An Improved User Authentication Protocol for Hierarchical Wireless Sensor Networks using Elliptic Curve Cryptography

Rakesh Maharana

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela – 769 008, India

An Improved User Authentication Protocol for Hierarchical Wireless Sensor Networks using Elliptic Curve Cryptography

A thesis submitted in partial fulfillment
of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering

by

Rakesh Maharana

(Roll No. 211CS2280)

under the supervision of

Prof. Pabitra Mohan Khilar

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela – 769 008, India

Dedicated to my family

Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, India. www.nitrkl.ac.in

May 22, 2013

Certificate

This is to certify that the work in the thesis entitled ***An Improved User Authentication Protocol for Hierarchical Wireless Sensor Networks using Elliptic Curve Cryptography*** by ***Rakesh Maharana***, bearing roll number *211CS2280*, is a record of an original research work carried out by him under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of *Master of Technology* in *Computer Science and Engineering*. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Dr. Pabitra Mohan Khilar

Acknowledgment

First of all, I would like to express my deep sense of respect and gratitude towards my supervisor Prof. Pabitra Mohan Khilar, who has been the guiding force behind this work. I want to thank him for introducing me to the field of Wireless Sensor Network and giving me the opportunity to work under him. His undivided faith in this topic and ability to bring out the best of analytical and practical skills in people has been invaluable in tough periods. Without his invaluable advice and assistance it would not have been possible for me to complete this thesis. I am greatly indebted to him for his constant encouragement and invaluable advice in every aspect of my academic life. I consider it my good fortune to have got an opportunity to work with such a wonderful person.

Secondly, I would like to thank Prof. S.K. Jena, Prof. A.K. Turuk, Prof. B. Majhi, Prof. B. D. Sahoo, Prof. D. P. Mohapatra, Prof. S. K. Rath and Prof. S. Chinara for their valuable suggestions, and encouragements during the research work.

I must acknowledge the academic resources that I have got from NIT Rourkela. I would like to thank administrative and technical staff members of the Department who have been kind enough to advise and help in their respective roles.

During my studies at NIT Rourkela, I made many friends. I would like to thank them all, for all the great moments I had with them.

My family is the backbone behind all my endeavors with their love and support. No word of thanks can be enough for them for their encouragement, support and belief in me.

Finally, I thank God for everything.

Rakesh Maharana

Abstract

In wireless sensor network, most of the queries are issued at the base station or gateway node the network. However, there are some critical WSN applications where real-time data are needed. But data at base station may not be real-time because of communication delay or periodic nature of data collection. So, real-time data can be accessed from the sensor nodes directly on demand. Before allowing the user to access real-time data from the sensor node, authentication of user must be ensured. But user authentication in case of wireless sensor network is a very critical task, as sensor nodes are deployed in unattached environment and are prone to possible hostile network attacks. Any authentication protocol in WSN must be designed keeping the fact that sensor nodes have limited computing power, memory, energy and communication capabilities.

In this thesis, an improved user authentication protocol based on Elliptic Curve Cryptography (ECC) has been introduced for hierarchical wireless sensor networks (HWSN). This thesis shows that the ECC based protocol is suitable for wireless sensor networks, where higher security is demanded. Besides this the proposed scheme provides mutual authentication and a secret session key for communication between the user and the cluster head. It also provides an option for addition or replacement of cluster head in the network whenever there is a need. Then a comparative study of the proposed scheme with various existing is presented.

Contents

Certificate **iii**

Acknowledgement **iv**

Abstract **v**

List of Figures **ix**

List of Tables **x**

Acronyms **xi**

1 Introduction **1**

1.1 Introduction 1

1.2 Obstacles of Sensor Security 3

1.2.1 Limited Resources 3

1.2.2 Unreliable Communication 4

1.2.3 Unattended Operation 5

1.3 Security Requirements 6

1.3.1 Data confidentiality 6

1.3.2 Data Integrity 7

1.3.3 Data Freshness 7

1.3.4 Availability 8

1.3.5 Self-Organization 8

1.3.6 Time Synchronization 9

1.3.7 Secure Localization 9

1.3.8 Access control 9

1.4 Access Control Challenges . . . 10
1.4.1 Sensor Network Architecture . . . 10
1.4.2 Access Control Services . . . 12
1.5 Authentication in Wireless Sensor Networks . . . 13
1.5.1 Outside user authentication . . . 13
1.6 Motivation . . . 14
1.7 Research Objective . . . 15
1.8 Organization of The Thesis . . . 15
1.9 Summary . . . 16

2 Literature Survey **17**
2.1 Introduction . . . 17
2.2 Related Work . . . 18
2.2.1 Watro et al. scheme . . . 18
2.2.2 Benenson et al. scheme . . . 18
2.2.3 Wong et al. scheme . . . 19
2.2.4 Banerjee et al. scheme . . . 19
2.2.5 Jiang et al. scheme . . . 19
2.2.6 Tseng et al. scheme . . . 20
2.2.7 Das scheme . . . 20
2.2.8 Nyang and Lee scheme . . . 21
2.2.9 Khan and Alghathbar scheme . . . 21
2.2.10 He et al. scheme . . . 21
2.2.11 Cheikhrouhou et al. scheme . . . 21
2.2.12 Tseng et al. scheme . . . 22
2.2.13 Kumar et al. scheme . . . 22
2.2.14 Fan et al. scheme . . . 23
2.2.15 Xue et al. scheme . . . 23
2.3 Summary . . . 23

3 An Improved User Authentication Protocol for Hierarchical Wireless Sensor Networks using ECC **24**
3.1 Introduction . . . 24
3.2 Network Model . . . 26
3.3 Overview of ECC . . . 27

3.4 Proposed Authentication Protocol 28
3.4.1 Notations Used 28
3.4.2 Registration Phase 30
3.4.3 Login Phase 30
3.4.4 Authentication Phase 31
3.4.5 Password Change Phase 34
3.4.6 Dynamic Node Addition 36
3.5 Summary 36

4 Analysis of Proposed Scheme **37**
4.1 Introduction 37
4.2 Security Analysis 38
4.3 Comparison with Related Schemes 41
4.4 Summary 45

5 Conclusion and Future Work **46**
5.1 Conclusion 46
5.2 Future Work 47

Bibliography **48**

Dissemination **52**

List of Figures

1.1 WSN's outside access control architecture [1]. 10
1.2 WSN's inside access control architecture [1]. 11

3.1 A hierarchical wireless sensor network model [2]. 27
3.2 Registration Phase. 31
3.3 Login Phase. 32
3.4 Authentication Phase. 34
3.5 Password Change Phase. 35

List of Tables

3.1 List of notations used in the proposed scheme 29

4.1 Comparison of enhanced security features of the proposed scheme with other schemes 43

4.2 Comparison of computational cost in different phases of proposed scheme with other schemes 44

Acronyms

Acronym	Description
WSN	Wireless Sensor Network
HWSN	Hierarchical Wireless Sensor Network
ECC	Elliptic Curve Cryptography
DLP	Discrete Logarithm Problem
CDLP	Computational Diffie-Hellman Problem
ECDH	Elliptic curve Diffie-Hellman
PKC	Public Key Cryptography
PDA	Personal Digital Assistant
DoS	Denial-of-Service
KDC	Key Distribution Center
AES	Advanced Encryption Standard
SCK	Self-Certified Cryptosystem
MAC	Message Authentication Code
SHA	Secure Hash Algorithm
PC	Personal computer
BS	Base Station

Chapter 1

Introduction

1.1 Introduction

Wireless sensor networks are distributed networks of autonomous sensors and are used to monitor physical or environmental condition. Recent technological advancements in micro-electro-mechanical systems technology, digital electronics and wireless communications have facilities the developments of a small size sensor node which are low cost, low power and multifunctional miniature devices having sort communication range [3]. Each sensor node is capable of only a limited amount of processing, but their collaborative efforts have the ability to measure a given physical environment in great detail. So a wireless sensor network can be described as a collection of sensor nodes which co-ordinate to perform some particular action. Differentiating them from traditional networks, sensor networks depend on high deployment density and co-ordinate among themselves to carry their task. These sensors can be deployed in two different ways [3].

- In first case, sensor nodes can be placed far from the actual event, i.e., something sensed by perception. In this case, uses of some complex procedures are required to differentiate the targets from surrounding noise.

- In second case, several sensor nodes which do only the sensing job can

be deployed. The positions of the sensor nodes and their topology of communications are carefully handled. They send time series of the sensed data to the central nodes where these data are processed and computations are performed, and data are aggregated.

A WSN is comprised of a huge number of sensor nodes, which are deployed densely either inside the monitoring area or very close to it. The pre-determination of position of sensor nodes is not needed, which permits deployments of sensor nodes in a remote territory. Besides that, sensor network protocols and algorithms must possess self-organizing capabilities. Sensor nodes co-operate with each other to achieve their goal. They are equipped with an in-built processor. They do not send the raw data directly to the nodes which are responsible for the data fusion. They use their processing abilities to perform simple computations locally and then perform transmission of the required and partially processed data [3].

Wireless sensor networks are generally deployed for the different variety of applications, which often includes environment monitoring, enemy movements sensing and tracking in a battle field, etc. Each sensor node has limited resources such as energy, computation power, memory. Sensor nodes are deployed in hostile environment. So they are in direct contact with environment. They communicate trough wireless media. These factors make them vulnerable to various attacks [1]. Thus, access control becomes a very important requirement.

Organization of the Chapter

The rest of this chapter is organized as follows. In Section 1.2, different types of constraint in WSN is described. In Section 1.3, security requirements of WSNs is given. In Section 1.4, access control challenges in WSNs is described. Section 1.5 shows authentication problems in WSNs. Section 1.6 and Section 1.7 describes motivation and research objective respectively. Section 1.8 shows the organization of the whole thesis. Finally, Section 1.9 gives the summary of the chapter.

1.2 Obstacles of Sensor Security

A wireless sensor network is different from a traditional computer network as it is having many constraints compared to the traditional computer network. Because of these constraints, it is difficult to apply existing security approaches to the wireless sensor networks directly. Those constraints are described below as [4], [5].

1.2.1 Limited Resources

A certain amount of resources is required by every security approaches for the implementation, including memory, storage memory, processing power, code space and energy. In case of wireless sensor networks, sensor nodes have a limited amount of memory, storage, processing power and energy to run them.

