Pertanika J. Sci. & Technol. 25 (4): 1317 - 1330 (2017)

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

A Lightweight Authentication Protocol based on ECC for Satellite Communication

Saroj, T. and Gaba, G. S.*

Discipline of Electronics and Communication Engineering, Lovely Professional University, Jalandhar, India

ABSTRACT

Satellite communication is an emerging field of communication. It is used for many applications, such as broadcasting, messaging, telephony, and for communication between military troops. The satellite communication is prone to impersonate attacks as the access to the satellite does not require a physical connection. Hence, there is a foremost need to restrict the access to only legitimate users. This study aims to solve achieve this. The proposed scheme is based on elliptic curve cryptography (ECC) and assures access to legitimate users only and also claims to be lightweight in working. The analysis indicates that the proposed technique is free from various attacks including internal and external attacks. Also, the performance analysis confirms the proposed authentication scheme as more reliable and robust against attacks compared with existing techniques.

Keywords: Authentication, elliptic curve cryptography, hash function, Kerberos, satellite communication

INTRODUCTION

The modernised satellite communication network is a wireless communication technology which has global coverage and allows users to remain connected almost everywhere on earth. The satellite receives the electromagnetic signal from the ground station, intensifies it and transmits it back to the receiver ground station, therefore, helping in forwarding the information to distant places (Elbert, 2008; Roddy, 1995; Pelton et al., 1998). The satellite communicates with the ground station through the medium of air, so it is easy for the attackers to steal or falsify transmitted data. Communication security has always been an important issue and user authentication scheme is necessary for the wireless network due to no requirement of any physical tapping

ARTICLE INFO

Article history:
Received: 05 June 2017
Accepted: 23 September 2017

E-mail addresses:
thokchomsarojsingh@gmail.com (Saroj, T.),
er.gurjotgaba@gmail.com (Gaba, G. S.)
*Corresponding Author

ISSN: 0128-7680

for fetching data. Many researchers who work on security fundamentals have found that communication through satellite network systems suffers in security provisioning and due to these shortcomings, attackers may intercept, capture, block the channel or attackers may get the control to supervise the entire communication network (Misra, Misra, & Tripathi, 2013; Shah, Nasir, & Ahmed, 2014). Thus, an efficient, lightweight and secure user authentication scheme is mandatory to be implemented in communication networks.

As technology advances, various authentication schemes have been proposed for the satellite communication. An efficient security system for satellite communication, where both the public key and the secret key cryptosystem are used to provide mutual authentication, encrypted information and digital signatures have been proposed by Cruickshank (1996). However, this scheme is vulnerable to attacks. A new mobile user authentication and data encryption schemes for mobile satellite communication are implemented (Lee, Li, & Chang, 2012), where the concepts of symmetric cryptosystems are used to obtain the session key and to resist replay attacks. However, this scheme is not resistant against man-in-the-middle attack. An authentication and key agreement protocol for satellite communication were suggested to improve the state of the art (Chang, Cheng, & Wu, 2014), where the discrete logarithm problem and the hash function is used along with a nonce to prevent replay attacks. However, this scheme suffers from mutual authentication.

Compared with other user authentication schemes, Kerberos user authentication scheme is the most secure mechanism. Since this scheme introduces mutual authentication, and a ticket to the way in the service from the server. The ticket carries a timestamp which enhances the security level of the mechanism (Neuman, Hartman, Yu, & Raeburn, 2005; Ozha, 2013).

Unlike RSA, the public key cryptography, elliptical curves cryptography (Brown, 2009) is the most widely used scheme as it uses smaller key size and has reduced overhead while attaining same level of security. In addition, ECC is based on discrete logarithm problem (El-Emam, Kelash, & Allah, 2009). So, it is hard to obtain effective solution from ECC computation (Johnson, Menezes, & Vanstone, 2001; Brown, 2009). Hence, the lightweight user authentication protocol based on ECC and Kerberos is considered to be reliable and fit for satellite communication.

