithmic problem is the most optimum security policy that can be implemented in a wireless sensor network to have a secure communication. In this chapter ECDH protocol is implemented over JAVA platform by simulating a wireless sensor network using JAVA SunSpot kit that consist of Sun motes acting as sensor device and Base Station. Here the benefits and the problem faced while implementing the entire scenario is also discussed.

## 4.1 Brief Introduction to Java SunSpot Platform

As discussed above Java SunSpot kit, is basically used here for simulating a wireless sensor network. The kit has two sensors and a basestation as shown

in Figure 4.1.


**Figure 4.1** JAVA SunSpot Kit

### 4.1.1 SunSpot Motes

Sun Spot(Sun Programmable Object Technology is a wireless sensor network(WSN) mote developed by Sun Microsystem. The device is built upon the IEEE 802.15.4 standard the IEEE 802.14 standard.Unlike other available mote systems, the Sun Spot is built on Squawk Java Virtual Machine.[25]

Figure 4.2 demonstrates the external Figure 4.2(a) and internal view Figure 4.2(b) of SunSpot devices showing the major parts of SunSpot kit.



**Internal Structure of SunSpots**

As has been shown in Figure 4.1(a), SunSpot device major hardware part has been discussed below:

- **Sun roof**:This is the shielding part of main circuit of the device which can be opened and close by pressing a cork on its body[25].

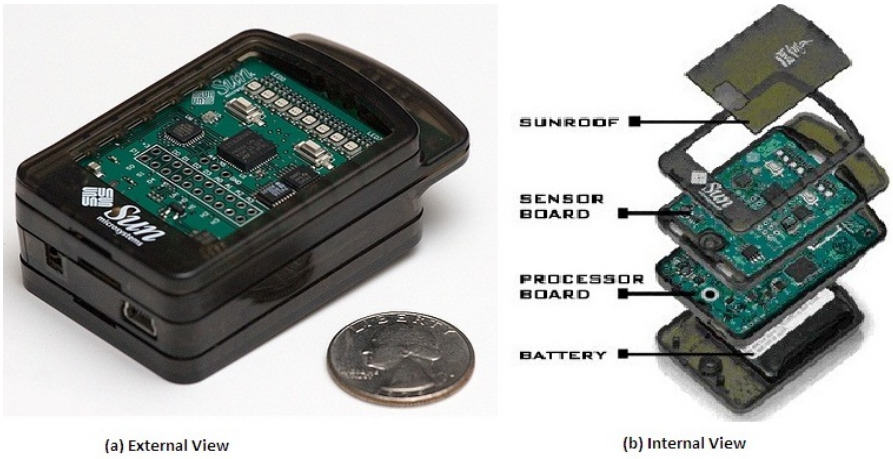


**Figure 4.2** External and Internal view of SunSpot devices

- **Processor:** Processor of SunSpot consist of 180Mhz 32 bit ARM920T core with 512 RAM.ALong with IEEE 802.15.4 radio with integrated antenna for over the air communication and an USB interface which can be connected to external devices[25].
- **Sensor Board**:The sensor board is the major part of the device that comprise of Light sensors with 8 tri-color LED's.Analaog Inputs, 2 momentary switches and 5 general purpose I/o pins and 4 high current putput device[25].
- **Battery**:Sun Spots devices are provided with 3.7v rechargeable mAh lithium-ion battery. This can be charged by connecting it with external devices[25].

### 4.1.2 SunSPOT Base Station

In wireless communication, Base Station is basically a device that is connected to a fixed location and facilitates the wireless device to communicate over the air with the help of radio antenna associated with it. In simulating

environment The purpose of the Sun SPOT basestation software is to allow applications running on the Host to interact with applications running on Targets. The physical arrangement is shown in Figure 4.3.


**Figure 4.3** Physical arrangement of Basestation with SunSpot devices[26]

The Host can be any of the supported platforms (e.g. Windows PC, Mac). The Host application is a J2SE program. The Target application is a Squawk Java program. Basestation access a SunSpot device remotely by using IEEE address assigned to it. Further explanation of the devices using various commands will be explained in actual experiment.

### 4.1.3 Managing SunSpots

The Sun SPOT SDK comes with two important tools for managing the software on SPOTs: SPOTManager and Solarium.

Spot Manager can be installed directly from the internet[27]. The installation steps of the software is beyond the scope of this report. However a brief functioning of the software has been given in the following sections.

### 4.1.4 Pre-Requisite Softwares for Spot Manager

Installing Spot Manager is not an easy task as it requires number of software to be installed already on your computer. But the best part is that the setup asks and provides the required one if any of them is not installed. Here it is

assumed that the installation procedure is supported by internet connection. Following is the list of the pre-requisite softwares:

- **Sun Development Kit** :SDK or Sun Development kit consist of all the packages and classes requires for running and deploying application on SunSpot.
- **Java Netbeans**:Java Neatens provide GUI for developing SUNSpot application come along with the SDK SUNSpot modules.
- **Ant server:**Apache Ant server provide various xml files required for deploying, accessing info, running application etc.

### 4.1.5 Spot Manager GUI

After installing GUI following steps given in [28] and with internet connection the Sun Spot manager GUI is shown in Figure 4.4 To be very brief following task can be performed using SunSpot manager :

- **SunSpot Management:**SunSpot spot management can be done using various options like Spot info, Spot properties, enabling and disabling OTA commands available on GUI as shown in Figure 4.4.
- **Solarium:**Solarium provides a simulator, where one can deploy application on virtual sunspot and see how it is working before deploying to actual SunSpots, basically helps in overcoming error before actual deployment.
- **Learing SDK:**Various demo application and documents are provided where novice can learn, actual functioning of SunSpot devices before starting developing the applications.


**Figure 4.4** SunSpot Manager GUI for managing SunSpots[26]

## 4.2 Experiment Details

In this section we are discussing the experimental architecture, results, problem faced during experiment and the benefits of doing the experiment.