Limited Memory and Storage Space

A sensor node is a very tiny device having a limited amount of memory and storage space for processing and storing values. To make an effective security mechanism, it is necessary to make the amount of codings required for the security algorithm small.

Power Limitation

The main constraint to wireless sensor capabilities is energy. It is hard to replace those sensors considering high operating cost. It is also difficult to recharge those sensors. In order to increase life of individual sensor nodes and the whole sensor network the amount of energy or battery charge carried by those nodes must be conserved. While applying any cryptographic protocol or function within sensor node, energy impact due to those security enhancements on the sensor node must be considered. Here the interest is to find the impact of the added security on the life span of a sensor that means battery life of sensors. Extra power is invested in processing required for security functions like encryption, decryption, signing data,

verifying signatures, etc. or transmitting data related to security or overhead like IV (initialization vectors) needed for encryption/decryption or the energy required for storing the security parameters securely like cryptographic key.

1.2.2 Unreliable Communication

Another threat to sensor security is unreliable communication. The security of WSNs depends heavily on a user's security protocol that is again dependent on communication.

Unreliable Transfer

The routing protocols used in a wireless sensor network are packet-based, and these routing protocols are connectionless, hence inherently unreliable. Due to channel errors, packet may get damaged or may be dropped in the path because of highly congested nodes. The results are lost due to damaged packets or dropped packets. Another cause of damaged packets is the unreliable wireless communication channel. So resources are used to avoid channel error and in wireless communication, channel error rate is very high. It is possible that during transmission necessary security packets, like a cryptographic key, may be lost if proper error handling is not included in the protocol.

Conflicts

Considering the communication channel to be reliable, there may be a case that the communication itself is unreliable. The reason behind this is the broadcast behaviour of the wireless sensor network. The transfer will fail, if the packets meet in the middle of transfer, due to conflict. This can be a major problem in case of high dense sensor network [6].

Latency

Another factor is latency. Latency can be increased due to network congestion, multi-hop routing and node processing, which will make it difficult in achieving synchronization among sensor nodes. The synchronization issues can make it hard for maintaining sensor security as security mechanism depends on critical event reports and cryptographic key distribution [7].

1.2.3 Unattended Operation

The sensor nodes may be left unattended for a long period of time which depends on function of the particular sensor network. There are mainly three types of concerned factors for the unattached sensor nodes:

Exposure to Physical Attacks

Generally, sensors are deployed in an environment which is open to adversaries, and also open to different physical condition like bad weather and so on. There are always potential risks that a sensor may suffer a physical attack in those environments which is very rare in case of typical PCs, which are located in a secure location and usually suffer attacks from networks.

Managed Remotely

The management of sensor network is done remotely, which make it impossible to find or detect physical tampering (like tamper proof seals) and physical maintenance (like replacement of battery). Most extreme example of sensor network is when, it is used for remote reconnaissance missions behind enemy lines. In that situation, there may not be any physical contacts with friendly force after their deployment.

No Central Management Point

A sensor network is distributed network, which does not have a central management point. This property will increase the vitality of the sensor network. However, if it is not designed correctly, it will make the network organization difficult, fragile and inefficient.

1.3 Security Requirements

A Wireless sensor network is a unique type of network. It shares some similarities with common computer network, but it also poses some unique requirements. Some security requirements are described below. Among those requirements, some of them are typical network requirements, and others are unique to wireless sensor networks [4].

1.3.1 Data confidentiality

Data confidentiality is the very important issue in network security. Whatever may be security requirements in a network data confidentiality problem must be addressed first. In wireless sensor networks following are some situation where data confidentiality comes into picture [4], [8] [5]:

- A sensor network should not leak information read by itself to its neighbors. Especially in a military application or battle field application as the data stored in the sensor node may be highly sensitive.
- It is very important to build a secure channel in a wireless sensor network as in many applications, nodes communicate highly sensitive data, e.g., key distribution.
- Public sensor information like identity of sensor nodes and public keys, must be encrypted to protect them against traffic analysis attacks.

The general approach to keep a sensitive data secret is to save those data in encrypted form with a secret key that is only possessed by the legitimate receivers thus confidentiality is achieved.

1.3.2 Data Integrity

After implementation of confidentiality, an attacker may not be able to steal information, but that does not make the data stored in sensor node in the network safe. There are possibilities that adversary can change the data so that it can put the network in disarray. A compromised or malicious node may manipulate data or add some wrong fragments to the data within the packets. This new packet can then be sent to the original receiver. In some cases, data loss or damage can occur without the presence of a malicious node. Severe communication can also lead to data loss or damage. Thus, data integrity ensures that any received data has not been altered during transmission.

1.3.3 Data Freshness

Even if we managed to maintain confidentiality and data integrity, there is no guarantee that received messages are fresh ones. Data freshness ensures that received messages are not replayed and should be fresh and created recently. In a design, where shared key strategies are employed, data freshness plays a very important role. Generally shared keys are needed to change over time. However, to propagate these shared keys over the network will take time. The adversary can easily perform replay attack. If a sensor is unaware of the new key change time, then it makes an adversary to disrupt the normal work of sensors easily. To ensure data freshness a time stamp or nonce can be added to the packet.

1.3.4 Availability

Implementing traditional encryption methods and adjust them to fit within WSNs is not free. It will introduce some extra overheads. Some of them choose some approaches that it can modify the code to reuse as much code as possible. Some of them use traditional communication to meet the same goal. In some cases, it may happen that some approaches force strict limitations on the data access or in order to make it simple some unsuitable scheme like a central point scheme may be proposed. However, all the approaches can weaken the availability of a sensor and sensor network for reasons described below [4]:

- Additional computation consumes additional energy. If all energies are consumed that means no more energy exists and sensor nodes are dead, the data will no longer be available.
- Additional communication also consumes more energy. Another problem is, as communication increases so does the chance of incurring a communication conflict.
- If a central point scheme is used, the chance of single point failure will increase which in turns badly affects the availability of the network.

The security requirements affect the operation of WSN and it also very important for maintaining availability of entire sensor network.

1.3.5 Self-Organization

A wireless sensor network is a basically a ad-hoc network. It requires every sensor node to be independent and flexible enough to be self-healing and self-organizing depending upon different situations. In case of wireless sensor networks, there is no fixed infrastructure. Those features bring a great challenge to wireless sensor network security as well.

1.3.6 Time Synchronization

There are so many applications that depend upon some form of time synchronization. However, in order to save power, a sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pairwise sensors. A sensor network may require group synchronization for tracking applications, etc.

1.3.7 Secure Localization

The utility of a sensor network often depends upon its ability to correctly and automatically locates every sensor node in the network. A sensor network designed to locate faults will need accurate location information in order to find the particular point of a fault. The attacker can easily change non-secured point of fault information by reporting wrong signal strengths, replaying network signals [4].

1.3.8 Access control

Access control is a critical security task in Wireless Sensor Networks (WSNs). To restrict malicious nodes and unauthorized user from joining the sensor network, access control is necessary. On one hand, WSN must be able to authorize and grant users the right to access to the network. On the other hand, WSN must organize data collected by sensors in such a way that an unauthorized entity (the adversary) cannot make arbitrary queries. This restricts the network access only to eligible users and sensor nodes, while queries from outsiders will not be answered or forwarded by nodes [1].

1.4 Access Control Challenges

1.4.1 Sensor Network Architecture

The wireless sensor network is a large network in which a huge number of sensor nodes is deployed over a large area which is having one or more sink nodes or base stations. These base stations are trusted by all sensor nodes. Considering two different kind of wireless sensor network condition, access control can of inside access control or outside access control [1]. Outside access control for WSN is

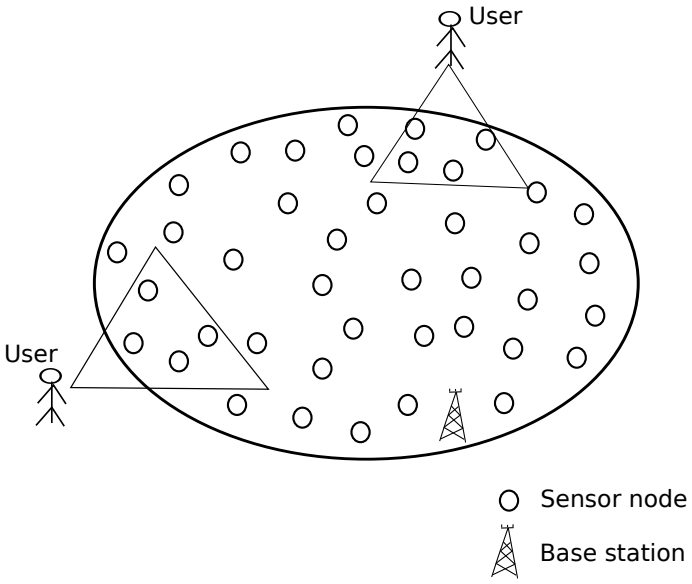

Figure 1.1: WSN's outside access control architecture [1].

shown in Figure 1.1 and Inside access control for WSN is shown in Figure 1.2 [1]. As mentioned in Figure 1.1 outside access control gives service to the mobile users. In this case, base station acts as a point of network administrator and responsible for managing security protocols and sensor nodes act as a point for data collection for user, i.e. laptop, mobile phones, etc. Only those users are allowed to collect data from WSN who have subscribed for that service. In case of sensor network shown in Figure 1.2, there are no connected users. The WSN may function as a time driven application or may function as an event-driven application. Query can only be sent

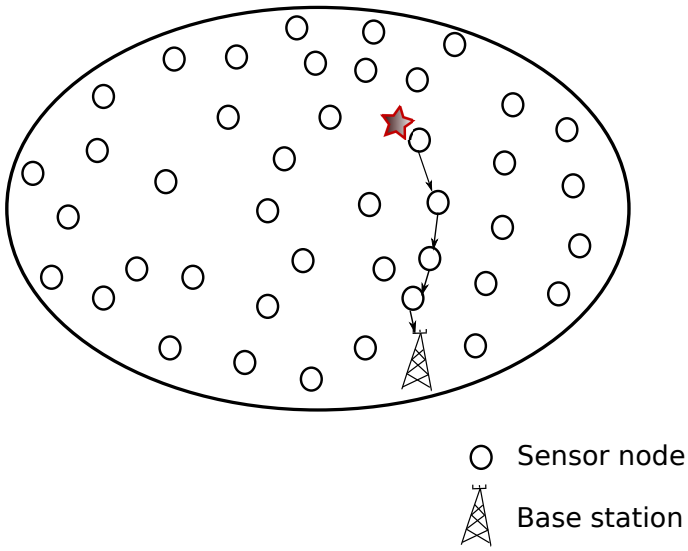

Figure 1.2: WSN's inside access control architecture [1].

by the base station. In order to stop an adversary or attacker from sending queries to the sensor nodes access control method must be included as a built in task in each sensor node. So above two architecture are divided as: [1].