In this paper, a user authentication scheme based on ECC and Kerberos is devised for satellite communication. In order to provide authenticity and to obtain reliable communication, the Kerberos protocol (Neuman et al., 2005) is modified using ECC (Brown, 2009; Zhao, Lv, Yeap, & Hou, 2009; Zhang, & Deng, 2009) and some new entities are also introduced. The proposed scheme is divided into three phases, namely authentication service exchange phase, ticket-granting service exchange phase and client/server authentication exchange phase. The client authenticates Authentication Server (AS) and requests a ticket to have access to the Ticket-Granting Server (TGS). The AS generates $Ticket_{tgs}$ and sends to the client in the authentication service exchange phase. The contents of $Ticket_{tgs}$ is then compared by the Ticket Granting Server with $Authenticator_c$ from where the request originated. Then, the TGS generates $Ticket_v$ for the client to have access to the satellite server in the ticket-granting service exchange Phase. $Ticket_v$ carries ECC secret key, which is shared between the client and the server for

producing message digest in order to obtain authenticity and integrity of the message. In the last phase, content of $Ticket_v$ is compared with $Authenticator_c$ to verify the real client identity. Additionally, HMAC is also added to obtain source and message authenticity.

The remainder of the paper is organised as follows. In section 2, the system model of proposed user authentication scheme is discussed. In section 3, dialogue exchange between the client and the server is presented followed by security and performance analysis of the proposed scheme in section 4 and 5 respectively. Section 6 concludes the paper.

METHODOLOGY

System Model

In the proposed model, the client first authenticates itself against the authentication server and also requests for a ticket to the way into the TGS. The authentication server provides the ticket and session key to the user/client in order to grant a ticket from the TGS as a way into the server. The user, after obtaining the service granting–ticket from the TGS, approaches the server from which the service has to be obtained. Figure 1 shows the proposed model of authentication whereas Table 1 displays the entities and parameters of the authentication protocol.

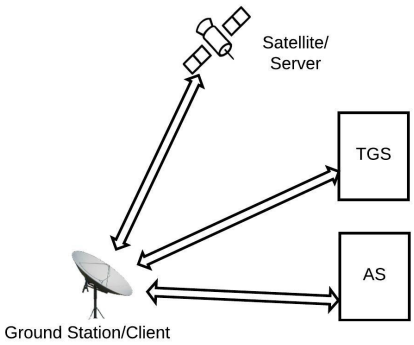

Figure 1. Proposed Authentication Model

Table 1
Entities and Parameters of Authentication Protocol

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 $y^2=x^3+ax+b(\text{mod } p)$, where $(4a^3+27b^2) \text{ mod } p \neq 0$
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

Table 1 *(continue)*

$Realm_c$	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_{add}	MAC address/Physical address
$Authenticator_c$	Generated by client to validate ticket
ID_v	Identity of the server (satellite)
$Realm_v$	Indicates the area 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 through 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

The Proposed User Authentication Protocol

This section elaborates the working of suggested user authentication scheme which is based on Kerberos (Stallings 2006; Steiner, Neuman, & Schiller, 1988) and ECC for initialising security between satellite and ground station communication. 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 a service-granting ticket, and the client/server authentication exchange phase to obtain services. 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 generates service-granting ticket for the client

to access the server. In the client/server authentication exchange phase, the client can access any service provided by the server with the help of the ticket generated by the TGS. The dialogue exchange of the proposed user authentication scheme is discussed in the subsequent section:

The authentication service exchange phase

In this phase, the client obtains a $Ticket_{tgs}$ from the authentication server. The working of this phase is shown in Figure 2.

Message 1. Client → Authentication Server (AS):

$$Options \| ID_c \| Realm_c \| ID_{tgs} \| Times \| Nonce_1 \quad (1)$$

When the client with ID_c, wants to join the system, it generates a nonce and requests ticket for accessing the TGS by sending the ID of the client and the ID of the TGS to the authentication server.

Message 2. Authentication Server → Client:

$$Realm_c \| ID_c \| Ticket_{tgs} \| E(K_c,[K_{c,tgs} \| Times \| Nonce_1 \| Realm_{tgs} \| ID_{tgs}]) \quad (2)$$

The authentication server verifies the information sent by the client and generates $Ticket_{tgs}$ to allow access of client to TGS.

$$Ticket_{tgs}=E(K_{tgs},[Flags \| K_{c,tgs} \| Realm_c \| ID_c \| AD_c \| MAC_{add} \| L_1 \| L_2 \| Times]$$

