

A Lightweight Authentication Protocol based on ECC for Satellite Communication

A Dissertation-2 report submitted in partial fulfillment of the requirements for
the award of the degree of

Masters of Electronics and Communication

by

Thokchom Saroj(11507024)



**Lovely Professional University Jalandhar Delhi G. T Road (NH-1),
Phagwara, Punjab, 144402, India**

2017

DECLARATION

I hereby certify that the work, which is being presented in the Thesis report entitled **A Lightweight Authentication Protocol based on ECC for Satellite Communication**, in partial fulfillment of the requirement for the award of the Degree of Master of Electronics and communication submitted to the institution is an authentic record of my own work Carried out during the period January to May under the supervision of **MR. GURJOT SINGH**. I also cited the reference about the text/figure/table from where they have been taken.

Date:

Signature of the Candidate

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

Date:

Signature Supervisor

ACKNOWLEDGEMENT

First, I would like to express my best regards to my thesis guide **MR. GURJOT SINGH**, whose valuable guidance, encouragement and provision of necessary facilities made this work possible.

I would also like to express my gratitude towards the **LOVELY PROFESSIONAL UNIVERSITY** for providing me with the best facilities and proper environment to work on my project

Finally, I offer my great thanks to my family for their support which helped me through the difficulty and hardships of life to earn this achievement.

ABSTRACT

The satellite communication is the vast wireless network communication. Many entities in the world use this communication for broadcasting, messaging, telephony and others user s application. Since there are many users the satellite communication may suffer from various attacks. We Knows that the user authentication is the first safety priority needed in the network from attackers. For the satellite communication, a secure and lightweight authentication scheme is must necessary. So a user authentication scheme is proposed based on elliptical curves cryptography and Kerberos for the satellite communication. The proposed scheme ensures that the mutual authentication and secure ticket-granting service can be accomplished. The security analysis implement that the proposed scheme is free from various attacks, including internal and external attacks. And also the performance analysis brings to a good conclusion that our proposed scheme result is similar or improves from the existing user authentication schemes.

TABLE OF CONTENT	PAGE NO.
PAC	.. i
DECLARATION	.. ii
ACKNOWLEDGEMENT	iii
ABSTRACT	.. iv
LIST OF FIGURE	.. vii
LIST OF TABLES	... viii
CHAPTER 1 INTRODUCTION	1-17
1.1 Overview of Satellite Communication	. 1
1.2 Objectives of Satellite Communication	2
1.3 Challenges in Satellite Communication	... 2-3
1.4 Need of Authentication in Satellite Communication	3-4
1.5 ECC Diffie-Hellman Key Exchange Protocol 4-5
1.6 Kerberos Protocol	5
1.6.1 The Authentication Service Exchange Phase...	5-6
1.6.2 The Ticket-Granting Service Exchange Phase.	5-6
1.6.3 The Client/Server Service Exchange Phase	. 6-7
1.7 Overview of HMAC	7
CHAPTER 2 LITERATURE REVIEW	.. 8-10
CHAPTER 3 SCOPE OF STUDY	11
CHAPTER 4 PROBLEM FORMULATION	. 12
CHAPTER 5 OBJECTIVES	13
CHAPTER 6 RESEARCH METHODOLOGY	. 14-18
6.1 Proposed Model	. 14-15
6.2 The Proposed User Authentication Protocol	. 15-16
6.2.1 The Authentication Service Exchange Phase	. 16
6.2.2 Ticket-Granting Service Exchange Phase	.. 17

6.2.3 The Client/Server Service Exchange Phase	. 18
CHAPTER 7 RESULTS AND DISCUSSION	. 19-23
6.1 Security Analysis	19-23
6.2 Performance Analysis	. 23
CHAPTER 7 CONCLUSION	24
REFERENCES	... 25-26
BIBLIOGRAPHY	.. 27
APPENDIX-1	. 28
Complete Work Plan with Time	
APPENDIX-2	. 29
Autobiography	

LIST OF FIGURES

FIGURE NUMBER	FIGURE CAPTION	PAGE NUMBER
1.1	Satellite communication	1
1.4.1	Satellite authentication scenario	3
6.1	The proposed model authentication	14
6.2.1	The authentication service exchange phase	16
6.2.2	The ticket-granting service exchange phase	17
6.2.3	The client/server authentication phase	18

LIST OF TABLES

TABLE NUMBER	TABLE CAPTION	PAGE NUMBER
1	Requirement of the presented protocol	14-15
2	The functionality comparison	23

1.1 Overview of Satellite Communication

The modernized satellite communication network is a wireless communication network technology, which has vast coverage to the entire world and allows all the users to remain connected almost everywhere on the earth station. When electromagnetic signal is transmitted towards the satellite then, the satellite intensify the signal and transmitted back to the receiver ground station. The satellite communicates with the ground station through the medium of air, so it is easy for the attackers to steal or falsify the transmitted [2][5]. The Fig. 1.1 shows the concepts of how satellite communication is performed.

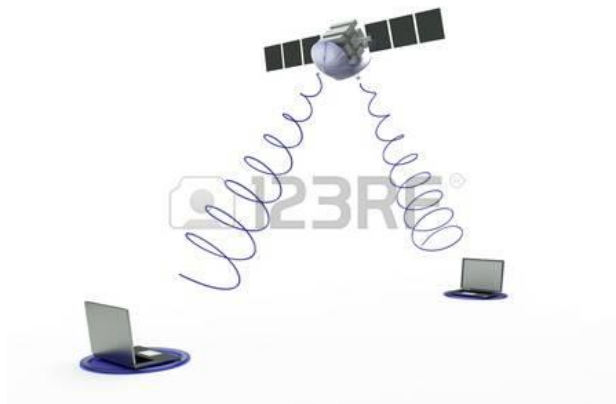


Fig. 1.1 Satellite communications

The satellite communications mainly involves four steps:

- i) Firstly, the earth station or the ground station transmits the desired signal to the satellite.
- ii) The satellite amplifies the incoming signal and changes the frequency.
- iii) The satellite transmits the signal back to the Earth.
- iv) The ground station then receives the signal.

The satellite communication is performed in two phases namely the uplink and the downlink process. The uplink process is between the transmitter and the satellite, and the downlink communication is between the receiver station and the satellite [1-4].

1.2 Objectives of Satellite Communication

The modernized satellite communication network is a wireless communication network technology, which has vast coverage to the entire world and allows all the users to remain connected almost everywhere on the earth station. The satellite communication provides many application areas including

- i) Weather forecasting: Many satellites are designed to continuously examine and predict the weather conditions of the earth.
- ii) Military: In military satellites are used to obtain intelligence information.
- iii) Radio and TV broadcast: For this purpose many satellites are employed to broadcast world news, live matches and radio services.
- iv) Navigation: Some satellites are employed to detect the location of a particular place or target and are mainly used for ships and aircrafts.
- v) Remote areas: For long distance communication it is impossible to have wired line connection to the telephone network or the internet. Since the satellite can cover world-wide communication and the medium is air. Hence the satellite is mainly used for connecting remotes areas.
- vi) Space science: Satellites are also employed to have the knowledge of space science and technology experiments.

The main objective of satellite communication is to provide world-wide communication around the globe and to provide good quality of service [4].

1.3 Challenges in Satellite Communication

Even though satellite communication is a global network communication, there are certain challenges faced by the satellite communication [4].