### 4.2.1 Elliptic Curve Diffie-Hellman

As has already been discussed in the previous chapters that ECDH is the most optimum security protocol that can be applied in the wireless sensor network algorithm so here major algorithm that has been implemented has been discussed. **Elliptic curve Diffie-Hellman(ECDH)**

The Elliptic Curve Deffi-Hellman key-agreement protocol is variant of the

Diffie-Hellman protocol using elliptic curve cryptography. It allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure communication channel. Suppose Alice want to establish a secret key with Bob. The following interchange between Alice and Bob demonstrates the Elliptic curve Diffie-Hellman key-exchange protocol.

1. Alice and Bob publicly agree on an elliptic curve $|EZ_p$and all the domain parameters, i.e$(p, A, B, G, n, h)$.
2. Alice and Bob each secretely choose random integers, a and b,such that $0 < a$,$b < n$.
3. Using elliptic curve scaler point multiplication, Alice calculates $G_A = aG$ while Bob calculates $G_B = bG$ on E.
4. Alice sends $G_A$ to Bob and Bob sends $G_B$ to Alice.
5. Alice calculates $aG_B = abG$ while Bob calculates $bG_A = baG$.
6. Both get the same value for the key.
7. Alice and Bob use some publicly agreed on method to extract a secret key from abG. For example they could use the x-coordinate of this point as the secret key.

The ECDH protocol is secure because no one can derive the private key of the other unless one can solve the Elliptic Curve Discrete Curve Logarithmic Problem.

### 4.2.2 Experiment Setup and explanation

The entire implementation is been performed using Java Sun Spot kit and the software installed as explained above.The algorithm illustrated above is implemented to secure data in a wireless media in the following way:

#### Experiment Architecture

The experiment consist of two sensor device and a base station. The devices here are communicate each other over wireless media and the base station is connected to a host as shown in Figure 4.5. According to the figure given

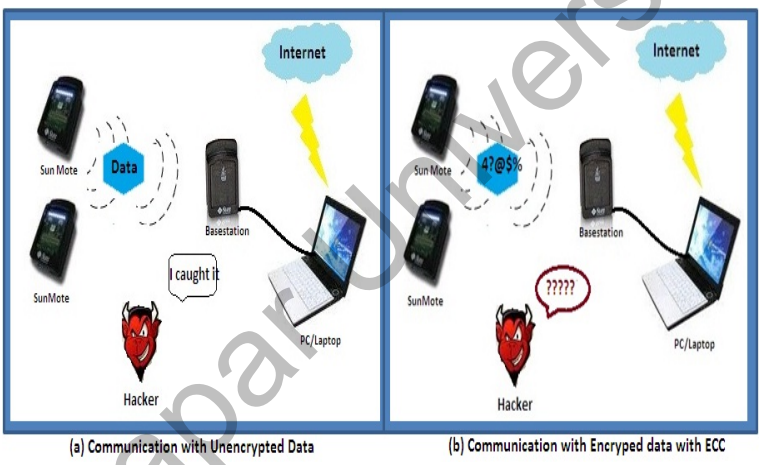


**Figure 4.5** Architecture of Experiment



above initially when data is exchanged between the two sensors, hacker can easily compromise it because of inherit nature of wireless media. Then, the data is encrypted using ECC algorithm which became quite hard for hacker to crack.

The major steps that are performed in the whole experiment are:

1. Deploying Bounce Demo application on SunSpot devices for making them

communicate with each other.

2. Capturing the packets exchanged between two devices using Packet Sniffer and Sniffer Client application on Base station.
3. Browsing the packets sniffed using Wireshark-Network Analyzer tool and identify the data exchanged.
4. Deploying the another secure version of Bounce Demo on spot with ECC based secure library suite.
5. Repeating step 2 and 3. This time data exchanged between them will be encrypted.

### 4.2.3 Implementation

The entire implementation is conducted by following the steps given below. The major softwares used here is Apcahe ant, SDK and NetBeans:

### 4.2.4 Analyzing Unencrypted Communication

**Accessing SpotInfo:**

Connect the SunSpot device to the system for accessing its information this can be done by using *ant info* command in the root directory where SDK is installed as shown in Figure 4.6: From the Figure 5.6 it can be analyzed that two SunSpot devices are there having the IEEE address as *0014.4F01.0000.181D* and *0014.4F01.0000.0E14*. These address are basically used for accessing he spot remotely. And as here cryptographic mechanism is of major concern, so it can be identified that no keys are previously installed on device.

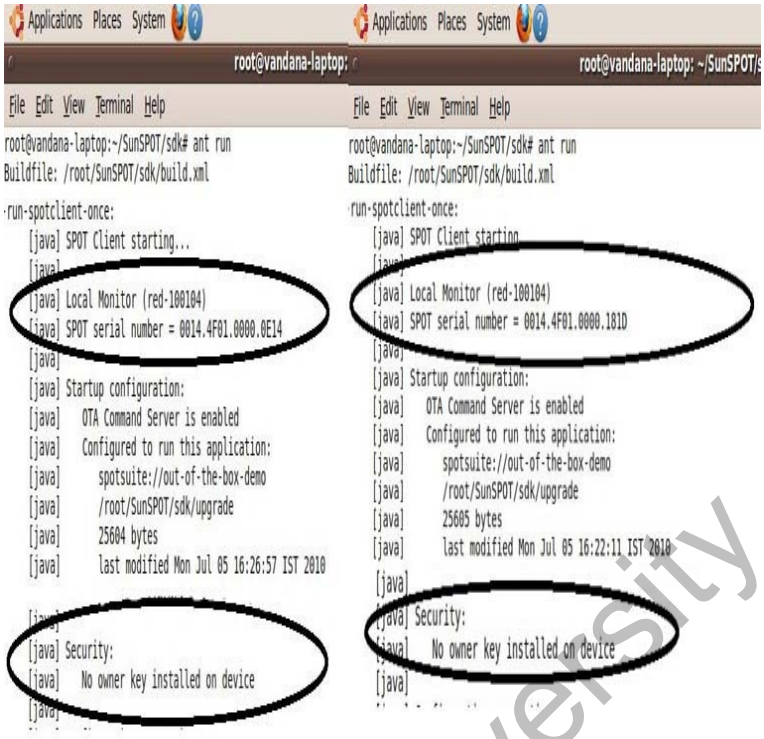


**Figure 4.6** Initial information of a SunSpot devices.



### Deploying BounceDemo Application

As the process of deploying any application on a Spot device is same let us consider it on the device having address *0014.4F01.0000.0E14*.