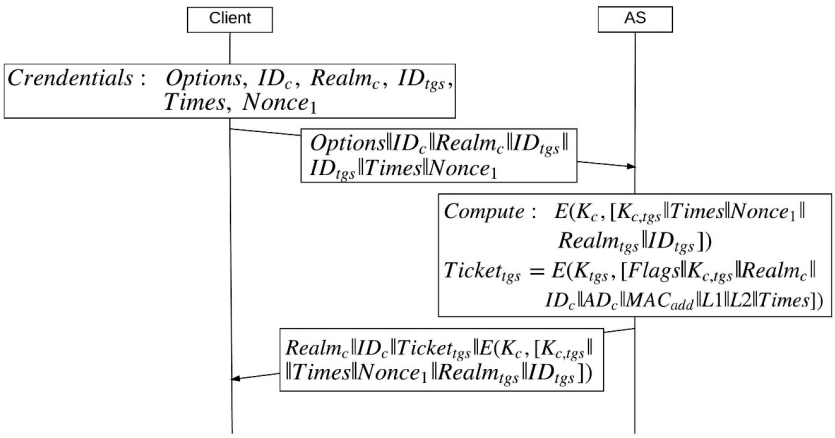

Figure 2. The Authentication Service Exchange Phase

The ticket-granting service exchange phase

This phase is mainly based on the generation and sharing of the service-granting ticket. In this phase, TGS is made aware of the exact position of the user by sending the longitude and

latitude of the user's work stations. When the client requests for service-granting ticket, it includes ID of the server, $Ticket_{tgs}$ and $Authenticator_c$. The whole process is shown in Figure 3.

Message 3. Client → TGS:

$$Options \| ID_v \| Times \| Nonce_2 \| Ticket_{tgs} \| Authenticator_c \quad (3)$$

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

The TGS verify the user authenticity by comparing the content of the $Ticket_{tgs}$ and $Authenticator_c$, the comparison is made on the entities which include ID, network address, MAC address, and latitude & longitude of the user. Upon successful verification, TGS issues a ticket-granting service to the client.

Message 4. TGS → Client:

$$Realm_c \| ID_c \| Ticket_v \| E(K_{c,tgs},[K_{c,v} \| K_1 \| Times \| Nonce_2 \| Realm_v \| ID_v]) \quad (4)$$

The TGS generates the service-granting ticket in order to provide client gateway to the server. The ingredients of the $Ticket_v$ are:

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

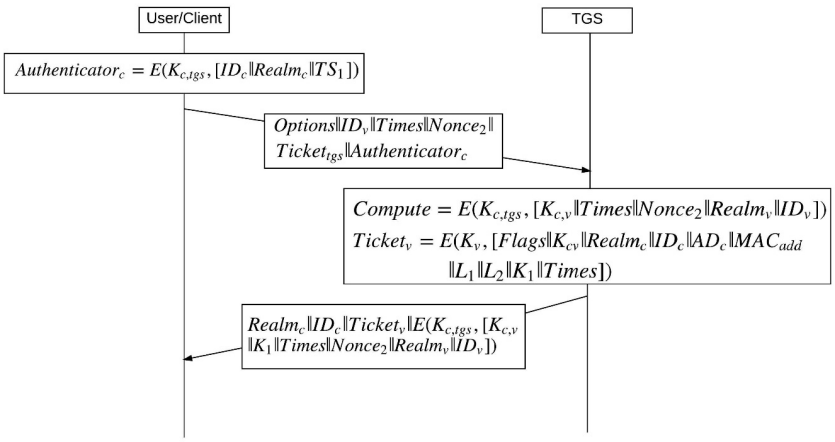

Figure 3. The Ticket-Granting Service Exchange Phase

The client/server authentication exchange phase

In this phase, mutual authentication between the user and the server (V) takes place. Successful authentication enables the client to use that particular service from the server which is specified in the ticket; the whole process is illustrated in Figure 4. The server provides authentication to

the client with the help of $Ticket_v$ granting to use the service from the server. To prevent the disclosure from intruders, the client and the server encrypts the data with the same secret key $K_{c,v}$. Through this secret key, the client is able to access the server for a certain amount of time as discussed during the handshake.

Message 5. Client → Server (V):

$$Options \parallel Ticket_v \parallel Authenticator_c \quad (5)$$

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

The server cross-check the information sent by the client by comparing the content of $Ticket_v$ and $Authenticator_c$, and if the information is found to be true i.e. unaltered, then the server replies to the client as:

Message 6. Server → Client:

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

Now the client can fetch a service from the server by using the secret key K_{cv} and also by the use of additional key known as Subkey, which is the user's choice key.