- Outside access control
- Inside access control

Outside access control

In this case, secure communication is performed between WSN and the outside users. Here only the authorized uses are able to send a request for data. These requests can be sent to some node or a set of nodes in the user proximity. This is shown in the Figure 1.1.

Inside access control

In this case, secure communication happens in between sensor nodes and between sensor nodes and the base stations. This architecture is shown in the Figure 1.2.

1.4.2 Access Control Services

Access control services in Wireless Sensor Networks can be divided into two types [1]: Authentication and Authorization.

Authentication

In case of authentication, a relation is established between the user and some identifier. That identifier or identity is unique to that user, and generally, it cannot be copied or modified or forged. In WSN, authentication can be classified as two types: user authentication and authenticated querying. In user authentication process, user's identity and name are sent by the user to the sensor node and sensor nodes decide whether the identity sent by the user is valid or not i.e. identity belongs to that user or not. However, in case of authenticated querying, it is decided whether a query comes from an authorized user or a sensor node or a base station.

Authorization

In authorization, a relation is established between a user and a set of access rights. In this process, user's name along with its requested operations i.e. read or write, is sent to the sensor nodes and then sensor nodes decide whether this user is allowed to perform the operations as it requested or not. Generally, operation like authentication, authorization and authenticated querying are combined as a single operation. When a request is received the access control mechanism checks whether or not the request is come from a legitimate entity along with its access rights, i.e. authentication and authorization. After that it sends back a response to the user, and that response may be the data which the user is requested, or it may be a failure message.

1.5 Authentication in Wireless Sensor Networks

Beneson et al. [9] distinguished between the inside security and the outside security in WSNs as:

- *Inside security* means secure communication between the sensor nodes and secure communication between the sensor nodes and the base station(s) or gateway node(s).
- *Outside security* refers to secure communication between outside users and sensor nodes.

Authentication in wireless sensor networks is a very crucial requirement which is a part of both outside security and inside security. If a strong authentication mechanism is not included, then an adversary can often generate dummy data packets and force sensor node to relay those packets to make sensor nodes energy exhausted. A fake message can cause sensor nodes to accept and transfer wrong information which in turn makes sensor nodes prone to various attacks. Authentication in wireless sensor networks can be classified into following categories [10]:

- Authentication of base station to the sensor nodes or in between sensor nodes.
- Authentication of user to the sensor nodes.

There are many solutions given to address the base station to sensor nodes authentication and sensor nodes to other sensor nodes authentication. In this thesis, we focus on the authentication of users, those are outside of the sensor network, to the sensor nodes. In this type of authentication, outside users are authenticated to a set of sensor nodes within their directly or via base station.

1.5.1 Outside user authentication

Sensor nodes in a wireless sensor network usually collect a wide variety of data. Those data are generally used by different types of users such as universities, research

organization, business organization, military personnel or individuals [10]. For example, the humidity level in an area might be useful information for a farmer. Enemy movement through body temperature analysis is important for military personnel. An individual may be interested to know about the weather in his surroundings. A researcher may be interested in environmental data collected by the sensor nodes. An oil company might be keen to obtain ocean reading data [10]. However, considering deployment and maintenance cost, it is difficult for everyone to deploy own sensor networks to collect data of their interests. Generally, deployment and maintenance are done by some deployment agencies. The users who want data from WSNs pay those agencies for their required sensor data. Therefore, owners and users of the networks are different for some large-scale WSNs. Sensor data in large scale wireless sensor networks are valuable, and that is avail to only subscribed users who paid those data. Besides these commercial applications, there are many military applications, which gather sensitive and confidential data, which should be accessible to authorized army officers and soldiers only. These facts raise the issue of authentication of a legitimate user in WSNs. User authentication is a process by which the system verifies the identity of a user who wants to access the sensor nodes data. A user authentication mechanism is necessary to prevent unauthorized users from accessing sensor nodes data.

1.6 Motivation

In Wireless Sensor Networks (WSN), there are several challenges. A proper user authentication scheme in a wireless sensor network is a difficult task. The main problem for this is resource-constraint nature of the WSN. That means sensor nodes have very limited energy, computing power and memory. Considerable progress has been made to solve the authentication problems in WSN, but they are inadequate. Most of the existing authentication frameworks concentrate on a specific problem in authentication but ignore others. Most of them deal with homogeneous wireless

sensor network. However, nowadays heterogeneous wireless sensor networks or hierarchical wireless sensor networks are on demand due to their better performance. In HWSNs, public key Cryptography(PKC) particularly elliptic curve cryptography can be applied as cluster head of HWSNs having more energy, computing power and memory. So that, a more secure user authentication protocol can be designed.

1.7 Research Objective

With the motivation as outlined in the previous section, we identify the objectives of our research work is as follows:

- To design a user authentication scheme in a hierarchicalwireless sensor network which can address all the problems of the former schemes.
- To make the scheme secure against all possible attacks.
- To make the scheme scalable in terms of sensor node addition anduser addition
- Compare the scheme in terms of security and computation timewithother related schemes.

1.8 Organization of The Thesis

The remainder of the thesis is organized as follows.
Chapter 2 describes existing works on userauthentication in Wireless Sensor Networks.
In **Chapter 3**, the proposed approach is discussed in detail including Network Model and Elliptic curve cryptography overview.
In **Chapter 4**, analysis of a proposed scheme is given.
Finally, in **Chapter 5**, concluding remark is given.

1.9 Summary

This chapter gives brief overview of wireless sensor networks. There are various obstacle in WSNs like limited resources, unreliable Communication and unattended operation . Various secuirty requirements needs to be taken into consideration like data confidentiality, data integrity, data Freshness and so on. There are different types of challenges related to access control in WSNs. Then it gives a brief overview about user authentication in WSNs.

Chapter 2

Literature Survey

2.1 Introduction

Authentication is a process of proving an entity's identity. User authentication in case of wireless sensor network is a very critical task, as sensor nodes are deployed in unattached environment and are prone to possible hostile network attacks. User authentication in wireless sensor networks may be designed using some user credentials like user's ID and a password known only to the user, or it may be a smart card along with like user's ID and a password. There are two approaches to achieve user authentication in case of WSNs [10]. First one is distributed approach. In this type of approach, the sensor nodes that receive the user request locally verify it and process the user's query. In this case, involvement of third party like base station is not required. However, this approach puts more loads on the sensor nodes and is not preferred as sensor nodes have very limited resources. Another approach is a centralize one. In this type of approach user send a log-in request to a central entity, i.e. base station or gateway node. After successful authentication, base station forwards the query to the sensor node for query processing. In some cases, user sends the log-in request to the sensor node directly. The sensor node forwards the log-in request to the base station to perform authentication. The base station

checks the legitimacy of the user request and makes the decision to grant access to user or not. Then it replies to the sensor node. Based on the decision sensor node provides the data to the user or sends a denial message. This chapter reviews the existing solutions to authentication problems in WSNs.

The rest of this chapter is organized as follows. In Section 2.2, we have given brief description of existing schemes along with their merits and demerits. Finally, in Section 2.3, We summarised the chapter.

2.2 Related Work

In this section, a brief discussion of the existing user authentication schemes in the wireless sensor network is given.

2.2.1 Watro et al. scheme

Watro et al. [11] proposed a user authentication scheme for WSN called TinyPK, which is based on PKC (public key cryptography). Here it uses RSA [12] and Diffie Hellman protocol [13]. This protocol suffers from the "masquerade as a sensor node to an unknowing user" attack [14]. After receiving the user's public key, the intruder encrypts a session key and other parameters. Then it sends it to the user. The user believes that the message has come from the sensor node. It decrypts the message with the private key and uses the session key for further communication. This scheme also computationally inefficient and does not provide mutual authentication.

2.2.2 Benenson et al. scheme

Benenson et al. [9] mentioned several security issues in WSN, specifically the access control and proposed a method where the user can successfully authenticate with any subset of n sensors. Then Benenson et al. [15] proposed another solution, which based on Elliptic Curve Cryptography. In this scheme, sensor nodes require high storage

space as each pair of nodes requires a secret key. Here all user queries are processed by a single node. This node should be identified while authentication. However, in Benenson's scheme, there is no procedure given to find that node. This process also requires each node to know the entire network. There is no provision to deal with the situation where the node responsible for process the query is compromised and sends false information [16].

2.2.3 Wong et al. scheme

Wong et al. [17] proposed an efficient user authentication scheme. It is based on user's password and uses cryptographic hash function. It has security flaws like many logged in users with the same login-Id threat in which if an attacker has a valid user's password, he/she can login to the sensor network. It also suffers from stolen-verifier attack as both GW-node and login-node keeps the look-up table of registered user's secret information.

2.2.4 Banerjee et al. scheme

Banerjee et al. [18] proposed a fully symmetric key based scheme for authenticating a user in WSN. Here any node can reply to the user's query. It uses the pairwise key pre-distribution scheme proposed by Blundo et al. [19]. The node which processes user's query generates a nonce, and user must calculate a valid MAC for the generated nonce and sends back this MAC to the node. If the sensor does not receive a valid MAC, then it discards the login request. This scheme does not provide mutual authentication and prone to node compromise attack. It does not give clues how to find the sensor node which will process the user's query [16].

2.2.5 Jiang et al. scheme

Jiang et al. [20] proposed a distributed user authentication scheme in WSN. It is based on self-certified cryptosystem (SCK) which is modified to use ECC to establish

pairwise keys in sensor networks. Here the nodes which are in the transmission range of user, act collaboratively to find out whether the user is allowed to access the sensor network or not. The drawback with this scheme is that each node which receives the access request from the user has to compute a pairwise key which will be shared with the user. It also uses an encrypted nonce using ECC, which is an expensive task for sensor node [16].

2.2.6 Tseng et al. scheme

Tseng et al. [21] proposed a user authentication scheme which is an improved version of Wong et al. [17] scheme. It is resistance to reply attack and forgery attack and also allows a user to change his/her password freely. It also allows a user to login from any sensor node in the network. After receiving the login request from user sensor node forward this request to GW-node, which verifies authenticity of the user. User registration is performed at the GW-node. The weakness of the scheme is, it cannot resist node compromise attack, and it requires time synchronization, which is a difficult task in case of WSN [16].