- i) **Battery:** The lifetime of the satellite is quite low since the satellites have limited storage of energy.
- ii) **Size:** Since the satellites have fixed weight and limited inner structure, this in turn limits the functionality of the satellite.
- iii) **Authentication:** In satellite communication the transmission of information is with direct line of sight. As the medium is air, any person or hacker can easily detect or capture the information. So there is a great need of authentication in satellite communication.
- iv) **Bandwidth:** To have better transmission of data the channel bandwidth of the satellite communication increases, this in turn leads to increase noise in a large scale.
- v) **Environment:** whenever there is cloudy or very high rainfall or snowy, the satellite or the earth station unable to transmit or receive the information due to disturbance in the medium.

1.4 Need of Authentication in Satellite Communication

Since the usage of satellite services increases the security becomes one of the most major concern areas. When security is mentioned the user authentication is the first safety barrier in the wireless communication. So authentication is must necessary for all communication system.

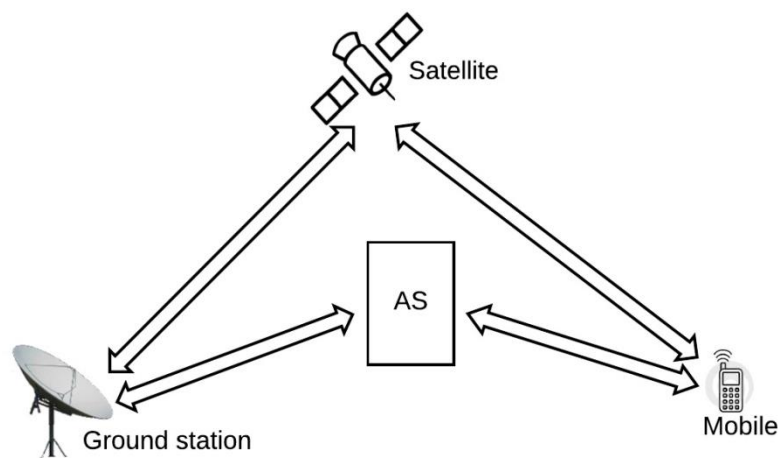


Fig. 1.4.1 Satellite authentication scenario

As shown in Fig. 1.4.1, in the satellite communication the authentication is provided by the authentication server that is the gateway to the satellite server. According to the figure both the

ground station and the mobile are the satellite service users, so authentication operation has to be performed prior to access to the satellite network in order to avoid from intruders. Authentication is an entity that helps the user to proof his or her identity is true to the system. It helps the user identity to protect from outside attackers. And also it provides common platform between the users. No other person can join the system without the proper authentication license. The authentication process is done as follows: (1) At first the user identity database containing all the user information is created within the authentication server; (2) Secondly if a person wants to access the system, his or her identity is compare with the information contained in the database. If the information is correct then the intended person is allowed to access the system. Suppose if there is no authentication scheme in the satellite communication. There may be some threat in the system like: (1) A user may try to access a specific workstation and may act as different user from that workstation; (2) a user may change the IP address of a workstation and the request will be coming from the impersonated workstation; (3) A user may capture the message exchange and disrupt the services by using replay attacks. So in all of this threat an uncertified user may be able to way in the service and data that he or she is not allowed to way in. Therefore authentication is the first priority security entities in the communication [15].

1.5 ECC Diffie-Hellman Key Exchange Protocol

This protocol exchanged secret key between the users so as to have secure communications. The operation of this key exchange protocol is performed on the ECC computation [22-23]. Since this protocol has small key size so it minimized the storage burden. The requirements of the ECC parameters for secret key exchange protocol are:

- i) The ECC parameters are ‘a’, ‘b’, and ‘q’, where ‘q’ is the prime number.
- ii) The point ‘G’ on the elliptical curve whose order is ‘n’.

The dialogue of secret key exchange protocol is performed as

- i) Consider Dev and Raj wants to exchange information, so a secret key is necessary to exchange information in order to protect from intruders.
- ii) At first Dev and Raj select their own private key which is less than ‘n’.

$$Dev \quad d(\text{private key}) < n$$

$$Raj \quad r(\text{private key}) < n$$

iii) Both Dev and Raj calculate public key and the public key is exchange between them.

$$P_d(\text{dev public key}) = d \times G$$

$$P_r(\text{dev public key}) = r \times G$$

iv) Now Dev calculate shared secret key as

$$K(\text{secret key}) = d \times P_r = d \times r \times G$$

v) Also Raj calculate shared secret key as

$$K(\text{secret key}) = d \times P_d = d \times r \times G$$

This protocol is a concept of cryptography. From this protocol we came to know that a secure communication can be performed using the shared secret key exchange mechanism.

1.6 Kerberos Protocol

Kerberos is the protocol which provides user authentication mechanism. Kerberos protocol is mainly established to have reliability, scalability, secure, and transparent in the communication system. The main purpose of Kerberos is to provide a centralized authentication server, whose main purpose is to authenticate user to servers and servers to users. The Kerberos version5 mechanism utilized the ticket granting-service system to way in to the server so as to obtain desired service [15] [18][20]. There are three phases of the Kerberos authentication mechanism. The three phases are discussed below:

1.6.1 The Authentication Service Exchange Phase

This phase allows the user to authenticate his or her identity to the authentication server and the server will generate a ticket, which proof that the user is the legitimate user that can way in to the TGS [15]. The exchange of information is as follows:

Message1. Client → Authentication server:

$$\text{Options} \parallel \text{ID}_c \parallel \text{Realm}_c \parallel \text{ID}_{\text{TGS}} \parallel \text{Times} \parallel \text{Nonce}_1 \quad (1)$$

When the user with ID_c , wants to join the system, he/she generates a nonce and request ticket for accessing the TGS, by sending the ID of the user's and the ID of the TGS to the authentication server.

Message2. Authentication server → Client:

$$\text{Realm}_c \parallel \text{ID}_c \parallel \text{Ticket}_{\text{tgs}} \parallel E(K_c, [K_{c,\text{tgs}} \parallel \text{Times} \parallel \text{Nonce}_1 \parallel \text{Realm}_{\text{tgs}} \parallel \text{ID}_{\text{tgs}}]) \quad (2)$$

$$\text{Ticket}_{\text{tgs}} = E(K_{\text{tgs}}, [\text{Flags} \parallel K_{c,\text{tgs}} \parallel \text{Realm}_c \parallel \text{ID}_c \parallel \text{AD}_c \parallel \text{Times}])$$

The authentication server verifies the information send by the client and generates $\text{Ticket}_{\text{tgs}}$ to allow accessible to TGS.

1.6.2 The Ticket-Granting Service Exchange Phase

This phase also allows the user to proof that he or she is a legitimate user to have ticket so as to access the server.

$$\text{Authenticator}_c = E(K_{c,\text{tgs}}, [\text{ID}_c \parallel \text{Realm}_c \parallel \text{TS}_1])$$

When the client request for service-granting ticket, it includes ID server, $\text{Ticket}_{\text{tgs}}$ and Authenticator_c .

Message3. Client \rightarrow TGS:

$$\text{Options} \parallel \text{ID}_v \parallel \text{Times} \parallel \text{Nonce}_2 \parallel \text{Ticket}_{\text{tgs}} \parallel \text{Authenticator}_c \quad (3)$$

Message4. TGS \rightarrow Client:

$$\text{Realm}_c \parallel \text{ID}_c \parallel \text{Ticket}_v \parallel E(K_{c,\text{tgs}}, [K_{c,v} \parallel \text{Times} \parallel \text{Nonce} \parallel \text{Realm}_v \parallel \text{ID}_v]) \quad (4)$$

$$\text{Ticket}_v = E(K_v, [\text{Flags} \parallel K_{c,v} \parallel \text{Realm}_c \parallel \text{ID}_c \parallel \text{AD}_c \parallel \text{Times}])$$

The TGS generates the service-granting ticket in order to way in to the server.