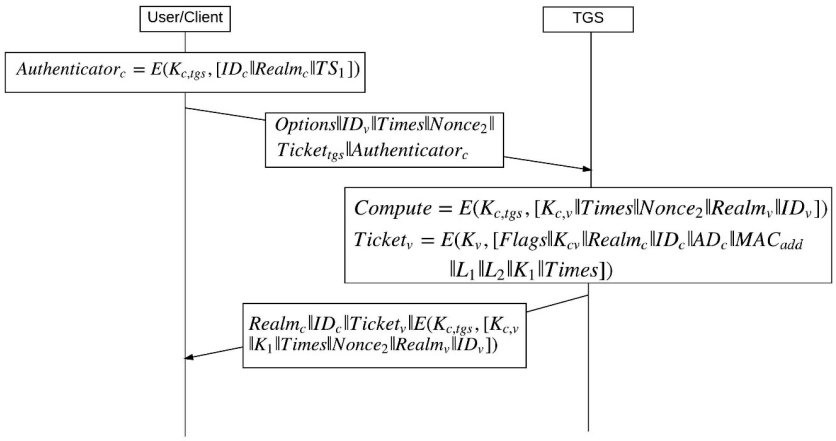

Figure 4. The Client/Server Authentication Exchange Phase

RESULTS AND DISCUSSION

Security Analysis

Masquerade attack resistance. Suppose an attacker has 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 authenticates

the users based on the stored information such as ID_c, AD_c, MAC_{add}, latitude and longitude of the users in the authentication server database which may not be known to the attacker. As the authentication request is processed, the authentication server will examine the given user's identity information with the pre-stored information. If the credentials match, then requesting user will be provided with access else denied. Therefore, the study's proposed scheme is free from masquerade attack.

Disclosure attack resistance. Suppose the attackers obtained the $Ticket_{tgs}$ and $Ticket_v$, during the dialogue exchange between client, AS and TGS.

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

$$Realm_c \parallel ID_c \parallel Ticket_v \parallel E(K_{c,tgs},[K_{c,v} \parallel K_1 \parallel Times \parallel Nonce_2 \parallel Realm_v \parallel ID_v])$$

Since $Ticket_{tgs}$ and $Ticket_v$ are encrypted by the secret key which is not known to the attacker, he cannot have access to the confidential information inside these tickets . Therefore, the proposed scheme is free from disclosure attack.

Resistance against password based attacks. Since the proposed protocol is a pre-authentication mechanism, the messages sent from AS to the client are encrypted with the user's password key K_c. 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 face difficulties in predicting the password key and hence, the content of the encrypted message is kept secured.

Replay attack resistance. When the unauthorised user captures the confidential information sent by the legitimate user and later retransmits the information to the destination again with a malicious thought, it is known as replay attacks.

Since we have used 'Nonce' in the proposed scheme to ensure the freshness of message and the parameter 'Times' to specify the lifetime of the message, so it is impossible for the attackers to perform replay attack.

$$Options \parallel ID_c \parallel Realm_c \parallel ID_{tgs} \parallel Times \parallel Nonce_1$$

Resistance against man-in-the-middle attack. This attack is a type of cyber-attack where an intruder inserts himself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send each other.

In this proposed scheme, $Ticket_{tgs}$ is exchanged between the client and the TGS, and $Ticket_v$ is exchanged between the client and the server. The content of $Ticket_{tgs}$ and $Ticket_v$ is encrypted by the keys K_{tgs} and K_v whereas the content of $Authenticator_c$ is encrypted by the session key $K_{c,tgs}$ and $K_{c,v}$.

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

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

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

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

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

Resistance against tampering attacks. Suppose the attacker captures the message (Options, $Ticket_v$, $Authenticator_c$) in phase 3 of authentication and attempts to alter the message:

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

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

Even if the attacker alters the data, he may not be able to change the content of HMAC appended by the client in the $Authenticator_c$. The client has generated HMAC through secret key shared by TGS between server and client. Hence, to tamper the HMAC, the attacker needs to have a secret key which is not possible as it shared through an encrypted content. Hence, the proposed scheme is free from tampering attacks.

Prevention against external attacks. In the proposed system, the whole area has been divided into realms. However, the differentiation is carried out amongst users on the basis of longitude and latitude. It is now easy to identify the masquerader through this proposed technique. When the AS and TGS receive the message, they will look for the latitude and longitude of the device. They will incorporate this latitude and longitude in the ticket and which will be used for verification whenever the ticket is presented.