2.2.7 Das scheme

M.L. Das [14] proposed a two-factor user authentication scheme in wireless sensor network. He mentioned security vulnerabilities in Wong et al. [17] scheme like many logged-in users with same login-Id threat and stolen verifier attack as GW-node and login-node maintain a lookup table of the entire registered user's secret information. He proposed protocol to overcome the security flaws of Wong et al. [17] scheme. He used a two-factor user authentication scheme based on a smart card and password. However, it cannot solve the problem like DoS attack and node compromise attack [22]. Here user cannot freely and securely change his/her password. Another problem is time synchronization as it uses the time stamp to restrict replay attack.

2.2.8 Nyang and Lee scheme

Nyang and Lee [23] proposed a user authentication scheme which is improved version of Das's two-factor authentication protocol. They have shown that ML. Das [14] scheme is vulnerable to gateway node impersonation attack, node compromise attack and password guessing attack. They have tried to overcome these problems in their proposed scheme. However, their scheme is vulnerable to attacks like parallel session attack, privileged-insider attack [24] and it also does not provide option for changing password. It suffers from the time synchronization problem.

2.2.9 Khan and Alghathbar scheme

Khan and Alghathbar [25] showed that ML. Das [14] scheme is not secure against gateway-node bypass attack, does not provide mutual authentication and also vulnerable to privileged insider attack. They also showed that ML. Das scheme does not have the provision to change password. They proposed a scheme which overcomes those security flaws. But it suffers from parallel session attack, partial mutual authentication [24]. It needs time synchronization to restrict the replay attack.

2.2.10 He et al. scheme

He et al. [26] proposed an improved scheme based on ML. Das [14] scheme. It keeps all the merit of the ML. Das [14] scheme and provides protocols to restrict insider attack and impersonation attack and provides methods to update the password.

2.2.11 Cheikhrouhou et al. scheme

Cheikhrouhou et al. [27] proposed a light-weight user authentication scheme for wireless sensor networks. Here user uses a PDA to authenticate himself/herself. It uses AES for encryption and decryption. In this proposed scheme, the administrator chooses a secret key x and loads it in the system server and coordinator node. This

secret x is used by the system server for registering the users. The coordinator uses this secret to verify the authenticity of users. Here a secret S is computed using secret x by the coordinator node. Here the problem is, if the coordinator node is compromised, all secret values of users will be known to the intruder who will create a valid ID and a secret value S [16].

2.2.12 Tseng et al. scheme

Tseng et al. [28] proposed a robust user authentication scheme for wireless sensor network based on elliptic curve crypto-system with self-certificates. In this scheme, KDC (key distribution center) is responsible for initialing system parameters, generating identity, generating private/public key-pair and distributing the certificate to each user and each sensor node. The problem is both users and sensor nodes have to store a lot of parameters. Here the user's identity is verified by the sensor node by checking the signature using Elliptic Curve, which is a costly task. It also suffers from DoS attack. Here by sending invalid certificates or signature to the sensor node the attacker can exhaust the memory at the node or make the node running out of energy [16].

2.2.13 Kumar et al. scheme

Kumar et al. [29] proposed an efficient two-factor user authentication framework for wireless sensor networks, which is based on password and smart card, and it uses one-way hash function. This scheme provides mutual authentication and gives user facility to change password at need. However, the problem here is, it does not restrict privileged insider attack as the password is sent to the base station in plain text. It also suffers from the synchronization problem as it uses the time stamp for avoiding replay attack.

2.2.14 Fan et al. scheme

Fan et al. [30] proposed an efficient and DoS-resistance user authentication scheme for two-tiered wireless sensor network. In this scheme, the user authenticates with Master Node / Cluster head in order to access information from the nodes in its cell. There is no provision to update the data table of user, so the user cannot be authenticated to Master Node not mentioned in the data table, even if he is legitimate one if some urgent requirement arises [16]. This scheme uses time stamps to avoid replay attack. However, time synchronization in the wireless sensor network is very difficult to achieve.

2.2.15 Xue et al. scheme

Xue et al. [31] a temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. It managed to provide mutual authentication and session key between user and sesnor node. However, here user cannot change password freely. It does not restrict privileged insider attack, prone to smart card security breach attack and there is no provision of identity protection [32]. It also needs time synchronization to prevent replay attack.

2.3 Summary

This chapter gives a brief idea about various existing authentication protocol in WSNs. Above discussed existing works target some authentication-related problem but ignore others. They have both advantages and disadvantages. This motivates us to design an improved authentication protocol in WSNs.

Chapter 3

An Improved User Authentication Protocol for Hierarchical Wireless Sensor Networks using ECC

3.1 Introduction

In a wireless sensor network (WSN), huge numbers of sensor nodes are deployed in the target field. After their deployment, the sensor nodes form ad-hoc infrastructure-less wireless networks. Then these nodes communicate with each other using wireless communication within their communication range. Those sensor nodes gather environmental data and transferred those data to a single point called base station or gateway node (GW node). Here data are routed to the base station via the multi-hop communication path. These sensor nodes are easy to deploy. They can be dropped on a particular area from the truck or plane, and then each sensor node coordinates with their neighboring sensor nodes, and together these nodes form a network which finally linked to base station [3]. These tiny sensors have limited energy, low processing power and less memory. However, they play a very important role in various areas like real-time traffic monitoring, military sensing and tracking,

building safety monitoring, measurement of seismic activity, wildlife monitoring and so on. When a user wants some data, he/she puts a query to the GW node or base station and GW node gives data collected from the sensor node. Consider the situation like a battle field where users are in the deployed area, and they need real-time data. In those situations if they collect data from the GW node the data may not be real-time as there is always transmission delay or periodic nature of data collection. In those cases, the appropriate decision cannot be taken quickly and correctly. So they need to collect data from the sensor node directly. If the data in the wireless sensor network are made available to users on demand, then authentication of user must be ensured before allowing the user to access data.

A proper user authentication scheme in the wireless sensor network is a difficult task. The main problem for this is resource-constraint nature of the WSN. That means sensor nodes have very limited energy, computing power and memory. As cryptographic concepts like public key cryptography take more computing power and require more energy, their use is avoided here. However, the use of PKC based on elliptic curve cryptography is feasible in case of wireless sensor network [33], [34]. Comparing RSA and ECC, it is found that RSA is based on integer factorization and the best algorithm to solve this integer factorization is sub-exponential whereas the best algorithm to solve ECC is exponential [34]. That's why compare to RSA. ECC can provide the same level of security with smaller key. ECC of key length 160 bits give the same level of security as RSA of 1024 bits key length [34]. This difference in length also affects the performance. For that reason, RSA consumes more energy than ECC [35]. As in case of WSN, there is limited energy, computational power and memory so ECC is preferred.

Here a smart-card based user authentication scheme in hierarchical wireless sensor network using ECC is proposed. This scheme combines ECDH and cryptographic hash function to provide authentication as well as a session key for further communication between user and cluster head.

The rest of this chapter is organized as follows. In Section 3.2 Network model is

given. In Section 3.3, overview of ECC is described. Section 3.4 describes the whole proposed scheme. Finally, in Section 3.5, we summarised the chapter.

3.2 Network Model

In traditional WSN, there is a trusted base station which is responsible for collecting data from the sensor nodes and also responsible for processing requests from the users. Here the sensor nodes have very limited energy, computing power and less memory storage. These sensor nodes also have a low transmission range. This architecture performs smoothly for small networks. For larger networks hierarchical wireless sensor network [2] (HWSN) is preferred. In this type of network, there is a hierarchy which is based on their capabilities, i.e. sensor node, cluster head and base station from lower to higher level.

Sensor node: These nodes are the generic sensor node. These nodes have very limited energy, computing power and short transmission range. In a cluster, these nodes communicate with the cluster head of that cluster. These nodes do the actual sensing job and then share the information with the cluster head.

Cluster head: These are a special type of nodes, which have more resources than generic sensor nodes. They have more energy, computing power, memory storage and also a higher transmission range. These cluster heads collect data from the sensor nodes in its cluster and communicate those data with other cluster heads as well as with base station. As they have the higher computing power, they can process complicated computing operations.

Base station: This is a powerful node having a wide communication range. The base station is not limited by energy, computing power or memory. It is also an access point for human interaction.

There are so many advantages of using HWSN. The cluster structure of HWSN makes it stable. If a user wants to know the information for a particular area, it can get from the cluster head within that area directly. It makes the sensor nodes

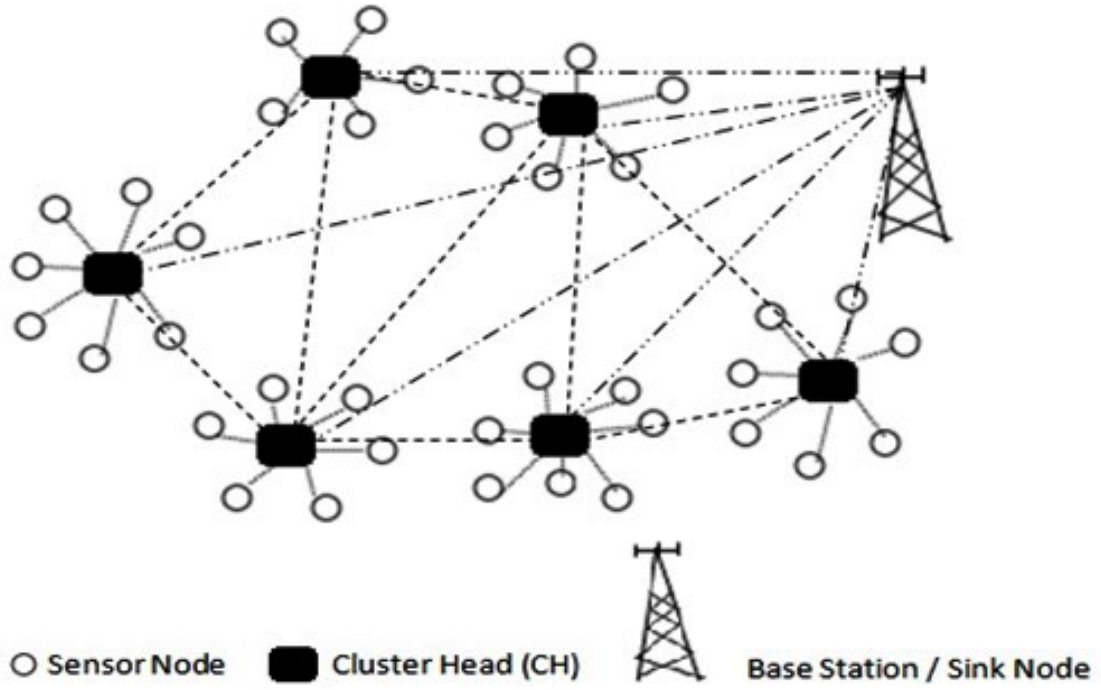

Figure 3.1: A hierarchical wireless sensor network model [2].

more efficient as they are not involved in transmission and user query processing. It also helps in eliminating redundant data. It improves network life time and also reduces network traffic and contention. The main advantage of this architecture is, cluster heads have more computing power and energy powerful security protocol can be integrated.