1.6.3 The Client/Server Authentication Exchange Phase

In this phase after the client proof that he or she is the intended user of the communication network, this in turn provides the user choice key ‘Subkey’ and the default key. With the help of these two key the user can use any service from the server.

Message5. Client \rightarrow Server:

$$\text{Options} \parallel \text{Ticket}_v \parallel \text{Authenticator}_c \quad (5)$$

$$\text{Authenticator}_c = E(K_{c,v}, [\text{ID}_c \parallel \text{Realm}_c \parallel \text{TS}_2 \parallel \text{Subkey} \parallel \text{Seq}])$$

The server cross-check the information sends by the client between the Ticket_v and the Authenticator_c, and if the information is correct then the server replies to client as:

Message6. Server → Client:

$$E(K_{c,v}, [TS_2 \parallel \text{Subkey} \parallel \text{Seq}]) \quad (6)$$

Now the client can operate a service from the server by using the secret key $K_{c,v}$ and also by the additional key known as Subkey, which is the user's choice key.

1.7 Overview of HMAC

Before understanding the concept of HMAC, first we have to know the basic function of MAC (Message Authentication Code). MAC is the cryptography algorithm that utilized the secret key. It takes variable length of message as input and with the secret key, produces an authentication code. MAC provides authentication and confidentiality with the help of symmetric key cryptosystem.

The formula of MAC is defined as

$$MAC = C(K, M)$$

where M is the input message, C is the MAC functions, and K is the shared secret key.

HMAC is nothing but it is just a MAC based Hash function, where hash function is applied to the MAC operation to obtain more secure mechanism for the exchange of information. There are some advantages of HMAC in design objectives:

- i) Easy replaceable.
- ii) To use hash function, which are freely and widely-available.
- ii) To use and handle key in a simple way.
- iv) To retain the original performance of the hash function.

Since HMAC design objectives are feasible, so the HMAC algorithm is quite useful in implementing the communication network security, which provides integrity, authentication and confidentiality.

CHAPTER 2

LITERATURE REVIEW

H. S. Cruickshank in 1996 titled '*A Security System for Satellite Networks*' which mainly focused on security network between the satellite and the user; and this scheme combined the public-key and secret-key cryptosystems in order to have mutual authentication between the users and the satellite, data encryption is also introduced in the authentication stage with the help of secret key algorithm, and also provided digital signatures. This paper utilized public-key technique for the initial authentication stage between the user and the satellite, and secret-key technique for encryption in the message exchange stage. Since the protocol better security, even if the private key of either the user or satellite is captured, the protocol will still be secure. Because it requires the compromise of both user and satellite private keys in order to detect the communications between the user and the satellite. And also this protocol provides end to end security [6].

M. S. Hwang.et.al in 2003 titled '*An Authentication Scheme for Mobile Satellite Communication Systems*' introduced a new scheme based on user authentication and encryption of data technique for the communication of satellite network systems. The main purpose of the said scheme is to remove replay attacks and it used symmetric cryptosystem. The scheme work under two phase, namely the Mobile User Registration Phase: this phase is to proof that user is the legal person to way in the system; and the Mobile User Authentication Phase: this phase is to provide authentication by using a session key. For every communication session, the session key is changed for each mobile user. So this scheme not only enhanced the security level but also minimize the computation level [9].

Y. F. Chang.et.al in 2005 titled '*An efficient authentication protocol for mobile satellite communication system*' mainly concerned with an efficient authentication protocol and to present perfect forward secrecy. This scheme introduced three phases namely, the registration phase, the mobile authentication phase, and the mobile updated phase. This protocol computation is done with only hash and XOR operation, which gives light computation. Through the three phases, this scheme has achieved mutual authentication, secure, efficiency and perfect forward secrecy [10].

G. Zheng.et.al in 2012 titled '*Design and logical analysis on the access authentication scheme for satellite mobile communication networks*' provide the way in authentication for the satellite communications network. The way in authentication is provided in the gateway between the mobile user and the Network Control Center (NCC). The said protocol consists of four phases: the mobile user registration phase, the mobile user management phase, the mobile authentication phase, and the mobile authentication update phase. The said protocol high-spot the authentication character of gateway, and also reduced the calculation burden of the NCC. From this paper we conclude that the system overburden is very less and not devalue the quality of service of the satellite system networks [13].

C.C. Lee.et.al in 2003 titled '*A simple and efficient authentication scheme for mobile satellite communication systems*' withstand various attacks and achieve some functionality. The said scheme operated only in hash and XOR function. In the registration phase, the user is registered with the NCC so as confirmed that the he or she is a legitimate user. In the login phase, the legitimate users can exchange information with other users with the use of the NCC card. And the authentication phase provides the user authentication. The said scheme does not apply complex computation and we can conclude that this scheme is a simple and efficient authentication protocol with low computation cost [8].

C. C. Chang.et.al in 2012 titled '*An authentication and key agreement protocol for satellite communications*' mainly concerned with the authentication for high data transmission satellite communication. The security of this scheme compute on the discrete logarithm problem and hash function and remove replay attack through nonce entity. The said protocol has three phases: the initialization phase, the registration phase, and the authentication phase. The initialization phase is to construct the NCC public and private key pair. If a user wants to communicates with another user via satellite communication networks. So first, in the registration phase the user must have the smart card from the NCC. Once the user received the smart card, he or she want a service and agree on a session key with the NCC in the authentication phase to keep their communication confidential. From this paper we conclude that the needs of untraceable, perfect forward secrecy, and smart card loss are accomplished. In addition to that, furthermore this scheme can detect insertion attack with the help of ElGamal signature concept and also obtain low computation cost [7].

T. H. Chen et al in 2009 titled '*A self-verification authentication mechanism for mobile satellite communication systems*' combines the single-key cryptosystem (symmetric cryptosystem) and the public-key cryptosystem. In this paper, an authentication scheme is developed by using the advantages of both single-key and the public-key cryptosystem. This scheme introduced an authentication scheme for a mobile satellite communication network that allows the NCC and the users to agree on the shared session key, which is mainly done in three phases namely, the phase of initialization, the phase of registration, and the phase of authentication. From this paper we conclude that based on the idea of self-verification, this scheme only utilizes a public-key scheme but not a public key infrastructure and therefore removes the key management load urged on authentication schemes based on a public-key infrastructure. Moreover, this scheme obtained a very low calculation burden on both the mobile user and the NCC; hence, this protocol achieved a lightweight device environment. Furthermore, the session key ensures the confidential communication in the system environments [11].

L. Lasc et al in 2011 titled '*Countering jamming attacks against an authentication and key agreement protocol for mobile satellite communications*' reviewed the protocol [11] of Chen, Lee and Chen. This analyzed protocol [11] disclosed that it is open to denial of service attack, where the intruders disrupt the whole system by immobilizing one message and therefore the functionality of mutual authentication will be failed between the NCC and the user. Hence, the legitimate user is denied from accessing to the intended services. So, the paper [12] protocol is designed based on key agreement and authentication for satellite communications to thwart the frailty in the reviewed protocol. The said protocol of the authentication phase enlarged the storage time of some shared secrets. Suppose if NCC detects de-synchronization, it denies user request and issues a re-synchronization challenge. Using the provided information from the re-synchronization challenge, the user updates the correct shared secrets and tries to re-authenticate again. From this paper, the new protocol ensured the removal of denial of service attacks and even so the connection accessibility undertaken by the satellite service provider, the synchronization issue is successfully maintained at the application layer by the said scheme.