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

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

Hence, the proposed scheme can resist external attack.

Prevention against internal attacks. To prevent misfeasance, HMAC is introduced. We know that for a certain realm, the latitude and longitude of the internal users will be same.

$$Ticket_v = E(K_v,[Flags \| K_{c,v} \| Realm_c \| ID_c \| AD_c \| Mac_{ad} \| L1 \| L_2 \| K_1 \| Times])$$

The person who commits misfeasance from getting access to the server (satellite) as he is not aware of the secret key, HMAC is generated by the legitimate user and the server. Hence, the proposed protocol is free from internal attacks.

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 in that scenario. However, to impersonate the TGS and the server in order 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 impersonates attack in the presented approach is not feasible.

Mutual trust. The message (options, $Ticket_v$, $Authenticator_c$) is sent by the client to the server (satellite). The server will verify the authenticity of the client by comparing the ingredients of $Authenticator_c$ and $Ticket_v$. Similarly, server transmits the message $E(K_{c,v},[TS_2 \| Subkey \| Seq])$ to the client in order to authenticate himself to the client. Thus, the proposed scheme provides the mutual authentication.

Brute-force attack resistance. In the proposed protocol, when the ticket is issued, it includes the timestamp. The 'Times' parameter in the ticket specifies the lifetime of the ticket (i.e. the time when the ticket is issued and the expiration of the ticket).

$$Ticket_{tgs} = E(K_{tgs},[Flags \| K_{c,tgs} \| Realm_c \| ID_c \| AD_c \| MAC_{add} \| L_1 \| L_2 \| Times])$$

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

The most secure ECC based cryptography and 'Times' parameter prevents the attacker from launching a brutal attack. The attacker usually tries to apply different combinations to predict the exact key. But this process needs time. Hence, in the proposed authentication protocol, two security features are presented. The encryption technique suggested is ECC based cryptography which is considered as the most reliable technique. Secondly, 'Times' parameter is added which limits the lifetime of ticket required to access the satellite. The time's value is usually kept less than the average time to conduct the attack. Hence, the proposed scheme is free from the threat of brute force attack.

Performance Analysis

The proposed protocol is analysed in terms of security:

Table 2
Strength Evaluation of Authentication Protocols against Attacks

Functionality Comparison and Resistance against Attacks	Zhang, & Deng, (2009)	Zhao et al. (2009)	Chen, Ge, & Xie, (2015)	Zhu, & Xu, (2012)	Proposed scheme
Replay attack	Yes	Yes	Yes	No	Yes
Internal attacks	Yes	Yes	Yes	Yes	Yes
Mutual trust	Yes	Yes	Yes	Yes	Yes
Man-in-the-middle attack	Yes	Yes	Yes	Yes	Yes
Brute-force attack	No	No	No	No	Yes
External attacks	No	No	No	No	Yes
Key compromise impersonation attack	No	No	Yes	No	Yes
Use of Tickets	No	No	No	No	Yes

The comparison is made in Table 2, in terms of functionality and resistance against attacks. The proposed protocol attributes are compared with the four different protocols, namely Authentication and Key Agreement Protocol based on ECC (Zhang, & Deng, 2009) (referred as ECC-AKAP), Diffie-Hellman Key Agreement (DHKA) Scheme (Zhu, and Xu, 2012) (referred as DHKA scheme), Authentication Scheme (Chen et al., 2015) and Authentication and Key Agreement (Zhao et al., 2009) (referred as Secure MAC protocol).

Table 2 shows that the proposed authentication protocol provides mutual authentication and ticket based services. Moreover, it is free from replay and brute force attacks, but DHKA scheme (Zhu, and Xu, 2012) is vulnerable to both attacks. In addition, the protocol also defends against external attacks unlike other authentication schemes mentioned in Table 2. Thus, our proposed protocol has better performance than the existing schemes.

CONCLUSION

Satellite communication has become very important for military, telephony, broadcasting and other applications. Security is the main concern. In addition, the first priority protection from intruders in the satellite network is the user authentication. This study has presented a lightweight user authentication protocol based on ECC, in which an efficient mutual authentication, the ticket granting service agreement and integrity of the message is accomplished. On analysing the security and performance of the proposed protocol, the presented scheme is found to be free from replay attacks, impersonation attack, masquerade attack, internal and outside attacks and also found to be bandwidth efficient.