- For running any application on SunSpot device proper library suite is to provide that assist devices to perform their function.This can be done using *ant flashlibrary* command. The outcome of this command when successfully build is shown in Figure 4.7.
- Here BounceDemo-onSpot application is deployed over the device using ant-deploy as shown in Figure.4.8 This application basically bounces the light ball over two devices making them communicate with each other.
- Finally the application can be made to run on the devices using *ant*

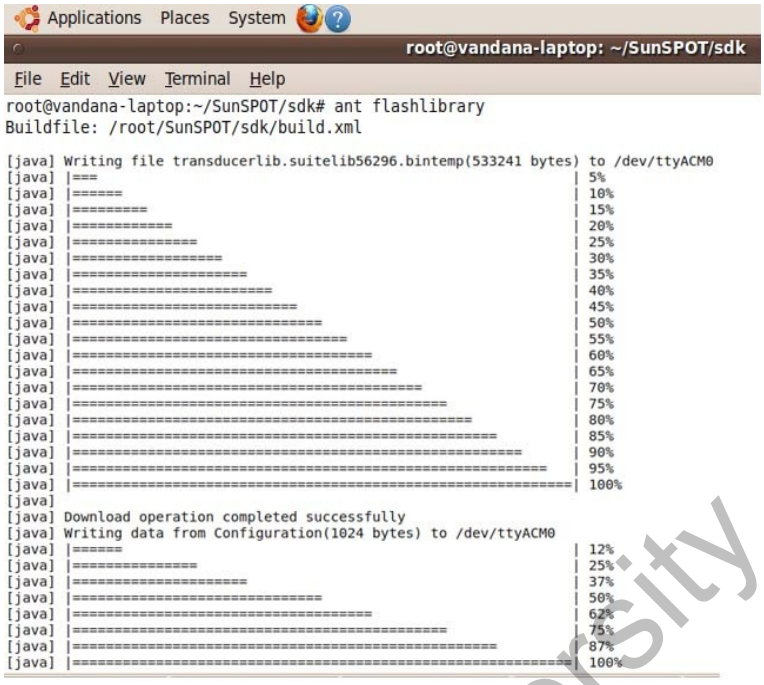


**Figure 4.7** Output of *ant flashlibrary* flash the library command.

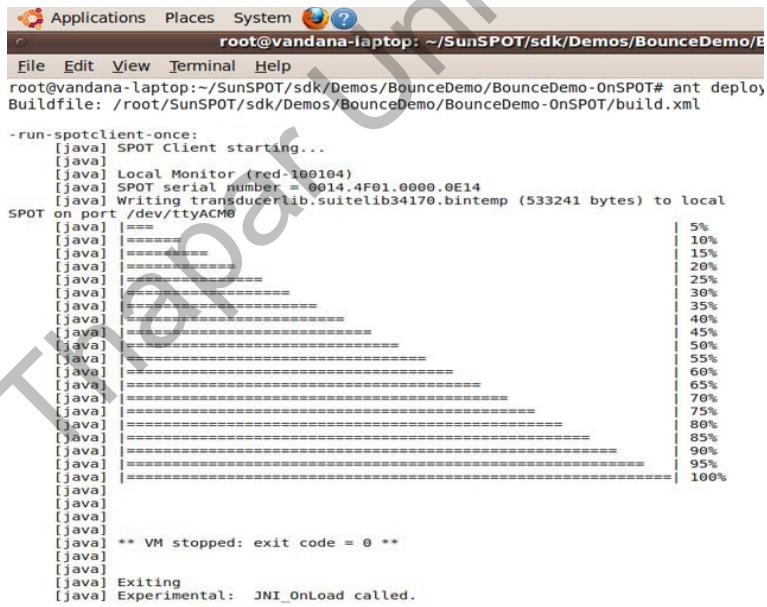


**Figure 4.8** Output of *ant deploy* command on SunSpot.

*run*command and the outcome is shown in the Figure 4.9

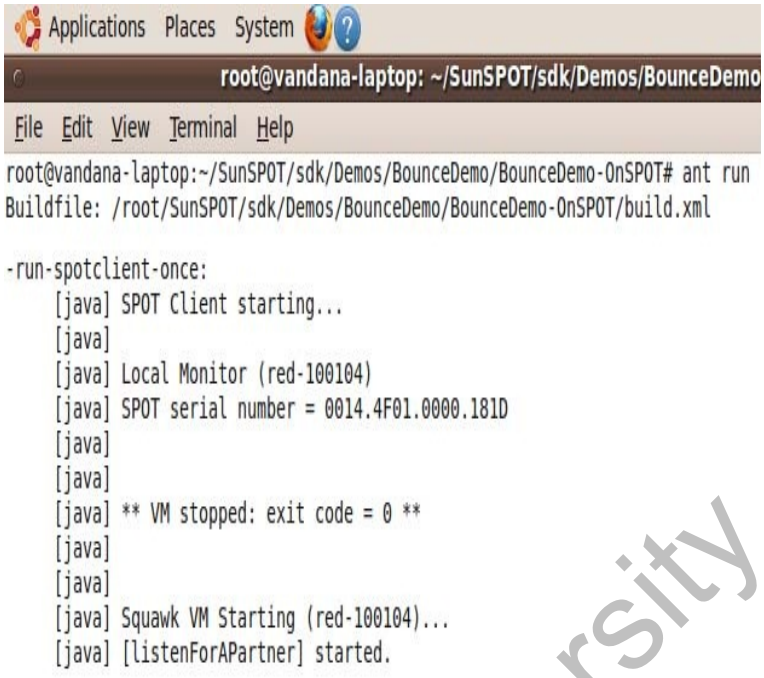


**Figure 4.9** Output of *ant run* command.



**Running Base Station for Capturing Packets**

Now for running Packet Sniffer and Sniffer client on BaseStation. It is required to disable Over-the-Air (OTA) and mesh routing over it. This is performed in the following way:

- **Accessing BaseStation Info:**BaseStation information can be accessed similarly as that of SunSpot using *ant info*.The initial info is as shown in Figure 4.10.

- **Disabling OTA and Mesh routing:**Now for disabling routing and OTA we have to issue ant disableota as shown in Figure 4.11.

- **Starting as a BaseStation**:A BaseStation can also be used as a Spot device. However to specifically start it as a basestation, ant **startbasestation** command required to be issued. This can be done in the following way:

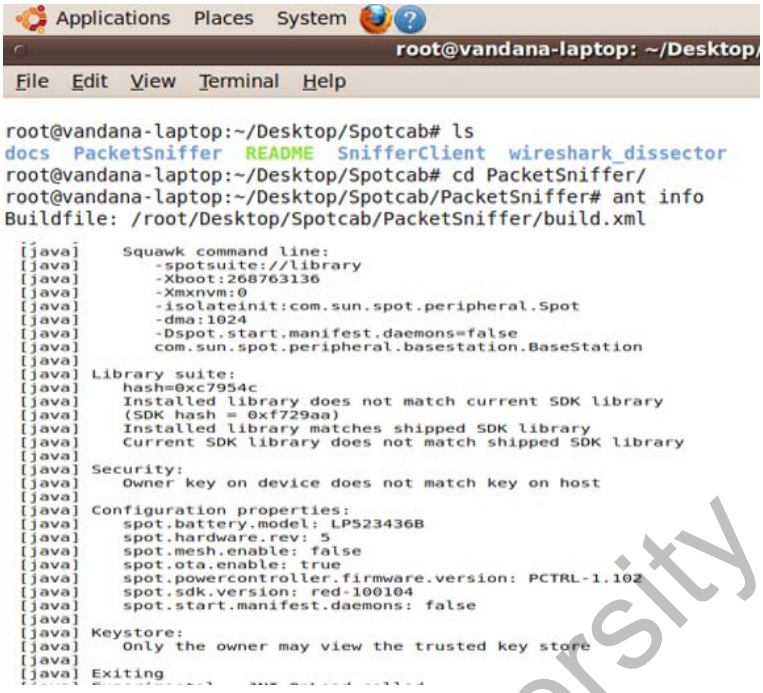


**Figure 4.10** Output of ant info command for basestation.

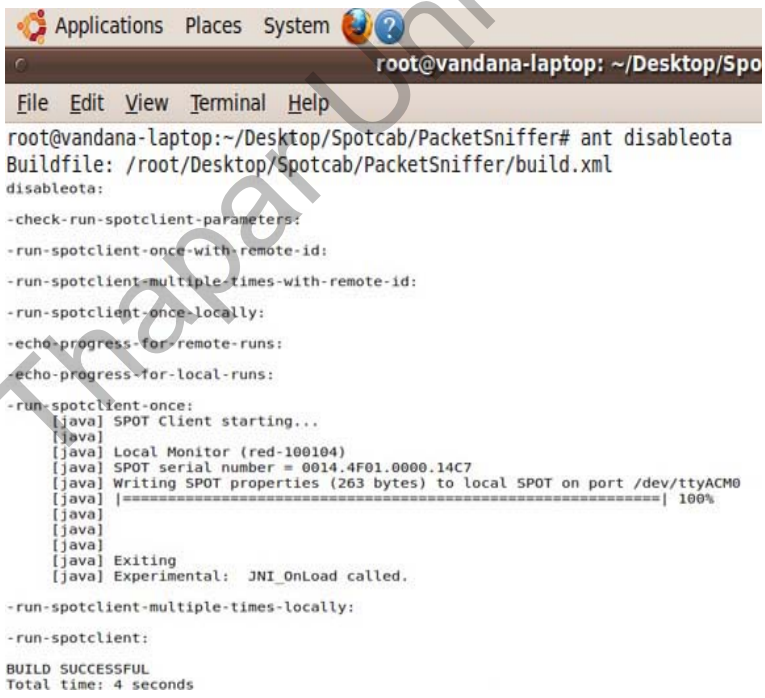


**Figure 4.11** Output of *ant disableota* command.

### Sniffing packets using BaseStation

After getting basestation prepared, Packet Snifffer application is to be deployed and then running the sniffer client in the following way:

### Browsing and Analyzing Sniffed Packets

After running the sniffer client, all the captured packet are stored in "sniffer.dump" file in the same folder of application. This file can be opened using wireshark as shown in the following Figure.4.12

