I J C T A, 9(38) 2016, pp. 431-435
© International Science Press

A Survey on Authentication Schemes for Satellite Communications

Thokchom Saroj[1], Gurjot Singh Gaba[2] and Sandeep Kumar Arora[3*]

ABSTRACT

The satellite communication uses wireless media which does not require tedious setup which makes it more preferable over other communication models. Satellite communications plays a very vital role for military services, weather forecasting, navigation and positioning system, and live broadcast services. But it is more prone to impersonate attack as the medium is wireless. So, different user authentication protocols have been proposed in the past in order to thwart this problem. In this paper, we have discussed various authentication schemes and have analyzed their behavior on the basis of their functionalities and attacks.

Keyword: authentication, attack, key, security, satellite.

I. INTRODUCTION

In the current generation of satellites, the wireless communication technology has been totally transformed. The satellite communication is considered as the largest global communications networking system which provide compatible protocols and standards. Satellite network has reached to every corner of the world and cover almost all of the remote, rural and inaccessible regions. The main widely used applications are weather forecasting, broadcast services, medicine services, audio and video services, navigation and positioning system, remote area sensing and many important military intelligence applications [1-3]. Since the usage of satellite services is increased, the security becomes one of the most major concerns. When security is sought, the user authentication is the first safety barrier to be thought to restrict the access of the system to the legitimate users only [4-5].

It is well noticeable from Figure 1 that the authentication is provided by the Authentication Server which is the gateway to the satellite. A wise protocol always suggest the major section of authentication to be carried out at ground as the satellite strives hard of energy. As observed from Figure 1, both the ground station and the mobile are the satellite service users, so authentication operation has to be performed prior to accessing the satellite network in order to prevent access by intruders. Authentication is an entity that helps the user to prove his/her identity to the system. No outsider can join the system without the proper authentication license. The authentication process is usually carried as follows: (1) Initially, 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 compared with the information contained in the database. If the information is correct, then the intended person is allowed to access the system else denied. Suppose if there is no authentication scheme in the satellite communication, then there may be 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 appears to be coming from the impersonated workstation; (3) A user may capture the message exchange and disrupt the services

[1,2,3] Discipline of Electronics and Communication Engineering, Lovely Professional University, Phagwara, Punjab, India - 144411, *E-mails: [1]thokchomsarojsingh@gmail.com, [2]er.gurjotgaba@gmail.com, [3]sandeep.16930@lpu.co.in[*]*

[*]*Corresponding Author*

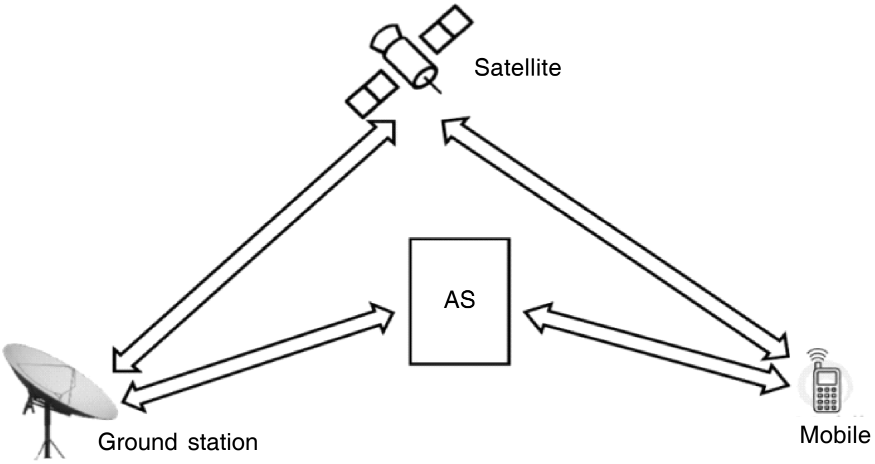

Figure 1: Satellite Authentication Scenario

by using replay attacks. Therefore, in all the cases, there is a probability that an uncertified user may be able to use the services and data that he or she is not allowed to use. Therefore, authentication should be the first priority security entity in the communication networks [14-15].

II. TRADITIONAL APPROACHES FOR USER AUTHENTICATION IN SATELLITE COMMUNICATION

Many researchers have developed authentication schemes to enhance the performance of the satellite communication by eliminating threats in the communication channel and the system. We have discussed many authentication schemes designed for satellite communication platform in this section.

(a) A Security System for Satellite Networks [6]

The suggested scheme has used the combination of public-key and secret-key cryptosystems in order to provide mutual authentication between the users and the satellite. Data encryption is also introduced in the authentication stage with the help of secret key algorithm. The author's utilized public-key technique for the initial authentication stage between the user and satellite, and secret-key technique for encryption in the message exchange stage. The strength of the proposed technique can be analyzed that 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 ongoing communications between the user and the satellite. Hence, end to end security can be provided using the advised technique.