The proposed technique has also minimised computational vis a vis client and storage requirement greatly. Moreover, our scheme uses the ticket to provide access to service from the server. Without the ticket, an unauthorised user cannot access the server. Latitude and longitude of user location are used to prevent external attacks while MAC address and HMAC help prevent internal attack and forgery. In addition, the HMAC also provides message and source authenticity. Therefore, the proposed protocol is efficient, reliable, and lightweight and can be considered for authenticity check in satellite communication.

REFERENCES

Brown, D. (2009). *Standards for efficient cryptography, SEC 1: elliptic curve cryptography (Version, 2.0).* Retrieved from Standards for Efficient Cryptography Group website: http://www.secg.org/sec1-v2.pdf

Chang, C. C., Cheng, T. F., & Wu, H. L. (2014). An authentication and key agreement protocol for satellite communications. *International Journal of Communication Systems, 27*(10), 1994-2006.

Chen, H., Ge, L., & Xie, L. (2015). A User Authentication Scheme Based on Elliptic Curves Cryptography for Wireless Ad Hoc Networks. *Sensors, 15*(7), 17057-17075.

Cruickshank, H. S. (1996). A security system for satellite networks. *Proceedings of Fifth International Conference on Satellite Systems for Mobile Communications and Navigation*. London, U.K.: IEEE. Retrieved from http://ieeexplore.ieee.org/document/576547/

Elbert, B. R. (2008). *Introduction to satellite communication*. Norwood, MA: Artech house.

El-Ema, M. E., Kelash, H., & Allah, O. F. (2009). A network authentication protocol based on Kerberos. *IJCSNS International Journal of Computer Science and Network Security,* 9(8), 17-26.

Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security, 1*(1), 36-63.

Lee, C. C., Li, C. T., & Chang, R. X. (2012). A simple and efficient authentication scheme for mobile satellite communication systems. *International Journal of Satellite Communications and Networking, 30*(1), 29-38.

Misra, D., Misra, D. K., & Tripathi, S. P. (2013). Satellite Communication Advancement, Issues, Challenges and Applications. *International Journal of Advanced Research in Computer and Communication Engineering, 2*(4), 1681-1686.

Neuman, C., Hartman, S., Yu, T., & Raeburn, K. (2005). *The Kerberos network authentication service (V5)*. Retrieved from The Internet Engineering Task Force website: https://tools.ietf.org/pdf/rfc4120.pdf

Ozha, T. (2013). Kerberos: An Authentication Protocol. *International Journal of Computer Technology and Applications, 4*(2), 354-357.

Pelton, J. N., Mac Rae, A. U., Bhasin, K. B., Bostian, C. W., Brandon, W. T., Evans, J. V., ... Townes, S. A. (1998). *Global Satellite Communications Technology and Systems*. Retrieved from World Technology Evaluation Center of Loyola University website: http://www.wtec.org/loyola/pdf/satcom2.pdf

Roddy, D. (1995). *Satellite Communications*. New York, NY: McGraw-Hill.

Shah, S. M. J., Nasir, A., & Ahmed, H. (2014). A Survey Paper on Security Issues in Satellite Communication Network infrastructure. *International Journal of Engineering Research and General Science, 2*(6), 887-900.

Stallings, W. (2006). *Cryptography and network security: principles and practices*. Boston, MA: Pearson.

Steiner, J. G., Neuman, B. C., & Schiller, J. I. (1988). Kerberos: An Authentication Service for Open Network Systems. *Proceedings of Usenix Winter*. Dallas, TX: USENIX Association. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.41.7538&rep=rep1&type=pdf

Zhang, J., & Deng, F. (2009). The authentication and key agreement protocol based on ecc for wireless communications. *Proceedings of International Conference on Management and Service Science*. Wuhan, China: IEEE. Retrieved from http://ieeexplore.ieee.org/document/5300817/

Zhao, X., Lv, Y., Yeap, T. H., & Hou, B. (2009). A novel authentication and key agreement scheme for wireless mesh networks. *Proceedings of Fifth International Joint Conference on INC, IMS and IDC*. Seoul, South Korea: IEEE. Retrieved from http://ieeexplore.ieee.org/document/5331675/

Zhu, X., & Xu, S. (2012). A new authentication scheme for wireless ad hoc network. *Proceedings of International Conference on Information Management, Innovation Management and Industrial Engineering*. Sanya, China: IEEE. Retrieved from http://ieeexplore.ieee.org/document/6339841/