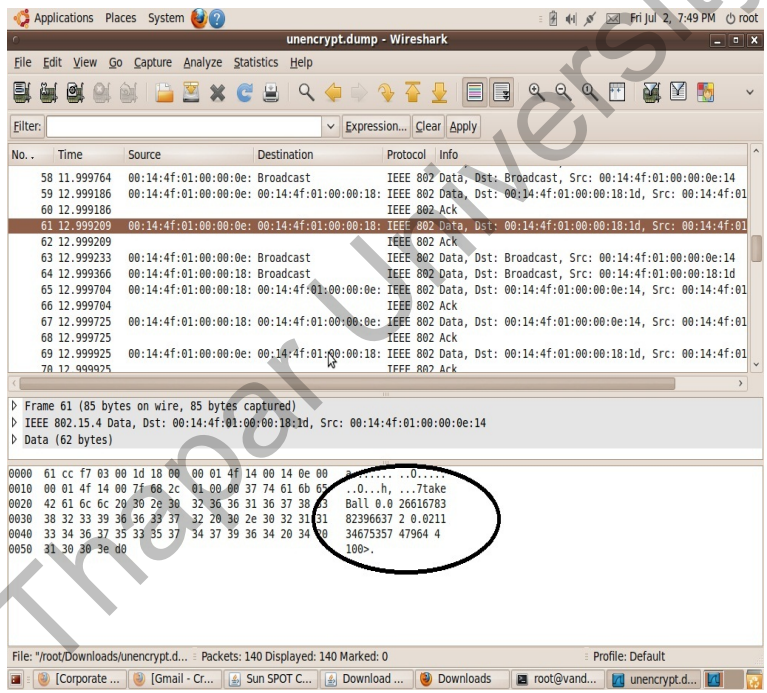


**Figure 4.12** Wireshark output showing unencrypted data

### 4.2.5 Analyzing Encrypted Communication

Until now the spot devices are made to communicate and data is captured which is quite unsecured. Now data will be crypted using ECC algorithm and then analyzed.The steps are been taken from readm.txt file in SSL folder given on the webpage[28]. The entire encryption steps are described in the following section:

1. **Deleteing Existing Public key** Before generating any key or secure communication, the device has to bring in the keyless state. This can be done using ant deletepublickey command as shown in Figure 4.13. As can be seen

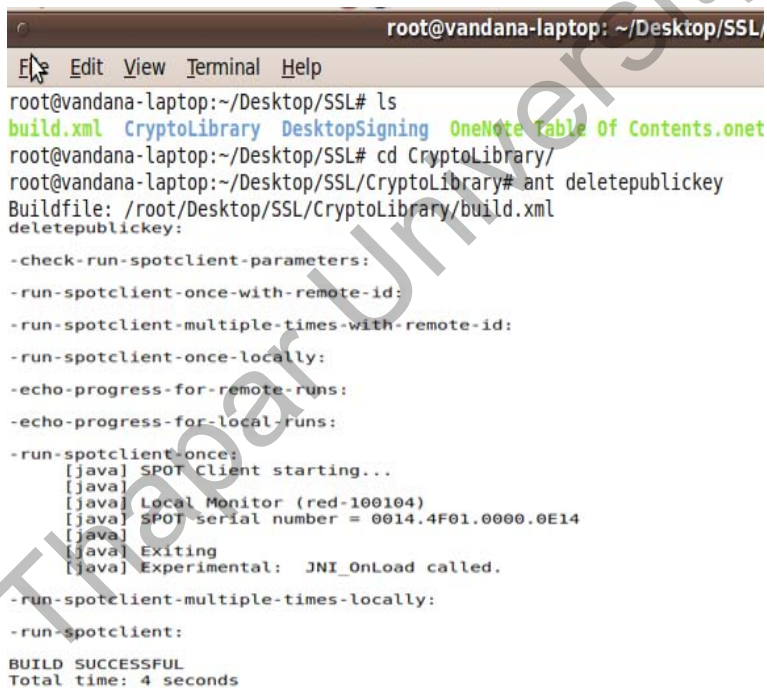


**Figure 4.13** Output of ant publickey command for basestation

in the Figure 4.13 the keystore became empty after executing the command.

2. **Editing sun property file and creating suitable library**: Now to create a new library certain changes has to be made in *.sun.properties* file stored in

user account when the SDK is installed properly.This entire changes has been given in the Figure 4.14. In Figure 4.15 it can be seen that a new library "cryp-

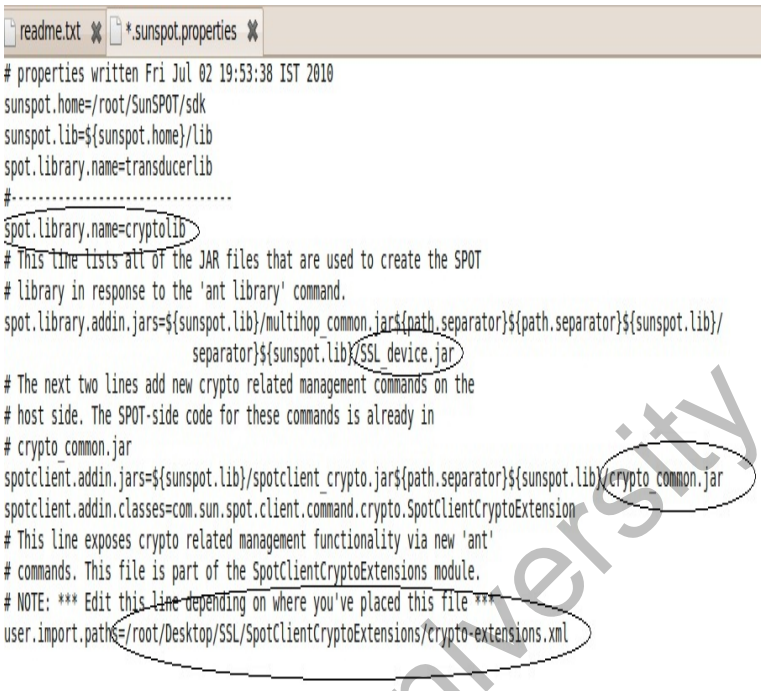


**Figure 4.14** Output of ant info command for basestation.

tolib" is to be created which contain three jar file $SSL.jar$, $crypto_common.jar$ and a host jar file $SpotCryptoClient.xml$.