CHAPTER 3

SCOPE OF STUDY

The main scope of the study is to optimize the security level of the communication system and also reduce overload and computation burden in the system.

The need to employ authentication in the satellite communication is that in this the medium of communication is air so the intruders can easily capture or eavesdrop the exchange information while communicating two parties. Due to this drawback authentication is much necessary in the satellite communication to avoid impersonate attack, external attacks, and also replay attack.

Even though the usage of satellite communication is growth day by day the most concerned important areas is the security. The security is the top priority major concerned areas of the whole communication system in the modern technology. Many researchers had developed various authentication techniques to provide better security performance and enhance the communication system. Since satellite application is included in every field like in military, telephony, remote sensing areas, marine, radio broadcasting etc., so authentication is needed in the satellite communication.

CHAPTER 4

PROBLEM FORMULATION

1. In satellite communication, the medium of communication is air so the attackers can easily captured the confidential information because of the absence of user authentication in the system.
2. In the satellite communication, man-in-the middle attack can happen between the client and the server while transmitting the confidential information. The intruder joins the conversation in between the legitimate user so as to impersonate both the parties and obtain the confidential information that is shared between two parties.
3. In the satellite communication, the masquerade attack can happen due to lack of security. This attack used fake identity by the intruders to way in to the unauthorized system so as to enjoy the privilege of the legitimate user.
4. The satellite communication is vulnerable to external attacks. Since the user work station is not protected from outsider attack, the location of the personal computer in the work station is easily known to the attackers. Therefore the satellite communication is not resistant to external attacks.

CHAPTER 5

OBJECTIVES

1. To construct an algorithm for authentication between base station and satellite.
2. To test the working of proposed authentication under sensitive attack conditions.
3. To improve the proposed protocol functionality from the previous authentication protocol.

6.1 Proposed Model

In this model, the client first authenticates itself with the authentication server and also request for ticket to way in to the TGS. The authentication server provides the ticket and session key to the user/client in order to grant a ticket from the TGS so as to way in to the server. The user after obtaining the service granting –ticket from the TGS, this ticket is used to request service from the server. The server provides server authenticator to the user, so that the user can easily access the service to the server by using a secret key shared between the user and the server (satellite) [15][18]. The Fig. 6.1 shown below is the proposed model authentication.

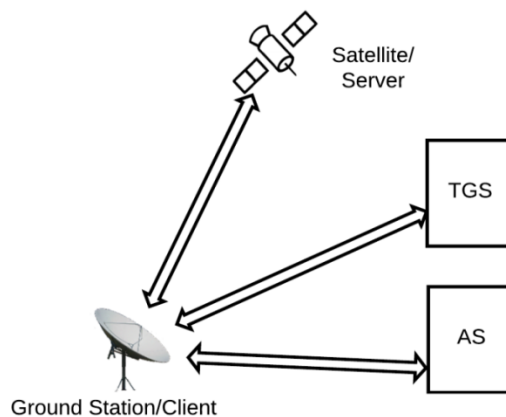


Fig. 6.1 The Proposed model of authentication

Table1. Requirement of the presented protocol

Requirement of ECC and other entities	
P	Prime number
GF(P)	Finite field
a, b	Real numbers
$E_p(a,b)$	The elliptic curve over GF(p) consisting of the elliptic group of points defined by $y^2 = x^3 + ax + b \pmod{p}$, where $(4a^3 + 27b^2) \pmod{p} \neq 0$
G	Generator point (x,y)
N	Order of G
L_1	Latitude of user

L_2	Longitude of user
Options	Request that certain flags be set in the returned ticket
Realm _c	Indicates the area of the client
ID _c	Identity of the client
Realm _{tgs}	Indicates the area of the TGS
ID _{tgs}	Identity of the TGS
AD _c	Network address
Mac _{ad}	MAC address/Physical address
Authenticator _c	Generated by client to validate ticket
ID _s	Identity of the server (satellite)
Ticket _{tgs}	Ticket to access the server (satellite)
Ticket _v	Ticket to access service
Flags	Reflect the status of the ticket and the requested options
Times	Indicates lifetime of the ticket
Nonce	Random value to assure that the response is fresh
Seq	Starting sequence number to be used by the server for message sent to client
TS ₁	Timestamp
TS ₂	Timestamp
Key used	
K_1	Secret key generated by ECC
K_c	User password key
K_{tgs}	Ticket granting server key
$K_{c,tgs}$	Session key created by AS
$K_{c,v}$	Session key created by TGS
K_v	Encryption key for server
Subkey	User choice key similar to session key K_{cv}
Abbreviations	
AS	Authentication Server
TGS	Ticket Granting Server
ECC	Elliptical Curve Cryptography
DHKE	Diffie-Hellman Key Exchange

6.2 The Proposed User Authentication Protocol

This section discussed the user authentication scheme based on Kerberos [15][18] and ECC for communication between satellite and receiver ground station on earth. The proposed scheme has three phases, namely the authentication service exchange phase to obtain ticket –granting ticket, the ticket-granting service exchange phase to obtain service-granting ticket, and the client/server authentication exchange phase to obtain service. In the authentication service exchange phase, the authentication server generates ticket –granting ticket for the client to access the TGS. In the ticket

granting service exchange phase, the TGS generate service-granting ticket for the client to access the server. In the client/server authentication exchange phase, the client can access any service with the help of the ticket generated by the TGS and also the server allows the client to select any user's choice to access the service. The detail of the proposed user authentication scheme is described as follows

6.2.1 The Authentication Service Exchange Phase

In this phase, we obtain a ticket-granting ticket i.e $Ticket_{tgs}$ from authentication server. The operation in this phase is represented in Fig. 6.2.1 and the exchange of information is as follows:

Message1. Client \rightarrow Authentication server:

$$Options \parallel ID_c \parallel Realm_c \parallel ID_{tgs} \parallel Times \parallel Nonce_1 \quad (7)$$

When the user with ID_c , wants to join the system, he/she generates a nonce and request s ticket for accessing the TGS, by sending the ID of the user's and the ID of the TGS to the authentication server.

Message2. Authentication server \rightarrow Client:

$$Realm_c \parallel ID_c \parallel Ticket_{tgs} \parallel E(K_c, [K_{c,tgs} \parallel Times \parallel Nonce_1 \parallel Realm_{tgs} \parallel ID_{tgs}]) \quad (8)$$

The authentication server verifies the information send by the client and generates $Ticket_{tgs}$ to allow accessible to TGS.

$$Ticket_{tgs} = E(K_{tgs}, [Flags \parallel K_{c,tgs} \parallel Realm_c \parallel ID_c \parallel AD_c \parallel Mac_{ad} \parallel Times \parallel L_1 \parallel L_2])$$