3.3 Overview of ECC

Weierstrass equation for the elliptic curve is $y^2 = x^2 + ax + b$ in which a and b is a real number. It is the simpler form of equation for the elliptic curve defined over the real number. The equation must satisfy $\Delta = -16(4a^3 + 27b^2) \neq 0$. Let F_q denote the finite field of points, where q is a large prime number and containing x, y, a, b elements E is a suitably chosen Elliptic curve defined over F_q. The points of

the equation and the point at infinity O compose the elliptic curve group over real numbers. A large prime number n is selected such that $nP = O$ using the elliptic curve addition algorithm. Here nP means elliptic curve multiplication. P is a base point in the generator point E [36] [37]. Security of ECC relies on the difficulties of following problems [38].

Discrete Logarithm Problem (DLP): given pubic key point $F = \alpha P$, it is hard to compute the secrete key α.

Computational Diffie-Hellman Problem (CDHP): given point elements αP and βP, it is hard to compute $\alpha\beta P$.

3.4 Proposed Authentication Protocol

In this section, a user authentication scheme for WSNs is presented, which assures the access and transfer of data to the legitimate user only. For that, first the user must register himself and on successful registration, the base station personalizes a smart card to the registered user. Under the network model mentioned in the section 3.2, the entire WSN is divided into number of clusters. Each cluster is administered by a cluster head. Each user has some device (like PDA), which has the ability to perform computational operations and commutate with cluster heads. Whenever a user needs some data, it can authenticate itself to the network and access data collected within the cluster from the cluster head.

3.4.1 Notations Used

In Table 3.1, the list of notations used in this proposed scheme is given. In this scheme, SHA-1 is considered to be as secure hash function. SHA-1 is one-way hash function, i.e. for a given $y = h(x)$, it is hard to find x [39], [37]. *cntr* is a counter used to specify communication between cluster head and base station. It is automatically incremented with new session and last *cntr* for each cluster head is stored in the database of base station.

Table 3.1: List of notations used in the proposed scheme

Notation	Definition
U_i	User i
ID_i	Identity of U_i
PW_i	Password of U_i
N_i	A secret random number known to U_i
BS	Base station.
CH_j	Cluster head in j^{th} cluster
ID_{CH_j}	Identifier of cluster head CH_j
S_n	Sensor node
x_a	A secret known to base station
K	Symmetric key of BS
x_{CH_j}	A secret shared between CH_j and BS
(.)	Cryptographic one-way hash function
$\bigoplus$	XOR operator
$\|\|$	String concatenation operator
q	The order of the underlying finite field F_q
E	A suitably chosen Elliptic curve defined over F_q
P	A base point in the generator point E
n	The prime order of P
O	The point at infinity, where $nP = O$ and $P \neq O$

3.4.2 Registration Phase

When a new user U_i wants to register himself/herself with WSN, he/she needs to perform following steps:

- The user U_i selects an identifier ID_i, password PW_i and a random number N_i to compute masked password $MPW_i = h(PW_i||N_i)$. User U_i provides the identifier ID_i and masked password MPW_i to the base station BS via a secure channel.
- if the above request is accepted, the base station BS computes $A_i = h(h(ID_i||x_a)||MPWi)$, $B_i = h(ID_i||x_a) \bigoplus MPW_i$ and $C_i = h(x_a||K)$.
- Then BS issues a tamper-proof smart card with A_i, B_i, C_i and $h(.)$ stored in it.
- After receiving smart card, user enters N_i into the smart card.

3.4.3 Login Phase

When a user U_i wants to access real-time data from the WSNs, he/she needs to perform following steps:

- User U_i insert the smart card into the smart card reader then enters his/her identifier ID_i and password PW_i into the reader terminal. Smart card computes the masked password of the user U_i as $MPW_i^* = h(PW_i||N_i)$ and $a_i = B_i \bigoplus MPW_i^*$.
- Then it computes $A_i^* = h(a_i||MPW_i^*)$ and checks whether it is equal to the stored A_i. If they are equal smart card reader sends a *hello* massage to the BS. If not, then report wrong password PW_i to the user. This process performs up

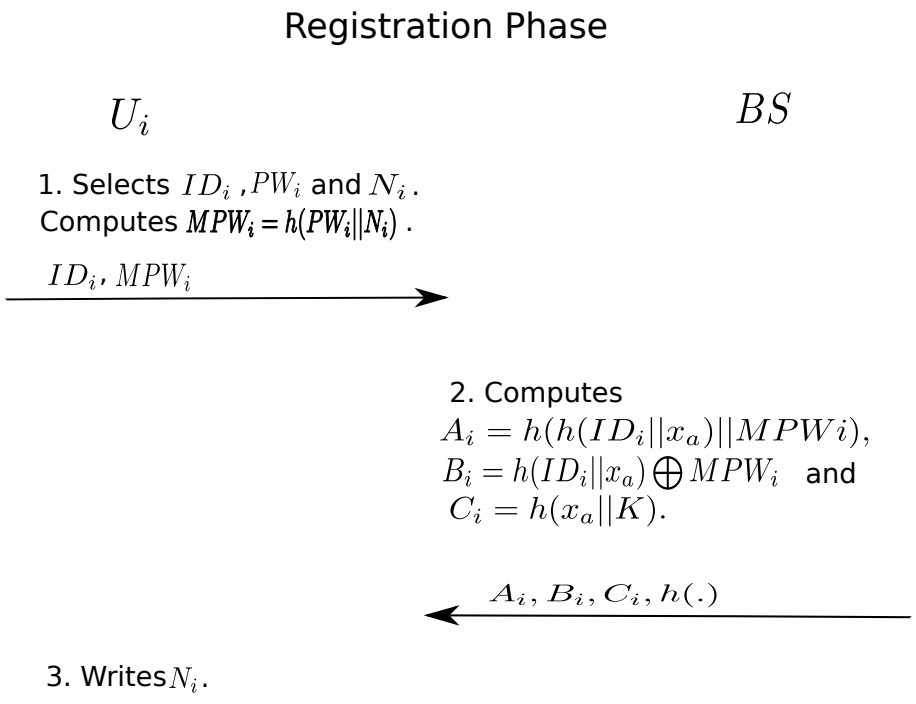

Figure 3.2: Registration Phase.

to some predefined number of times so that it can withstand password guessing attack by using stolen or lost smart.

- Upon receiving the *hello* message the BS sends a random nonce RN_1 to the reader.
- Then the reader computes $DID_i = ID_i \bigoplus h(C_i||RN_1)$ and selects a random number $\alpha\epsilon[2, n-2]$. After that it computes αP and $R_u = h(DID_i||\alpha P||a_i||RN_1)$.
- Smart card reader sends a message $< DID_i, \alpha P, R_u, RN_1 >$ to the base station BS.

3.4.4 Authentication Phase

When BS receives login message $< DID_i, \alpha P, R_u, RN_1 >$ from the user U_i, it perform s following step to authentication with the user U_i.

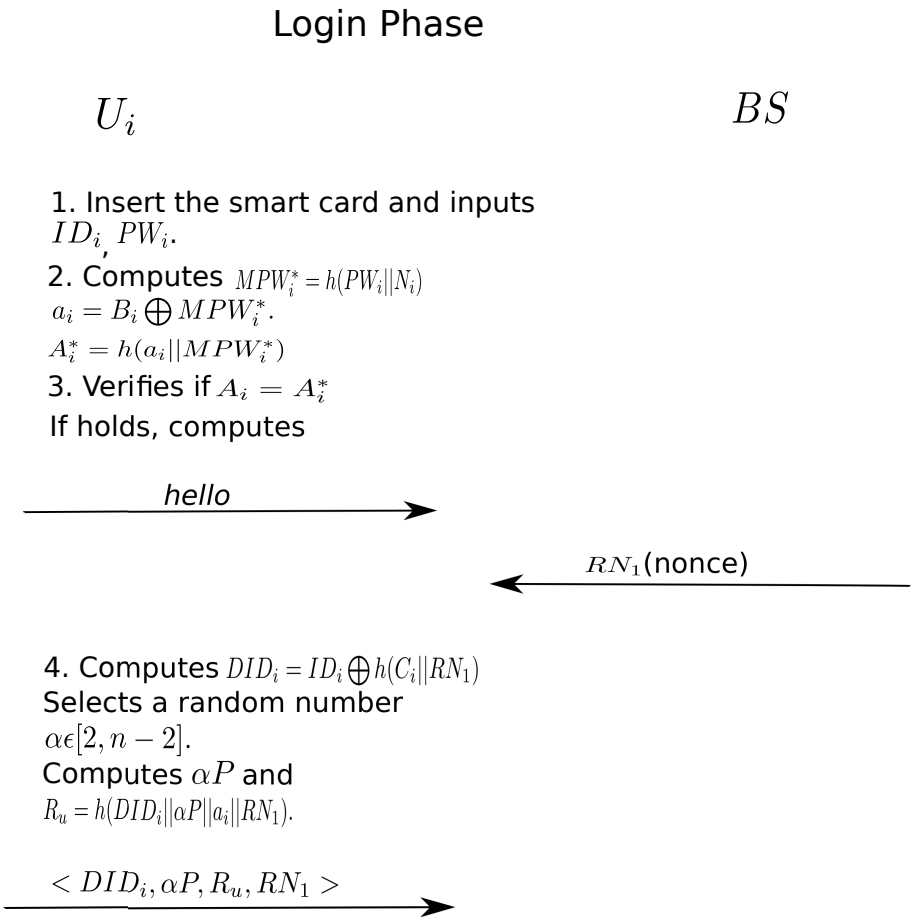

Figure 3.3: Login Phase.