Similarly the creation of $SSL.jar$ and host jar can be shown in Figure 4.16. and 4.17

Finally a new library is created by issuing ant library command as in Figure 4.18 And then flashing this library on the Sun Spot as in Figure 4.19 With the creation of new library the ant server will support new list of commands for manipulating like listtrustedkeys, addtrustedkey, deletetrustedkeys and others. However here for making the two device trust each other, a key would be added in both the device as shown in Figure 4.20 Now to list out new set of keys can

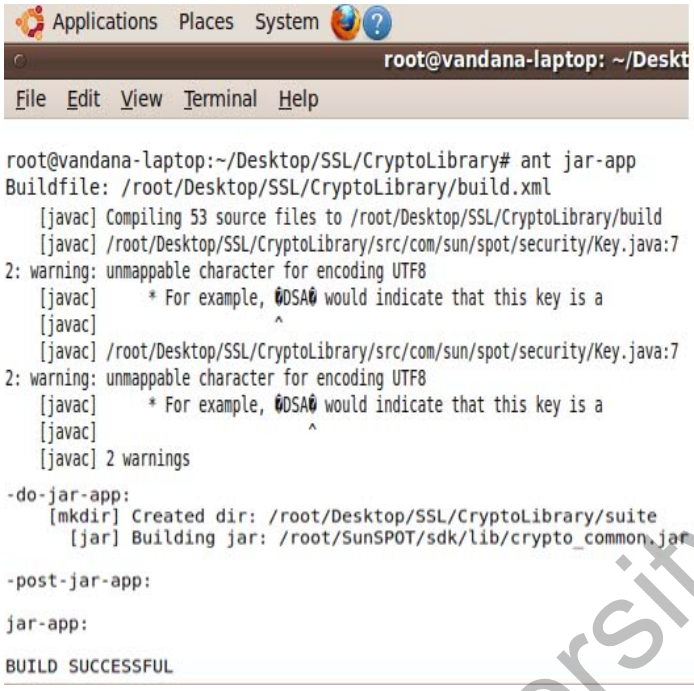


**Figure 4.15** Output of *ant jar-app* command.


**Figure 4.16** Output of ant jar apps command.

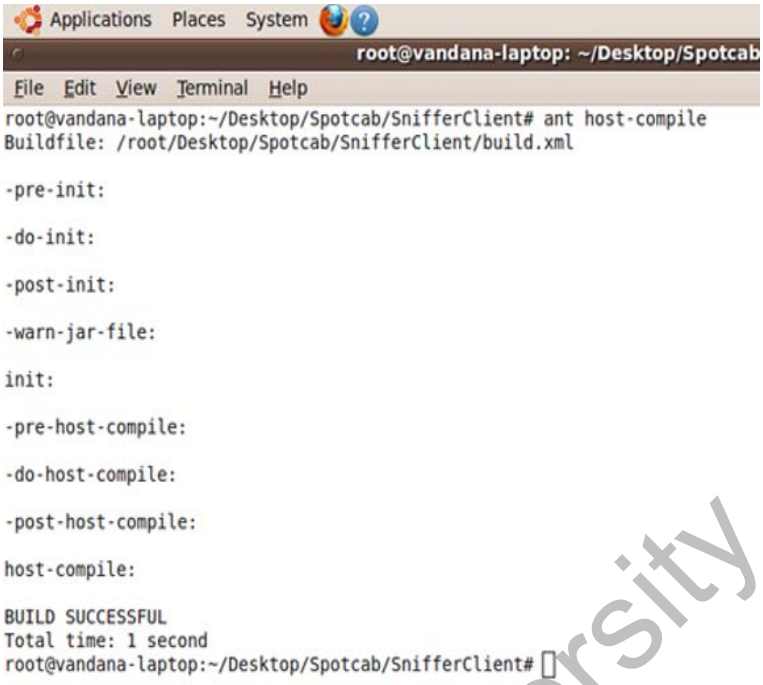


**Figure 4.17** Output of ant info command for basestation.

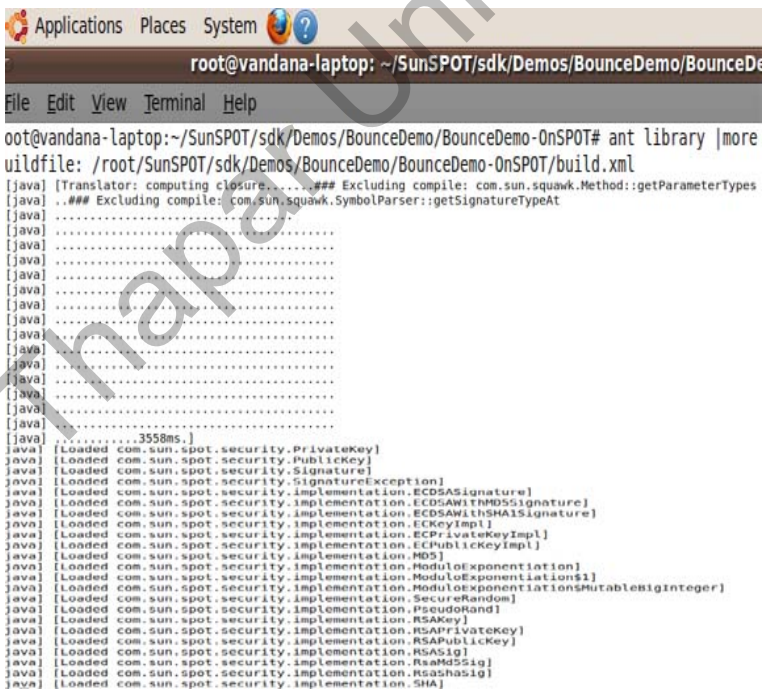


**Figure 4.18** Output of ant library command.

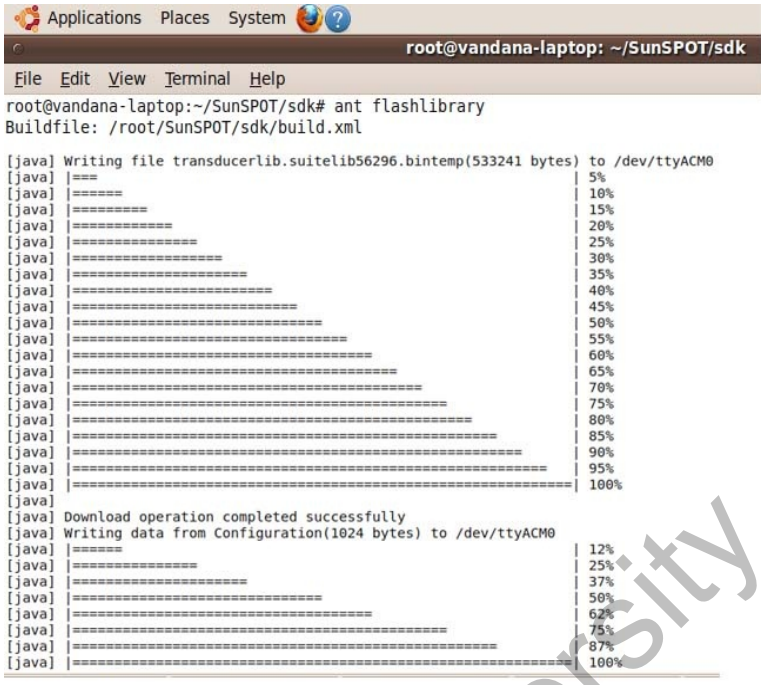


**Figure 4.19** Output of ant reset command.

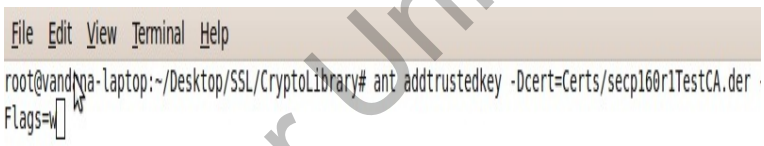


**Figure 4.20** Output of ant addtrusted command.

be listed using *ant listtrustedkeys* as shown in Figure 4.21

3. **Deploying application and creating keys on device:**Here again BounceDemo-onSPOT application is deployed as described in previous sections. However to support the crypting algorithm "radiostream" is changed to "sradiostream" which are analogue of "http" to "https".