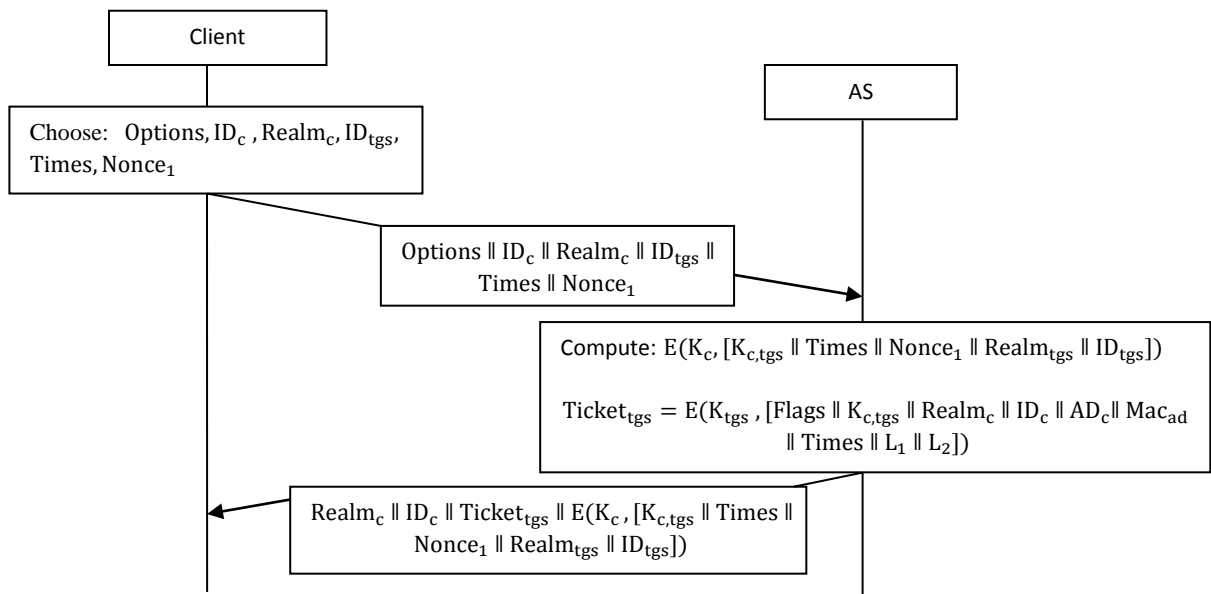


Fig. 6.2.1. The Authentication Service Exchange Phase

6.2.2 The Ticket-Granting Service Exchange Phase

This phase is mainly based on the service-granting ticket so as to access the server and the details mechanism is depicted in Fig. 6.2.2. In this phase, the client helps the TGS to know the exact position of the user by sending the longitude and latitude of the user's work stations.

The client includes the longitude and the latitude of the user's through the $Authenticator_c$. $Authenticator_c$ is encrypted with the session key $K_{c,tgs}$ as:

$$Authenticator_c = E(K_{c,tgs}, [ID_c \parallel Realm_c \parallel TS_1 \parallel L_1 \parallel L_2])$$

When the client request for service-granting ticket, it includes ID server, $Ticket_{tgs}$ and $Authenticator_c$.

Message3. Client \rightarrow TGS:

$$Options \parallel ID_v \parallel Times \parallel Nonce_2 \parallel Ticket_{tgs} \parallel Authenticator_c \quad (9)$$

Message4. TGS \rightarrow Client:

$$Realm_c \parallel ID_c \parallel Ticket_v \parallel E(K_{c,tgs}, [K_{c,v} \parallel Times \parallel Nonce_2 \parallel Realm_v \parallel ID_v]) \quad (10)$$

The TGS generates the service-granting ticket in order to way in to the server.

$$Ticket_v = E(K_v, [Flags \parallel K_{c,v} \parallel Realm_c \parallel ID_c \parallel AD_c \parallel Mac_{ad} \parallel L_1 \parallel L_2 \parallel K_1 \parallel Times])$$

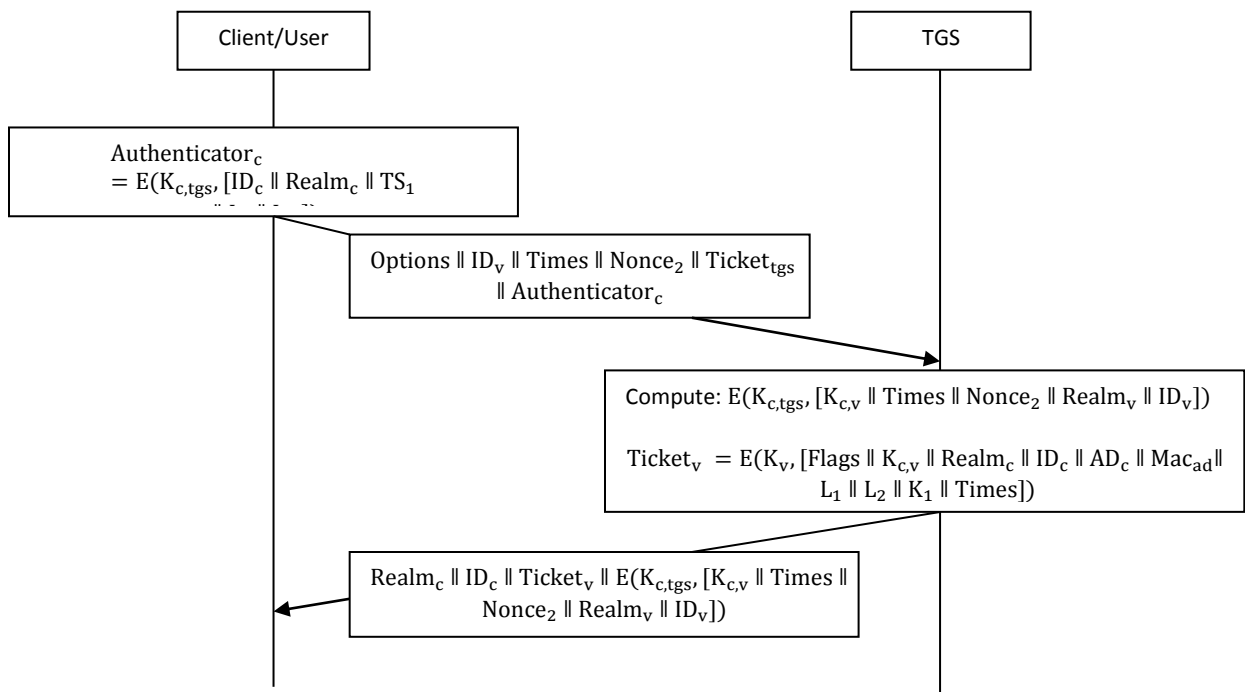


Fig. 6.2.2. The Ticket-Granting Service Exchange Phase

6.2.3 The Client/Server Authentication Exchange Phase

This phase provides the client security to use any service from the server and the details is shown in Fig. 6.2.3. The server provides authentication to the client with the help of $Ticket_v$ granting to use the service from server. And also the client and the server shared the same secret key $K_{c,v}$. Through this secret key the client is able to access the server to use any service for a certain amount of time that the client wants.

Message5. Client \rightarrow Server:

$$\text{Options} \parallel \text{Ticket}_v \parallel \text{Authenticator}_c \quad (11)$$

$$\text{Authenticator}_c = E(K_{c,v}, [\text{ID}_c \parallel \text{Realm}_c \parallel \text{TS}_2 \parallel \text{Subkey} \parallel \text{Seq} \parallel \text{HMAC}])$$

The server cross-check the information sends by the client between the $Ticket_v$ and the Authenticator_c , and if the information is correct then the server replies to client as:

Message6. Server \rightarrow Client:

$$E(K_{c,v}, [\text{TS}_2 \parallel \text{Subkey} \parallel \text{Seq}]) \quad (12)$$

Now the client can operate a service from the server by using the secret key $K_{c,v}$ and also by the additional key known as Subkey, which is the user's choice key.