- BS first checks whether received RN_1 is fresh. If it is fresh, then it computes $ID_i = DID_i \bigoplus h(h(x_a||K)||RN_1)$ and $a_i^* = h(ID_i||x_a)$ and use a_i^* to computes $R_u^* = h(DID_i||\alpha P||a_i^*||RN_1)$. Then it checks if $R_u = R_u^*$. If it holds, BS accepts the login request and proceeds to the next step.

- BS selects a cluster head nearest to the user. It retrieves *cntr* for that cluster head from its database. Then it computes $S_b = h(DID_i||ID_{CH_j}||x_{CH_j}||\alpha P||cntr)$.

- BS sends a message $< DID_i, \alpha P, S_b, cntr >$ to the corresponding cluster head CH_j.

- After receiving the message in previous step from BS, first CH_j checks whether received *cntr* is greater than or equal to the stored *cntr* in its memory. If yes then it computes $S_b^* = h(DID_i||ID_{CH_j}||x_{CH_j}||\alpha P||cntr)$. Then cluster head checks if $S_b = S_b^*$. If it holds, the cluster head accepts the login request and updates the previous *cntr* with received *cntr* and proceeds to the next step.

- Then it selects a random number $\delta\epsilon[2, n-2]$. After that it computes δP and $T_{CH_j} = h(DID_i||ID_{CH_j}||x_{CH_j}||\delta P||cntr)$ and session key $SK = \alpha\delta P$.

- The cluster head sends a message $< DID_i, ID_{CH_j}, \delta P, T_{CH_j}, cntr >$ to the base station.

- After receiving the message in previous step from the cluster head, BS checks whether the received *cntr* is equal to the saved *cntr* for that cluster head in its memory. If it is equal, then it computes $T_{CH_j}^* = h(DID_i||ID_{CH_j}||x_{CH_j}||\delta P||cntr)$ and checks if $T_{CH_j} = T_{CH_j}^*$. If it holds, then it accepts the request. Then BS increments *cntr* by one and proceeds to the next step.

- Then BS selects a random number $\gamma\epsilon[2, n-2]$. After that it computes γP, $z = \alpha\gamma P$ and $V_r = h(z||\gamma P||a_i||ID_{CH_j}||\delta P||RN_1)$.

- Then BS sends a message $< V_r, \gamma P, ID_{CH_j}, \delta P, RN_1 >$ to the user U_i.

- After receiving the message in previous step from the BS, the user U_i checks whether received RN_1 is equal to the RN_1 in its temporary memory. If they are equal, then smart card of user U_i computes $L = \alpha\gamma P$ and uses it to compute $V_r^* = h(L||\gamma P||a_i||ID_{CH_j}||\delta P||RN_1)$. Then it checks if $V_r = V_r^*$. If it holds, then smart card of U_i computes session key $SK = \alpha\delta P$.

The above generated session key is used in further communication between user U_i and cluster head CH_j.

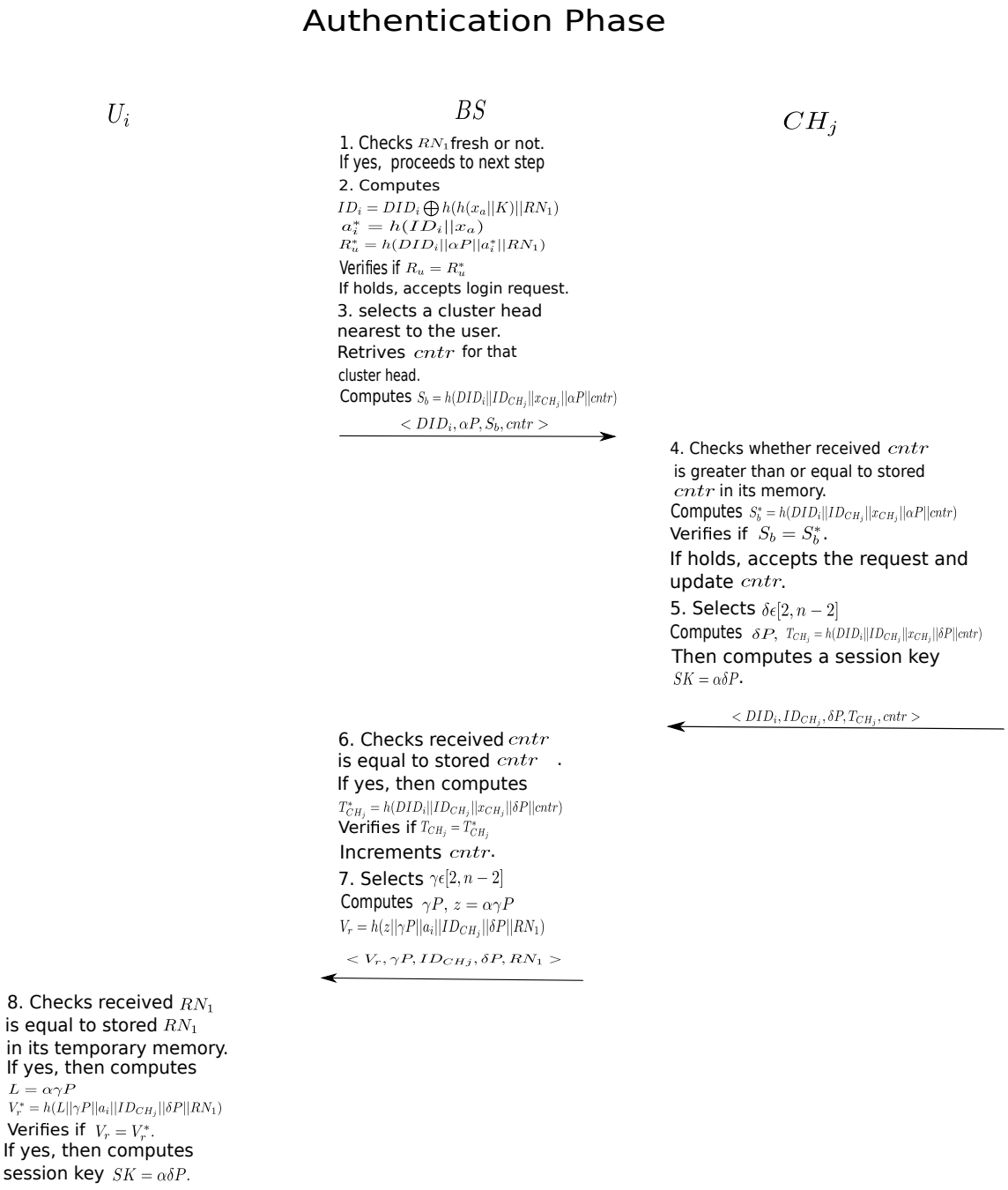

Figure 3.4: Authentication Phase.

3.4.5 Password Change Phase

Whenever a user U_i wants to change his/her password, he/she has to perform following steps. Here all steps are performed locally. Involvement of the base station

is not required.

- User U_i insert his/her smart card into the smart card reader. Then the reader terminal asks the user to insert his/her identifier ID_i, current password PW_i^{old}. After that smart card computes the masked value of current password as $MPW_i^{old} = h(PW_i^{old}||N_i)$, $a_i = B_i \bigoplus MPW_i^{old}$ and $A_i^* = h(a_i||MPW_i^{old})$.

- This computed A_i^* is compared with A_i, which is stored in the smart card. If they match, proceeds to next steps. If they do not match, then report wrong password PW_i to the user. This process performs up to some predefined number of times so that it can withstand password guessing attack by using stolen or lost smart card.

- Then it asks the user to enter a new password PW_i^{new}. Then it computes the masked value of the new password as $MPW_i^{new} = h(PW_i^{new}||N_i)$. Then it computes $A_i^{new} = h(a_i||MPW_i^{new})$ and $B_i^{new} = a_i \bigoplus MPW_i^{new}$.

- Finally, the stored A_i and B_i are replaced with A_i^{new} and B_i^{new} respectively in the smart card memory.

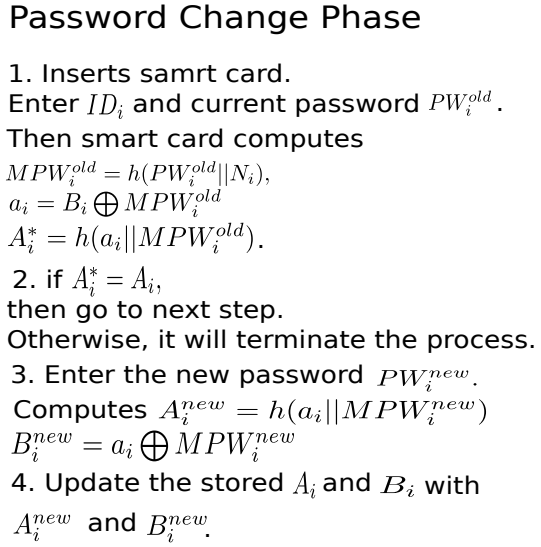

Figure 3.5: Password Change Phase.

3.4.6 Dynamic Node Addition

In a wireless sensor network, there are chances that some sensor nodes or cluster heads are captured by the attackers, or they expire due to energy consumption. In that situation, new nodes are added to the network. In this proposed scheme as there is no common parameter shared between the users and cluster head as well as users and sensor nodes, so any number of nodes can be added to the network freely at any time. Here the same smart card is used to perform authentication with newly added cluster heads.

3.5 Summary

In this chapter, a user authentication scheme based on elliptic curve cryptography for large scale hierarchical wireless sensor network is presented. The proposed scheme applies ECC to establish a session key between user and cluster head. This also facilitates option for password change and dynamic node addition.

Chapter 4

Analysis of Proposed Scheme

4.1 Introduction

In this chapter, we have analysed the proposed scheme in terms of security and compares the computation time of the proposed scheme with other related schemes. In security analysis, we consider various attacks like privileged insider attack, replay attack, guessing attack, stolen verifier attack, man-in-the-middle attack, DoS attack, password change attack, many logged-in users with same login-id attack, smart card breach attack, masquerade attack. Other criteria like mutual authentication, use anonymity and resiliency against node capture attack are also considered. Then in computation cost comparison section, computation cost of the proposed scheme is compared with other related schemes.