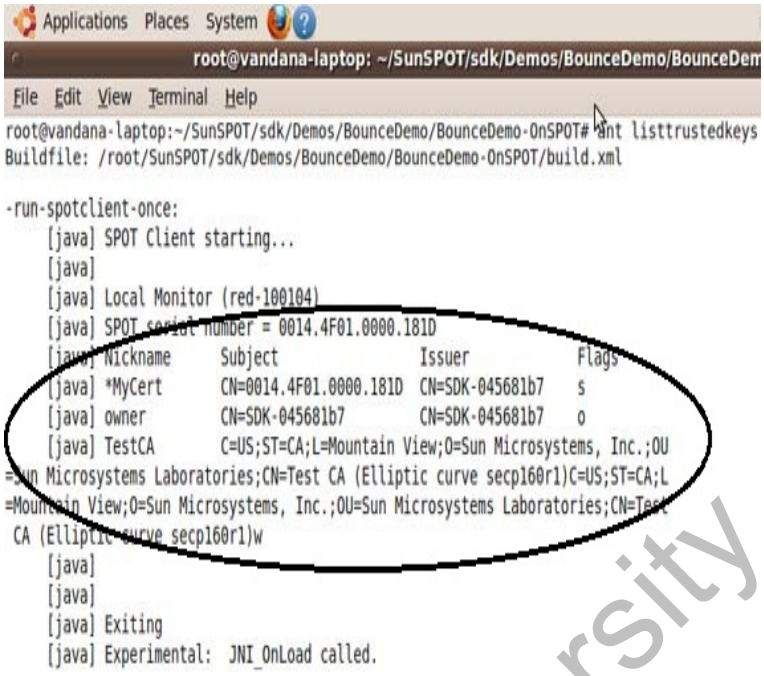


**Figure 4.21** Output of ant listtrusted command

### Analyzing Encrypted packets

Now Sniffer Client on the Base Station can be defined similarly in the same way as described in the previous section now when we open the encrypted packets in wireshark as shown in Figure 4.21.

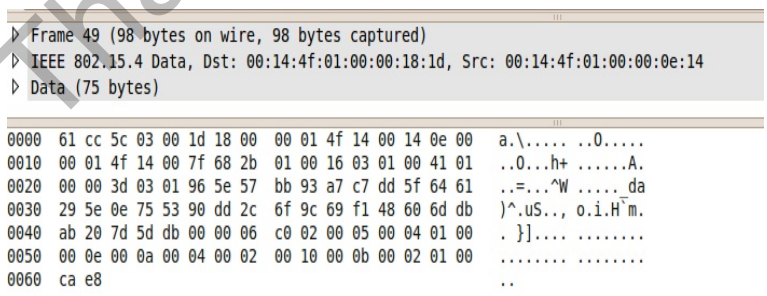


**Figure 4.22** Output of wireshark showing encrypted data.

.

The Figure 4.22 shows any data exchanged between two spot is encrypted and can-

not be deciphered easily. As in previous section where one can easily see cleartext flow.

## 4.3 Problem Faced during Implementation:

1. **Wireshark Plugin Installation:** While using wireshark or analyzing the packet a particular dissector required to be installed i.e "lowpan". Because without it the software is able to read only physical layer info and cannot detect the transport layer information. This required changing in the source code of wireshark. Initially the entire setup was done on Windows 7 but then it was done on Ubuntu 9.1.0 as the compiling of wireshark required number of softwares which are easily available on Linux as compared to windows.

2. **Internet Connection**: Working on Sun Spot Manager tool requires regular internet connection. So at any point the connection is not there one cannot work over the tool.