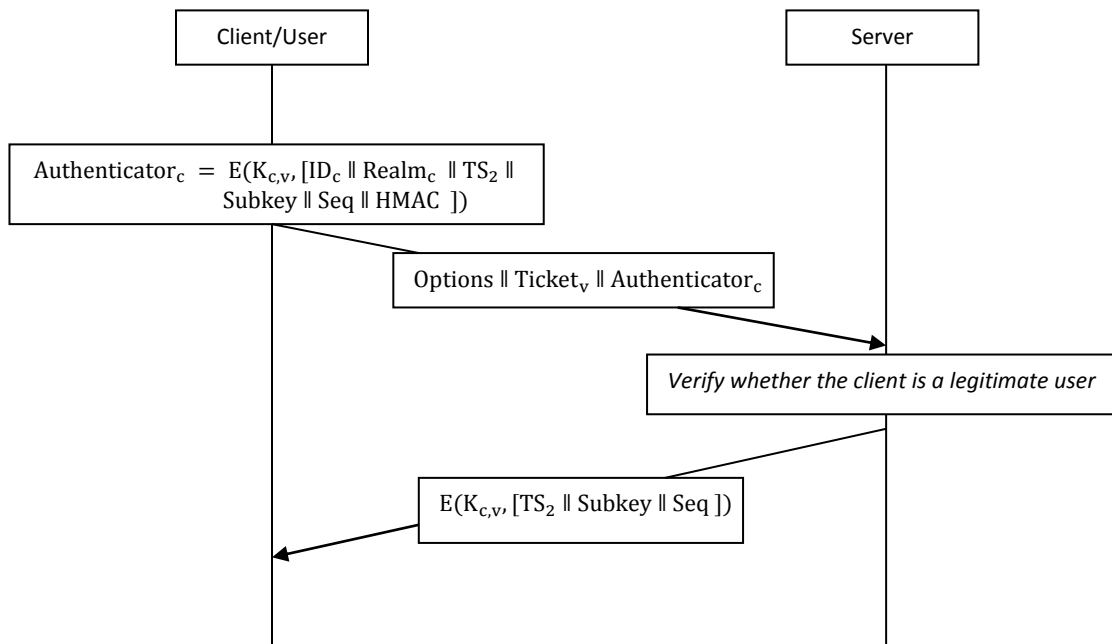


Fig. 6.2.3. The Client/Server Authentication Exchange Phase

CHAPTER 7

RESULT AND DISCUSSION

7.1 Security Analysis

The proposed user authentication protocols undergo certain security analysis. The result of the security analysis of the proposed protocol is discussed below:

(1) Masquerade attack resistance

Suppose an attacker have the legitimate user information and tries to masquerade the legal user to enter into the network. Even if the attacker intercepts ID_c of the user he/she cannot masquerade the valid user. Since the Authentication Server stores the ID_c , AD_c , and Mac_{ad} of the user's in the authentication server file, but the attacker cannot have the network address and physical address of the client .As the authentication request is granted, the authentication server will examined the given user's identity information in the pre-storage location file so as not to register again. Therefore, our proposed scheme is free from masquerade attack.

(2) Forgery attack resistance

Suppose the attackers obtained the $Ticket_{tgs}$ when the AS send message as: $Realm_c \parallel ID_c \parallel Ticket_{tgs} \parallel E(K_c, [K_{c,tgs} \parallel Times \parallel Nonce_1 \parallel Realm_{tgs} \parallel ID_{tgs}])$ to the client. Since the $Ticket_{tgs}$ is encrypted by the secret key K_{tgs} , so the attacker cannot have the confidential information inside the $Ticket_{tgs}$, unless he/she knows the secret key. Therefore, the proposed scheme is free from message-forgery attack.

(3) Resistance of password based attacks

Since Kerberos is a pre-authentication mechanism, the messages send from AS to the client encrypted with the user's password key K_c is totally secure. The message is,

$$Realm_c \parallel ID_c \parallel Ticket_{tgs} \parallel E(K_c, [K_{c,tgs} \parallel Times \parallel Nonce_1 \parallel Realm_{tgs} \parallel ID_{tgs}]).$$

Therefore the attackers have some difficulties in predicting the password key and the content of the encrypted message is secured.

(4) Replay attack resistance

When the confidential information send by the legitimate user is captured by the unauthorized user and later transmitted the information to the intended destination, this disrupts the system services. This process is known as replay attacks.

Since we have use nonce in the proposed scheme to ensure the freshness of message and the parameter Times indicates the lifetime of the message. So it is impossible for the attackers to perform replay attack.

$$\text{Options} \parallel \text{ID}_c \parallel \text{Realm}_c \parallel \text{ID}_{\text{tgs}} \parallel \text{Times} \parallel \text{Nonce}_1$$

Therefore the proposed scheme is resistance to replay attacks.

(5) Resistance of the impersonate attack

Impersonate attacks means to pretend someone identity and enjoy the privilege of the legitimate users. In our proposed scheme we use an authenticator to proof the identity of the real user to the ticket-granting server (TGS). The authenticator includes identity of the client, realm of the client, times and the latitude and longitude of the client.

$$\text{Authenticator}_c = E(K_{c,\text{tgs}}, [\text{ID}_c \parallel \text{Realm}_c \parallel \text{TS}_1 \parallel L_1 \parallel L_2])$$

$$\text{Ticket}_{\text{tgs}} = E(K_{\text{tgs}}, [\text{Flags} \parallel K_{c,\text{tgs}} \parallel \text{Realm}_c \parallel \text{ID}_c \parallel \text{AD}_c \parallel \text{Mac}_{\text{ad}} \parallel \text{Times} \parallel L_1 \parallel L_2])$$

Since the authenticator is encrypted with the session key ($K_{c,\text{tgs}}$) which is known to the client and the TGS, so it is impossible for the attacker to impersonate the client. And also the TGS will cross-check the contents of the Authenticator_c and the $\text{Ticket}_{\text{tgs}}$, so as to ensure that the user is the legitimate user. Therefore the proposed scheme is free from impersonate attack.

(6) Man-in-the-middle attack resistance

This is the attack where the attacker captures the information and alters the communication between two parties.

In our proposed scheme, $\text{Ticket}_{\text{tgs}}$ is exchange between the client and the TGS; and Ticket_v is exchange between the client and the server. The content of $\text{Ticket}_{\text{tgs}}$ is encrypted by the key K_{tgs}

and generates session key $K_{c,tgs}$ and also $Ticket_v$ is encrypted with the key K_v and also generates the session key $K_{c,v}$.

$$Ticket_{tgs} = E(K_{tgs}, [Flags \parallel K_{ctgs} \parallel Realm_c \parallel ID_c \parallel AD_c \parallel Mac_{ad} \parallel Times \parallel L_1 \parallel L_2])$$

$$Ticket_v = E(K_v, [Flags \parallel K_{c,v} \parallel Realm_c \parallel ID_c \parallel AD_c \parallel Mac_{ad} \parallel L_1 \parallel L_2 \parallel K_1 \parallel Times])$$

Man-in-the middle attack is possible only if the attackers have the secret keys K_{tgs} and K_v and also the session key $K_{c,tgs}$ and $K_{c,v}$. Therefore the proposed schemes thwart the man-in-the-middle attack.

(7) Tampering attacks resistance

Suppose the attacker have the message ($Options, Ticket_v, Authenticator_c$) in the phase 3 and attempts to alter the message.

$$Authenticator_c = E(K_{c,v}, [ID_c \parallel Realm_c \parallel TS_2 \parallel Subkey \parallel Seq \parallel HMAC])$$

$$Ticket_v = E(K_v, [Flags \parallel K_{c,v} \parallel Realm_c \parallel ID_c \parallel AD_c \parallel Mac_{ad} \parallel L_1 \parallel L_2 \parallel K_1 \parallel Times])$$

Since we have used ECC key in $Ticket_v$ and HMAC in $Authenticator_c$ to provide integrity of the message and authentication of the user, so the proposed scheme resist to tampering attacks. In order to know the contents of the message in $Ticket_v$ and $Authenticator_c$, the attacker have to know the secret key K_v and the session key $K_{c,v}$.