The rest of this chapter is organized as follows. The Section 4.2 shows the security analysis of the proposed scheme Then the Section 4.2 shows the security and computation comaprison of the proposed scheme with other related schemes. Finally, in Section 4.4, We summarised the chapter.

4.2 Security Analysis

This section analyzes security of the proposed scheme which is based on security of ECC described in Section 3.3 and difficulties associated with one-way hash function. This proposed scheme can resist against the following attacks.

Privileged insider attack

In this scheme, the user does not send his/her password in plain text during registration. Here the password PW_i is first masked to produce MPW_i, which is $h(PW_i||N_i)$. It is computationally infeasible to find PW_i from MPW_i due to one way property of the hash function. So the privileged insider of the base station cannot know the password PW_i. Thus he/she cannot impersonate the user in those servers where the user might have registered himself/herself with the same password. So this proposed scheme is resistance to the privileged insider attack.

Replay attack

In case of replay attack, a legal entity's transmitted message is intercepted and that message is replayed later by an adversary. However, in this scheme, a random nonce is used to restrict replay message between user and base station and a *cntr* or a counter is used to restrict replay message between base station and cluster head.

Guessing attack

Consider the situation where a user lost his/her smart card, and it is found by an attacker or is stolen by an attacker. In that case, the attacker cannot impersonate that user by using the smart card because no one can find the password from the B_i without knowing the value of secrete x_a, which is only known to base station. This secret is also protected by cryptographic one-way hash function. The shared secret a_i between U_i and BS is also protected in R_u and V_r by same cryptographic one-way hash function. So this scheme is resistance to guessing attack.

Stolen verifier attack

As this scheme does not keep any password/verifier table at the base station or cluster head, so no one can steal password/verifier table. So it is resistance to stolen verifier attack. Here even in registration phase user does not send password directly

to the BS. It is masked and sent to the base station to produce smart card. Then the masked password is deleted from temporary memory of base station.

Man-in-the-middle attack

Suppose an attacker intercept a login request message $< DID_i, \alpha P, R_u, RN_1 >$, then it generates a random number α^* and computes $\alpha^* P$, which is later used to generates session key. However, it cannot modify the login request message to $< DID_i, \alpha^* P, R_u^*, RN_1 >$ as the attacker does not know the secret x_a, which is used to calculate R_u. Thus man-in-the-middle attack is not possible in this proposed scheme.

Mutual authentication

In case of mutual authentication, both entities in a communication link authenticate to each other. In this proposed scheme, mutual authentication is assured between cluster head (CH) and base station (BS) as well as user and BS. Here first BS is authenticated to CH_j using $S_b = h(DID_i||ID_{CH_j}||x_{CH_j}||\alpha P||cntr)$. S_b can be computed only by CH_j and BS as the secret x_{CH_j} is known exclusively to CH_j and BS. Similarly CH_j is authenticated to BS using $T_{CH_j} = h(DID_i||ID_{CH_j}||x_{CH_j}||\delta P||cntr)$.

The user is authenticated to BS by using $R_u = h(DID_i||\alpha P||a_i||RN_1)$ likewise, BS is authenticated with the user using $V_r = h(z||\gamma P||a_i||ID_{CH_j}||\delta P||RN_1)$. Only legitimate user who has the correct password can only extract a_i and hence can compute R_u. Similarly BS can compute V_r as it has the secret x_a which is used to compute a_i.

DoS attack

Suppose an adversary has found or stole the smart card of a legitimate user U_i. However, in this proposed scheme, the smart card computes $A_i^* = h(h(ID_i||x_a)||h(PW_i||Ni))$ and compares it with the stored value of A_i in smart card's memory. This comparison will show the validity of user identity ID_i and password PW_i before the password updates procedure. But the adversary cannot guess both user identity ID_i and password PW_i correctly in polynomial time. If

login failure exceeds some predefined number of times, then the smart card will be locked immediately. Thus the proposed scheme is secure against denial of service attack.

Password change attack

This scheme is resistance to password change attack. Suppose for a stolen smart card if the attacker wants to change password he/she still must know the old password PW_i^{old}. Smart card allows a predefined number of times to enter correct the old password. If the attacker fails to enter the old password correctly, then that smart card is blocked.

User anonimity

In this proposed scheme, in each login request user anonymity is preserved. Consider a situation, where an attacker has intercepted a login request message $< DID_i, \alpha P, R_u, RN_1 >$. But it cannot retrieve any static parameter from this message as all the values here are session dependent. Only base station can find ID_i from the DID_i as it has the knowledge of secret parameter x_a and its symmetric key K. Hence in the presented scheme, an intruder or attacker cannot identify the user trying to login.

Many logged-in user with same login-id attack

This scheme can prevent the risk of many logged-in users with the same login ID as well as parallel session attack. Here login process starts only when the user inserts his/her card into the card reader, and all computations is performed only during the period when the card is still inside the card reader. Once the card is removed the login process is terminated.

Smart card breach attack

Suppose a smart card is lost or stolen. Although it is assumed that a smart card cannot be cracked, an adversary may perform side channel attacks, including differential power analysis and invasive attack and extract parameters like A_i, B_i, C_i and N_i. Then the adversary tries to impersonate the user to login to the Base Station. For that purpose, adversary must be able to create a valid login request

message $< DID_i, \alpha P, R_u, RN_1 >$. Here $R_u = h(DID_i||\alpha P||a_i||RN_1)$ and to compute a_i the adversary must have knowledge of either MPW_i or x_a. But adversary cannot find MPW_i as he does not have knowledge of PW_i and he also cannot extract x_a from the C_i as it is protected by one-way hash function. Thus, the proposed scheme can resist smart card breach attack.

Resilience against node capture attack

As sensor nodes and cluster heads are deployed in a hostile environment, those nodes can easily capture by an adversary. So the adversary can steal the stored secret information in those nodes. Suppose some cluster heads are captured by an attacker. So the attacker knows the secret x_{CH_j} stored in the cluster head. As x_{CH_j} for each cluster head is different, and they are stored in the cluster heads before deployment, so only those cluster heads will send false data to the user. However, other non-compromised nodes will continue to communicate securely with the users. It means, if some captured cluster heads are compromised, then that does not affect secure communication between other non-compromised cluster heads and users. So this scheme is resilience against node capture attack.

Masquerade attack

Suppose an adversary wants to impersonate himself as a legal user to the WSN. Then he must compute a valid DID_i and R_u which will be sent to base station with the login request. However, $DID_i = ID_i \bigoplus h(C_i||RN_1)$ and $R_u = h(DID_i||\alpha P||a_i||RN_1)$ where $C_i = h(x_a||K)$ and $a_i = h(ID_i||x_a)$. Only the base station has the knowledge of secret x_a and symmetric key K. So the adversary cannot create a valid DID_i and R_u as he does not know the value of x_a and K. So this scheme is resistance to masquerade attack.

4.3 Comparison with Related Schemes

In this section, the performance of the proposed scheme is compared with some selected existing related schemes: Watro et al. [11] scheme, Wong et al. [17] scheme,

ML Das [14] scheme, Nyang and Lee [23] scheme, Khan and Alghathbar [25] scheme, Kumar et al. [29] scheme, Fan et al. [30] scheme and Xue et al. scheme [31].

In Table 4.1, the comparison of the security features among different schemes is presented. Here it shows that the proposed scheme is stronger in terms of security features. Our scheme along with Watro et al. [11] and Khan and Alghathbar [25] provides protection against privileged-insider attack. Password change or update feature is supported by our scheme, Khan and Alghathbar [25] and Kumar et al. [29] scheme whereas only our scheme is resilient against node capture attack. Mutual authentication is supported by our scheme, Watro et al. [11], Nyang and Lee [23] and Fan et al. [30] scheme and Xue et al. scheme [31]. Only our scheme, Nyang and Lee [23], Fan et al. [30] scheme and Xue et al. scheme [31] establishes secret session key between the user and sensor/cluster head. Only our scheme provides an option for dynamic node addition. In our scheme time synchronization is not needed to provide protection against replay attack.

In Table 4.2, the comparison of computational cost in different phases of the proposed scheme with other schemes is given. Here the computation cost for XOR is not considered as it is negligible. This scheme uses cluster head to authenticate with user and cluster head is more resource-rich compared to usual sensor node. This scheme uses the advantage of using computational power of base station and cluster head to provide more secure login to a user.

Table 4.1: Comparison of enhanced security features of the proposed scheme with other schemes

Security Feature	Proposed Scheme	Watro et al.	Wong et al.	Das	Nyang and Lee	Khan and Alghathbar	Kumar et al.	Fan et al.	Xue et al.
S_1	Yes	Yes	No	No	No	Yes	No	No	No
S_2	Yes	No	No	No	No	Yes	Yes	No	No
S_3	Yes	Yes	No	No	Yes	Partial	Partial	Yes	Yes
S_4	Yes	No	No	No	No	No	No	No	No
S_5	Yes	No	No	No	Yes	No	No	Yes	Yes
S_6	Yes	No	No	No	No	No	No	No	No
S_7	Yes	Yes	No	No	No	No	No	No	No

S_1: Privileged Insider Attack; S_2: Support Password Change; S_3: Mutual Authentication; S_4: Resilient Against Node Capture; S_5: Provide Secret Session Key; S_6: Support Dynamic Node Addition; S_7: Resistance to Time Synchronization

Table 4.2: Comparison of computational cost in different phases of proposed scheme with other schemes

Phase	Entity	Proposed Scheme	Watro et al.	Wong et al.	Das	Nyang and Lee	Khan and Alghathbar	Kumar et al.	Fan et al.	Xue et al.
Registration	User	T_h	$T_{pu} + T_{pr}$	-	-	-	T_h	-	-	$2T_h$
	BS	$3T_h$	-	$3T_h$	$3T_h$	$3T_h$	$2T_h$	$3T_h$	$6T_h$	$9T_h$
	Sensor	-	-	-	-	-	-	-	-	$3T_h$
	CH	-	-	-	-	-	-	-	-	-
Login + Authentication	User	$5T_h + 3T_{em}$	$2T_{pr} + T_h$	-	$4T_h$	$4T_h + 2T_{kdf} + T_{mac} + T_{dec}$	$4T_h$	$4T_h$	T_h	$10T_h$
	BS	$7T_h + 2T_{em}$	-	T_h	$4T_h$	$3T_h + 2T_{kdf} + T_{enc} + T_{mac}$	$5T_h$	$5T_h$	$2T_h$	$13T_h$
	Sensor	-	$2T_{pu} + T_h$	$3T_h$	T_h	$2T_{kdf} + 2T_{mac} + T_{dec} + T_{enc}$	$2T_h$	$2T_h$	$2T_h$	$6T_h$
	CH	$2T_h + 2T_{em}$	-	-	-	-	-	-	$8T_h$	-

T_h: hash computation; T_{em}:elliptic curve point multiplication; T_{pu}:public-key computation; T_{pr}:private-key computation; T_{kdf}:key derivation computation; T_{mac}:message authentication code computation; T_{enc}:symmetric-key encryption; T_{dec}:symmetric-key decryption

Lastly considering computation cost at sensor node/cluster head, the proposed scheme uses two hash operation and two elliptic curve multiplication in the whole authentication process. As cluster heads have more computing power and energy resources so above operations are feasible. The proposed scheme is also stronger than other scheme in term of security. It includes six message transfers in the whole authentication process. The first two messages are to receive random nonce from the base station. This random nonce helps this scheme from time synchronization problem which is a very difficult task in case of WSN.