3. **Irregular responses of devices:** Device once detached and again attached when again asked for the information refuse to respond and do not display the information, so proper shutdown or plugging in different USB port is required. Another method to perform all the programmming steps OTA, which is vulnerable to disconnections due to interferrence.

Here the two devices are made to trust each other by adding the key explicitly, the system can be extended to have secure key exchange for large scale deployments.

# Chapter 5

# Conclusion and Future Scope



This thesis investigated the mathematical foundation of Diffie-Hellman key exchange protocol and the elliptic curve cryptography for the purpose of understanding the practical problems of implementing the theoretical concepts on wireless sensor networks.The main results are as follows:

1. Designed a technique for establishing secure communication between nodes in wireless sensor networks.The protocol is not vulnerable to man-in-middle attacks problem.

2. Implemented the technique over Java Sun Spots for its analyzing the cryptographic behaviour. Here one spot sent the light information to other. It appears as ball bouncing between the SunSpots. The packet captured first, in human readable form and, then in cryptographic form.

## 5.1 Future Work

In future this research work can be extended as :

- Design and implement a set of attacks against ECDH protocol.
- Calculating the computation cost of ECDH protocol after deploying it on the Sun Spot.
- Testing the key generation process between multiple Sun Spots nodes and test it in a multiple using complex enviornment of WSN networks.
- Calculating the power and energy consumption of SunSpot devices after deploying ECDH protocol on it, required for key management authentication etc.

# References

[1] F.L. Lewis, Associate Director of Research and Head, Advanced Control and Sensor MEMS Group "Wireless Sensor Networks", Smart Environments: Technologies, Protocols, and Applications, Newyork 2004.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci "Wireless sensor networks: a survey" Published by Elsevier Science B.V.,2002.

[3] Rabi N. Mahapatra ,"Embedded System for Wireless Sensor Networks",http://courses.cs.tamu.edu/rabbi/cpsc617.

[4] Ian F.Akylidiz, Welian Su, Yogesh Sankarasubramaniam and Erdal Cayirci, Georgia Institute of Technology "A Survey on Sensor Networks" ,IEEE Communication Magazine, August 2002.

[5] F.Amin, A.H. Jahangir and H.Rasifard "Analysis of Public Key Cryptography", World Academy of Science Engineering and Technology, 2008.

[6] Y.W.Law "Key Management and Link Layer Security of WSN" Phd Thesis, University of Twente, Netherland 2005.

[7] Al-Sakib Khan Patan, Choong Seon Hoong, Hyung-Woo Lee, "Smartening the Enviornment using Wireless Sensor Networks in Developing Country", ICACT,2006.

[8] John Paul Walters, Zhengqiang Liang,Weisong Shi, and Vipin Chaudhary "Wireless Sensor Network Security :A Survey" Chapter 17.

[9] Mark Luk, Ghita Mezzour, Adrian Perrig, Virgil Gligor, "A Secure Sensor Network Communication Architecture", 6th International Conference Information processing in Sensor Networks pg 479-488, 2007.

[10] Anthony D.Wood, John A.Stankovic "Denial of Service in Sensor Networks" IEEE, 2002.

[11] Dr. G. Padmavathi, Mrs. D. Shanmugapriya "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security,Vol. 4, No. 1 2, 2009.

[12] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", ICACT, 2006.

[13] M.J.Carmel Mary Belinda, ,C.Suresh Gnana Dhas "A Study of Security in Wireless Sensor Networks", MASAUM Journal Of Reviews and Surveys, Volume 1 Issue 1, September 2009.

[14] Sophia Kaplantzis, "Security Models for Wireless Sensor Networks" Phd Thesis under Supervisors: Dr N. Mani, Prof. M. Palaniswami, Prof. G. Egan,

March 2009, http://users-monash.edu.au.

[15] Pyrgelis Apostolos, "Cryptography and Security in Wireless Sensor Networks", FRONTS 2nd Winterschool Braunschweig, Germany 2009

[16] Cryptography, 25 June 2010 "http://en.wikipedia.org/wiki/Cryptography".

[17] Ian Curry "An Introduction to Cryptography and Digital Signatures", Copyright-Entrust, version 2.0,March 2002.

[18] Dr.Rahul Banerjee, Introducton to Symmetric Key Cryptography, BITS Pilani presentation.

[19] B.A.Frouoazan, "Cryptography and Network Security", International Edition McGrraw Hill, 2008

[20] J.Katz and Y.Kindell, "Introduction to Modern Cryptography", Champan and Hall/CRC 2008

[21] Navdeep Shohaib, "A portable and Improved Implementation of Diffie Hellman Protocol for Wireless Sensor Networks", Phd Thesis, Youngstown State University, August 2009.

[22] N.Koblitz, "Elliptic Curve Cryptosystem, "Mathematics of Computation vol 48 pp208-209,1987.

[23] Anoop MS, "Elliptic Curve Cryptography-An Implementation", www.security.ittoolbox.com/research.

[24] David Boyale,Thomas Nave "The Imapct of Java and public key Cryptography", The Fourth International Conference on Wireless and Mobile Communication, 2008.

[25] Sun Labs, "SunSpot Owners Manual", copyright SunMicrosystems.

[26] Sun Labs, "SunSpot Developer' Manual", copyright SunMicrosystems.

[27] SunLabs, "http://www.sunspotworld.com/index.html", copyright SunMicrosystems.

[28] SunLabs, "http://www.sunspotworld.com/GettingStarted/Linux.html", copyright SunMicrosystems.

[29] Hemanta Kumar Kalita, Avijit Kar "WIRELESS SENSOR NETWORK SECURITY ANALYSIS", International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009.

# List of Publications

"Design and Develop Elliptical Curve Cryptography for Wireless Sensor Network", Vandana Ladha, Maninder Singh,"International Journal of Network Security", communicated, June 2010.