(8) Resistance from external attacks

We have introduced latitude and longitude in the proposed scheme. This positioning of the client workstation in the proposed scheme leads to identify the same workstation of the client. The latitude and longitude of the workstation is first pre stored in the authentication server. There may be many workstations in one realm which may be allowed to fetch data or control the satellite. We have,

$$Ticket_{tgs} = E(K_{tgs}, [Flags \parallel K_{ctgs} \parallel Realm_c \parallel ID_c \parallel AD_c \parallel Mac_{ad} \parallel Times \parallel L_1 \parallel L_2])$$

Since the attacker does not know the secret key K_{tgs} so it is impossible for the attackers to identify the workstation which prevents from impersonating the client. So latitude and longitude along with MAC address of the devices, network address of the client and the client provides different

authentication services to different block in the same realm or headquarter. Hence the proposed scheme can resist external attack.

(9) Resistance from internal attack

The presented protocol introduced the ECC concept, so we have used the ECC key to prevent internal attacks. We know for a certain realm the latitude and longitude of the internal user will be same.

$$\text{Ticket}_v = E(K_v, [\text{Flags} \parallel K_{c,v} \parallel \text{Realm}_c \parallel \text{ID}_c \parallel \text{AD}_c \parallel \text{Mac}_{ad} \parallel L_1 \parallel L_2 \parallel K_1 \parallel \text{Times}])$$

He/she may occupy the same workstation but if he wants to access service to the server (satellite) from other user devices, the unauthorized person is not aware of the secret key exchange through ECC-DHKE between the legitimate user and the server through the Ticket_v . Hence the proposed protocol is free from internal attacks.

(10) Key compromise impersonate attack

It is assumed that the session keys $K_{c,v}$ and $K_{c,tgs}$ are known to the attackers. Obviously the attacker can impersonate the client. However to impersonate the TGS and the server, so as to interact with the client, the attacker would need the secret keys K_v for the server and K_{tgs} for the TGS. Hence the key compromise impersonate attack can be limited to low range.

(11) Mutual trust

The message (options, Ticket_v , Authenticator_c), sent by the client is verify by the server(V) by comparing the information between the Ticket_v and the Authenticator_c , Which authenticates the client. The server sends the message (TS_2 , Subkey, Seq) to the client in order to authenticate to the client.

Thus, the proposed scheme provides the mutual authentication protocol

(12) Brute-force attack resistance

In the proposed protocol when the ticket is issued it includes the time. The Times in the ticket tells the limited duration of the ticket (i.e the time when the ticket is issued and the expiration of the ticket).

$$\text{Ticket}_{tgs} = E(K_{tgs}, [\text{Flags} \parallel K_{c,tgs} \parallel \text{Realm}_c \parallel \text{ID}_c \parallel \text{AD}_c \parallel \text{Mac}_{ad} \parallel \text{Times} \parallel L_1 \parallel L_2])$$

$$\text{Ticket}_v = E(K_v, [\text{Flags} \parallel K_{c,v} \parallel \text{Realm}_c \parallel \text{ID}_c \parallel \text{AD}_c \parallel \text{Mac}_{ad} \parallel L_1 \parallel L_2 \parallel K_1 \parallel \text{Times}])$$

So it is impossible for the attacker to have ticket by trying many possible keys to decrypt the ticket since the ticket include the Times parameter. Therefore the proposed protocol is free from brute-force attack.

7.2 Performance Analysis

The proposed protocol is analyzed in terms of security:

Comparison is made in table 2, in terms of functionality and free from attack of the proposed protocol with three different protocol, namely Authentication and Key Agreement Protocol based on ECC in[25] (referred as ECC-AKAP), Diffie-Hellman Key agreement scheme in[21] (referred as DHKA scheme), Authentication scheme in [26] and Authentication and Key Agreement in[24] (referred as Secure MAC protocol).

Table2. The functionality comparison

Functionality	ECC-AKAP in [25]	AKA Scheme in [24]	Authentication Scheme in [26]	DHKA Scheme in [21]	Proposed scheme
Replay attack resistance	Yes	Yes	Yes	No	Yes
Internal attacks	Yes	Yes	Yes	Yes	Yes
Mutual trust	Yes	Yes	Yes	Yes	Yes
Man-in-the-middle attack resistance	Yes	Yes	Yes	Yes	Yes
Brute-force attack resistance	No	No	No	No	Yes
External attacks	No	No	No	No	Yes
Key compromise impersonation attack Resistance	No	No	Yes	No	Yes

Thus our proposed protocol has better performance than the existing scheme, and free from various attacks.

CHAPTER 8

CONCLUSION

The modern communication depends on satellite communication mainly for military, telephony, broadcasting and other applications. The security concept is the main crisis which is unable to tackle all the times. In addition, the first priority protection from intruders in the satellite network is the user authentication.

We presented a lightweight user authentication protocol based on ECC and Kerberos, in which an efficient mutual authentication, ticket granting service agreement and integrity of the message are accomplished. On analyzing the security and performance of the proposed protocol, the presented scheme is free from attack such as replay attack, impersonation attack, masquerading attack, internal and outside attacks as well as reduce bandwidth significantly, and minimized the computational load of the client and storage requirement greatly. Moreover our scheme as more advantages security concept since it utilized ticket service to access any service from the server. Without the ticket an unknown person cannot access the server. We have also achieved internal and external attacks resistance. Through the use of latitude and longitude user location the user system is free from external attacks and also with the ECC our proposed scheme is free from internal attacks. In addition, the HMAC reduces the amount of traffic information. Therefore the proposed protocol achieved authenticity, efficient, reliable, and lightweight for the satellite communications.

REFERENCE

- [1] B. R. Elbert, "Introduction to Satellite Communication", 3rd Edition Book, Arctech House, 685, Canton Street, Norwood, MA 02062, 2008.
- [2] D. Roddy, "Satellite Communication", McGraw Hill Text, 1995.
- [3] J. N. Pelton, A. U. M. Rae, K. B. Bhasin, C. W. Bostain, "Global Satellite Communications Technology and System", WTEC Report, ITRI, Maryland, USA, 1998.
- [4] D. Misra, D. K. Misra, and Dr. S. P. Tripathi, "Satellite Communication Advancement, Issues, Challenges and Applications", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, No. 4, April 2013.
- [5] S. M. J. Shah, A. Nasir, and H. Ahmed, "A Survey Paper on Security Issues in Satellite Communication Network infrastructure", International Journal of Engineering Research and General Science Vol. 2, No. 6, 2014.
- [6] H. S. Cruickshank, "a security system for satellite networks", satellite Systems for Mobile Communications and Navigation, conference Publication No. 424 0 IEE, 1996.
- [7] C. C. Chang, T.F. Cheng, and H.L. Wu, "an authentication and key agreement protocol for satellite communications", international journal of communication systems, 2012.
- [8] C.C. Lee, C.T. Li, and R. X. Chang, "a simple and efficient authentication scheme for mobile satellite communication systems", international journal of satellite communications and networking, pp.29-38, 2012.
- [9] M. S. Hwang, C. C. Yang, and C. Y. Shiu, "An authentication scheme for mobile satellite communication systems", *ACM SIGOPS Operating Systems Review*, pp. 42–47, 2003.
- [10] Y. F. Chang, C. C. Chang, "An efficient authentication protocol for mobile satellite communication systems", *ACM SIGOPS Operating Systems Review*, pp.70–84, 2005.
- [11] T. H. Chen, W. B. Lee, and H. B. Chen, "A self-verification authentication mechanism for mobile satellite communication Systems", *Computers & Electrical Engineering*; pp.41–48; Jan-2009.
- [12] L. Lasc, R. Dojen, and T. Coffey, "Countering jamming attacks against an authentication and key agreement protocol for mobile satellite communications", *Computers & Electrical Engineering*, pp.160–168; Mar-2011
- [13] G. Zheng, H. T. Ma, C. Cheng, and Y. C. Tu, "Design and logical analysis on the access authentication scheme for satellite mobile communication networks", *IET Information Security*, pp.6–13, 2012.
- [14] J. G. Steiner, C. Neuman, and J. I. Schiller, "Kerberos: an authentication service for open network systems", Project Athena, pp.18-28, March 30, 1988.
- [15] W. Stallings, "cryptography and network security", fifth edition, 2011.