4.4 Summary

In this chapter, we have done security analysis of the proposed scheme and compare security features of our scheme with other existing schemes. Then the comparison of computational cost in different phases of the proposed scheme with other schemes is shown. Considering over-all scenarios this scheme is better than all other schemes. The scheme is also scalable in terms of user addition, cluster head addition and sensor node addition.

Chapter 5

Conclusion and Future Work

5.1 Conclusion

In this thesis, a user authentication scheme based on elliptic curve cryptography for large scale hierarchical wireless sensor network is presented. Here feasibility of ECC in context of WSN is demonstrated. The proposed user authentication scheme can address all the problems of the former schemes and provide better security. This scheme allows the user to authenticate at both the base station and the cluster heads inside WSN. It provides mutual authentication between user and base station as well as base station and cluster head. The proposed scheme also provides the option for dynamic node addition where there is no need to update any information in user smart card for accessing real-time data for any addition or replacement of cluster heads in the networks. After successful authentication, both user and cluster head from which data will be forward to the user, will be able to establish a secrete session key between them. Later using this session key, the user can contact the cluster head for real-time data inside WSN. This scheme implements merit of using ECC-based mechanism in WSN and enhances the WSN authentication with higher security than other protocols.

5.2 Future Work

For future work, we suggest to do improvement of the protocol by adding access rights of different users along with the authentication.

Bibliography

[1] Youssou Faye, Ibrahima Niang, and Thomas Noel. A survey of access control schemes in wireless sensor networks. *Proc. World Acad. Sci. Eng. Tech*, 59:814–823, 2011.

[2] Yi Cheng and Dharma P Agrawal. An improved key distribution mechanism for large-scale hierarchical wireless sensor networks. *Ad Hoc Networks*, 5(1):35–48, 2007.

[3] Ian F Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. Wireless sensor networks: a survey. *Computer networks*, 38(4):393–422, 2002.

[4] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary. Wireless sensor network security: A survey. *Security in distributed, grid, mobile, and pervasive computing*, 1:367, 2007.

[5] David W Carman, Peter S Kruus, and Brian J Matt. Constraints and approaches for distributed sensor network security (final). *DARPA Project report,(Cryptographic Technologies Group, Trusted Information System, NAI Labs)*, 1:1, 2000.

[6] Ian F Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. A survey on sensor networks. *Communications magazine, IEEE*, 40(8):102–114, 2002.

[7] John A Stankovic, TE Abdelzaher, Chenyang Lu, Lui Sha, and Jennifer C Hou. Real-time communication and coordination in embedded sensor networks. *Proceedings of the IEEE*, 91(7):1002–1022, 2003.

[8] Adrian Perrig, Robert Szewczyk, JD Tygar, Victor Wen, and David E Culler. Spins: Security protocols for sensor networks. *Wireless networks*, 8(5):521–534, 2002.

[9] Zinaida Benenson, Felix Gartner, and Dogan Kesdogan. User authentication in sensor networks. In *Informatik 2004, Workshop on Sensor Networks*, 2004.

[10] Rehana Yasmin. *An efficient authentication framework for wireless sensor networks*. PhD thesis, University of Birmingham, 2012.

[11] Ronald Watro, Derrick Kong, Sue-fen Cuti, Charles Gardiner, Charles Lynn, and Peter Kruus. Tinypk: securing sensor networks with public key technology. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pages 59–64. ACM, 2004.

[12] Ronald L Rivest, Adi Shamir, and Len Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[13] Whitfield Diffie and Martin Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644–654, 1976.

[14] Manik Lal Das. Two-factor user authentication in wireless sensor networks. *Wireless Communications, IEEE Transactions on*, 8(3):1086–1090, 2009.

[15] Zinaida Benenson, Nils Gedicke, and Ossi Raivio. Realizing robust user authentication in sensor networks. *Real-World Wireless Sensor Networks (REALWSN)*, 14, 2005.

[16] A Mnif, O Cheikhrouhou, and M Ben Jemaa. An id-based user authentication scheme for wireless sensor networks using ecc. In *Microelectronics (ICM), 2011 International Conference on*, pages 1–9. IEEE, 2011.

[17] Kirk HM Wong, Yuan Zheng, Jiannong Cao, and Shengwei Wang. A dynamic user authentication scheme for wireless sensor networks. In *Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on*, volume 1, pages 8–pp. IEEE, 2006.

[18] Satyajit Banerjee and Debapriyay Mukhopadhyay. Symmetric key based authenticated querying in wireless sensor networks. In *Proceedings of the first international conference on Integrated internet ad hoc and sensor networks*, page 22. ACM, 2006.

[19] Carlo Blundo, Alfredo De Santis, Amir Herzberg, Shay Kutten, Ugo Vaccaro, and Moti Yung. Perfectly-secure key distribution for dynamic conferences. In *Advances in cryptologyCRYPTO92*, pages 471–486. Springer, 1993.

[20] Canming Jiang, Bao Li, and Haixia Xu. An efficient scheme for user authentication in wireless sensor networks. In *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*, volume 1, pages 438–442. IEEE, 2007.

[21] Huei-Ru Tseng, Rong-Hong Jan, and Wuu Yang. An improved dynamic user authentication scheme for wireless sensor networks. In *Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE*, pages 986–990. IEEE, 2007.

[22] Ashok Kumar Das, Pranay Sharma, Santanu Chatterjee, and Jamuna Kanta Sing. A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. *Journal of Network and Computer Applications*, 2012.

[23] DaeHun Nyang and Mun-Kyu Lee. Improvement of das's two-factor authentication protocol in wireless sensornetworks. *AvailableOnline: http://eprint. iacr. org/2009/631. pdf/(accessed on 07 July 2010)*, 2009.

[24] Sang Guun Yoo, Keun Young Park, and Juho Kim. A security-performance-balanced user authentication scheme for wireless sensor networks. *International Journal of Distributed Sensor Networks*, 2012, 2012.

[25] Muhammad Khurram Khan and Khaled Alghathbar. Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks. *Sensors*, 10(3):2450–2459, 2010.

[26] Daojing He, Yi Gao, Sammy Chan, Chun Chen, and Jiajun Bu. An enhanced two-factor user authentication scheme in wireless sensor networks. *Ad Hoc & Sensor Wireless Networks*, 10(4):361–371, 2010.

[27] Omar Cheikhrouhou, Anis Koubaa, Manel Boujelben, and Mohamed Abid. A lightweight user authentication scheme for wireless sensor networks. In *Computer Systems and Applications (AICCSA), 2010 IEEE/ACS International Conference on*, pages 1–7. IEEE, 2010.

[28] Huei-Ru Tseng, Rong-Hong Jan, and Wuu Yang. A robust user authentication scheme with self-certificates for wireless sensor networks. *Security and Communication Networks*, 4(8):815–824, 2011.

[29] Pardeep Kumar, Mangal Sain, and Hoon Jae Lee. An efficient two-factor user authentication framework for wireless sensor networks. In *Advanced Communication Technology (ICACT), 2011 13th International Conference on*, pages 574–578. IEEE, 2011.

[30] Rong Fan, Dao-jing He, Xue-zeng Pan, et al. An efficient and dos-resistant user authentication scheme for two-tiered wireless sensor networks. *Journal of Zhejiang University SCIENCE C*, 12(7):550–560, 2011.

[31] Kaiping Xue, Changsha Ma, Peilin Hong, and Rong Ding. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. *Journal of Network and Computer Applications*, 2012.

[32] Ding Wang and Chun guang Ma. On the (in)security of some smart-card-based password authentication schemes for wsn. Cryptology ePrint Archive, Report 2012/581, 2012. `http://eprint.iacr.org/`.

[33] Sheetal Kalra and Sandeep K Sood. Elliptic curve cryptography: survey and its security applications. In *Proceedings of the International Conference on Advances in Computing and Artificial Intelligence*, pages 102–106. ACM, 2011.

[34] Haodong Wang, Bo Sheng, Chiu C Tan, and Qun Li. Public-key based access control in sensornet. *Wireless Networks*, 17(5):1217–1234, 2011.

[35] Arvinderpal S Wander, Nils Gura, Hans Eberle, Vipul Gupta, and Sheueling Chang Shantz. Energy analysis of public-key cryptography for wireless sensor networks. In *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*, pages 324–328. IEEE, 2005.

[36] Lawrence C Washington. *Elliptic curves: number theory and cryptography*, volume 50. Chapman and Hall/CRC, 2008.

[37] Behrouz A Forouzan. *Cryptography & Network Security*. McGraw-Hill, Inc., 2007.

[38] Fagen Li, Xiangjun Xin, and Yupu Hu. Indentity-based broadcast signcryption. *Computer Standards & Interfaces*, 30(1):89–94, 2008.

[39] Moni Naor and Moti Yung. Universal one-way hash functions and their cryptographic applications. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 33–43. ACM, 1989.

[40] Jason Hill, Robert Szewczyk, Alec Woo, Seth Hollar, David Culler, and Kristofer Pister. System architecture directions for networked sensors. In *ACM SIGOPS operating systems review*, volume 34, pages 93–104. ACM, 2000.

Dissemination

- **Rakesh Maharana** and Pabitra Mohan Khilar, "An Improved Authentication Protocol for Hierarchical Wireless Sensor Networks using ECC "International Journal of Computer Applications 67(22):23-30, April 2013.