- [16] J. G. Steiner, C. Neuman, and J. I. Schiller, "Kerberos: an authentication service for open network systems", Project Athena, pp.18-28, March 30, 1988.
- [17] S. P. Miller, B. C. Neuman, J. I. Schiller, and J. H. Saltzer, "Section E.2.1: Kerberos Authentication and Authorization System", M.I.T. Project Athena, Cambridge, Massachusetts, pp.1-36, December 21, 1987.
- [18] C. Neuman, S. Hartma, and K. Raeburn, "internet standard (RFC 4120)", July 2005.
- [19] E. El-Emam, M. Koutb, and H. Kelash et al., "A Network Authentication Protocol Based on Kerberos", International Journal of Computer Science and Network Security, Vol.9, No.8, pp.17-26, August 2009.
- [20] T. Ozha, "Kerberos: An Authentication Protocol", Int.J.Computer Technology & Applications, Vol. 4, No. 2, pp.354-357, 2013.
- [21] X. Zhu, S. Xu, "a new authentication scheme for wireless ad hoc network", International Conference of Information Management, Innovation Management and Industrial Management(ICIII 2012), Sanya, China, pp.312-315, October 2012.
- [22] D. Johnson, A. Menezes, and S. Vanstone, "the elliptical curve digital signature algorithm", Int. J. Inf. Secur., pp.36-63, 2001.
- [23] R. L. B. Daniel, "standards for efficient cryptography, SEC 2: recommended elliptical curve domain parameters", Certicom Corp, Missisauga, Canada, pp.1-45, 2012.
- [24] X. Zhao, Y. Lv, and T.H. Yeap. et.al, "a novel authentication and key agreement scheme for wireless mesh networks", the 5th IEEE Joint Conference on INC, IMS and IDC (NCM 2009), Seoul, Korea, pp.471-474, August 2009.
- [25] Z. Juan, and D. Fangmin, "the authentication and key agreement protocol based on ECC for wireless communications", IEEE International Conference of Management and Service science, September 2009.
- [26] H. Chen, L. Ge, and L. Xei, "a user authentication scheme based on elliptical curves cryptography for wireless ad hoc networks", *Sensors*, pp.17058-17074, 2015.

BIBLIOGRAPHY

- [1] T. Logsdon, "Mobile Communication Satellites", McGraw Hill Text, 1995.
- [2] G. Comparetto, R. Ramirez, "Trends in mobile satellite technology", Vol. 30, No. 2, pp.44–52, 1997.
- [3] J. V. Evan, "Satellite systems for personal communications", IEEE Antennas and Propagation Magazine, Vol. 39, No. 3, pp.7–20, 1997.
- [4] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, Vol. 31, No. 4, pp.469–472, 1985.
- [5] E. Lutz, "Issues in satellite personal communication systems", Vol. 4, No. 2, pp.109–124, 1998.
- [6] H.Y. Lin, "Security and authentication in PCS", Computers and Electrical Engineering, pp.225-148, 1999.
- [7] Z. Sun, "Satellite networking principles and protocols", John Wiley and Sons Ltd, 2005
- [8] C. C. Lee, M. S. Hwang, and W. P. Yang, "Extension of authentication protocol for GSM", IEEE Proc. Commun., Vol. 150, No. 2, pp.91–95, 2003.
- [9] A. Char, A. Mhamed, B. E. Hassan, "A fast and secure elliptic curve based authenticated key agreement protocol for low power mobile communication", pp. 235–240, 2007.
- [10] A. Liu, P. Ning, "A Configurable Library for Elliptic Curve Cryptography in WSNs", International Conference on Information Processing in Sensor Networks, pp.245-256, 2008.
- [11] R. Amin, G. Biswas, "An improved rsa based user authentication and session key agreement protocol usable in tmis", Journal of Medical Systems, Vol. 39, No. 8, pp.1–14, 2015.
- [12] S. R. Pravin, A. P. Renold, "An Enhanced Elliptic Curve Algorithm for Secured Data Transmission In Wireless Sensor Network", IEEE Global Conference on Communication Technologies, pp.891-896, 2015.
- [13] S. Ju, "A Lightweight Key Establishment in Wireless Sensor Network Based on Elliptic Curve Cryptography", pp.138-141, 2012.
- [14] k. Prakasha, B. Muniyal, and Deeksha.et.al, "Electrocardiogram-Kerberos authentication Scheme for services", International Conference on Inventive Computation Technologies, 2016.

APPENDIX 1

COMPLETE WORK PLAN WITH TIME

WEEKS	JANUARY 2017	FEBRUARY 2017	MARCH 2017	APRIL 2017
1ST WEEK	Holidays	Started working on the basic code of Caesar cipher	Finalized the proposed technique	Worked on paper writing.
2ND WEEK	Dissertation 1 viva scheduled	Completed basic code.	Worked on the finalized technique code.	Communicated paper in journal and started working on report
3RD WEEK	Studied all about the tool MATLAB	Started working on the Xor Caesar cipher code.	Done with the code and got efficient results.	Completion of the report.
4TH WEEK	Learned MATLAB tool	Done with the objective	Started writing a paper.	

APPENDIX 2

AUTOBIOGRAPHY

Thokchom Saroj is currently pursuing M. Tech in Electronics and Communication Engineering from Lovely Professional University, Phagwara with Wireless Communication as specialization. This interest includes, Satellite Communication, Wireless Communication, ECC, Kerberos and security of the communication system.

TOPIC APPROVAL PERFORMA

School of Electronics and Electrical Engineering

Program : P175::M.Tech. (Electronics and Communication Engineering) [Full Time]

COURSE CODE : ECE521 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** EEERGD0024

Supervisor Name : Gurjot Singh **UID :** 17023 **Designation :** Assistant Professor

Qualification : _____ **Research Experience :** _____

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Thokchom Saroj	11507024	2015	E1514	7508799584

SPECIALIZATION AREA : Wireless Communication **Supervisor Signature:** _____

PROPOSED TOPIC : A lightweight Authentication Protocol based on ECC for Satellite Communications

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	Parameter	Rating (out of 10)
1	Project Novelty: Potential of the project to create new knowledge	8.00
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	8.00
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	8.00
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	8.00
5	Social Applicability: Project work intends to solve a practical problem.	8.00
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	8.00

PAC Committee Members		
PAC Member 1 Name: Rajeev Kumar Patial	UID: 12301	Recommended (Y/N): Yes
PAC Member 2 Name: Lavish Kansal	UID: 15911	Recommended (Y/N): Yes
PAC Member 3 Name: Dr. Gursharanjeet Singh	UID: 13586	Recommended (Y/N): NA
DAA Nominee Name: Amanjot Singh	UID: 15848	Recommended (Y/N): NA

Final Topic Approved by PAC: A lightweight Authentication Protocol based on ECC for Satellite Communications

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11106::Dr. Gaurav Sethi

Approval Date: 05 Oct 2016