(b) An Authentication Scheme for Mobile Satellite Communication Systems [9]

A new scheme based on user authentication and encryption of data for satellite network systems is unveiled. The main purpose of the said scheme is to eliminate the risk of replay attacks by using symmetric cryptosystem model. The scheme works in two phases, namely the *Mobile User Registration Phase*: This phase proves that user is the legal person to *way in* the system; and the *Mobile User Authentication Phase*: This phase provides authentication by using a session key. For every communication session, a new session key is allocated to each mobile user. So this scheme has not only enhanced the security level, but has also minimized the computation level.

(c) An efficient authentication protocol for mobile satellite communication system [10]

The technique claims to provide an efficient authentication protocol which in turn also attains perfect forward secrecy. This scheme operates in three phases namely, *the registration phase*, *the mobile* *authentication phase*, and *the mobile updating phase*. The protocol algorithm includes Hash and XOR operations, which makes it lightweight in operation. The three phases of the scheme provides enormous security benefits such as mutual authentication, secure & efficient and perfect forward secrecy.

(d) Design and logical analysis on the access authentication scheme for satellite mobile communication networks [13]

The prime focus is to provide the robust method of authentication for the satellite communications network. The authentication process is affixed 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 update phase*. The protocol has considerably reduced the calculation burden at the NCC.

(e) A simple and efficient authentication scheme for mobile satellite communication systems [8]

This prime motive of the recommended technique is to withstand various attacks and to achieve authentication. The said scheme in the algorithm makes use of Hash and XOR function. In the *registration phase*, the user is registered with the NCC and considered as a legitimate user. In the *login phase*, the legitimate users can exchange information with other users through the use of NCC card whereas in *authentication phase, user authentication process* is carried out. The advised scheme does not apply complex computations and thus we can conclude that the scheme provides simple and efficient authentication at low computation cost.

(f) An authentication and key agreement protocol for satellite communications [7]

This authentication scheme is designed for high data transmission satellite link. The algorithm computes discrete logarithm problem and hash function and involves a mechanism to get rid of replay attacks through nonce entity. The proposed protocol works on three phases: the *initialization phase*, the *registration phase*, and the *authentication phase*. The initialization phase is used to construct the NCC public and private key pair. The scheme comes into existence when a user wants to communicates with another user via satellite communication networks. Initially, in the registration phase, the user must have the smart card availed from the NCC. Once the user received the smart card, user must agree on a session key with the NCC in the authentication phase to keep their communication confidential. In addition to that, this scheme also has the capability to detect insertion attack with the help of ElGamal signature concept.

(g) A self-verification authentication mechanism for mobile satellite communication systems [11]

This scheme is a hybrid scheme which combines the single-key cryptosystem (symmetric cryptosystem) and the public-key cryptosystem. It suggests 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 done through three phases namely, the phase of *initialization*, the phase of *registration*, and the phase of *authentication*. The idea revolves around self-verification which utilize public-key scheme but not public key infrastructure which in turn reduce the key management load. Moreover, it is observed that the algorithm puts low calculation overburden on both the mobile user and the NCC. Hence, this protocol accomplishes a lightweight working environment. Furthermore, the session key ensure the confidential flow of communication between the users in the sensitive environments.

(h) Countering jamming attacks against an authentication and key agreement protocol for mobile satellite communications [12]

The analysis revealed that the authentication protocol suggested in [11] is susceptible to Denial of Service attack, where the intruders disrupt the whole system by immobilizing one message and therefore, the functionality of mutual authentication will no longer exist between the NCC and the user. Hence, the legitimate user is denied from accessing to the intended services. So, the proposed protocol is designed to meet to overcome the problems. It is based on key agreement and authentication to thwart the frailty in the traditional protocol [11]. 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. The new protocol ensures the knockout of Denial of Service attacks.

Table 1
Comparison of different authentication schemes based on its functionalities

Authentication Schemes	*Mutual authentication*	*User privacy*	*Confidentiality*	*Low computation cost*	*Anonymity*	*Un-traceability*
[9]	Yes	Yes	No	Yes	Yes	No
[10]	Yes	No	No	No	Yes	No
[11]	Yes	Yes	Yes	Yes	Yes	Yes
[12]	Yes	Yes	Yes	Yes	Yes	Yes
[13]	Yes	Yes	Yes	Yes	No	No
[8]	Yes	Yes	Yes	Yes	Yes	No
[7]	Yes	Yes	Yes	Yes	Yes	Yes
[6]	Yes	No	Yes	No	Yes	No

Table 2
Comparison of different authentication schemes based on its attack resistance

Authentication Schemes	*Insertion attack*	*Impersonation attack*	*Replay attack*	*Stolen-verifier attack*	*Security of smart card loss*
[9]	No	No	Yes	No	NA
[10]	No	No	Yes	No	NA
[11]	Yes	Yes	Yes	Yes	No
[12]	Yes	Yes	Yes	Yes	No
[13]	NA	Yes	Yes	No	NA
[8]	NA	Yes	Yes	Yes	Yes
[7]	Yes	Yes	Yes	Yes	Yes
[6]	Yes	Yes	No	NA	NA

*Data Not Available

Table 3
Comparison of different authentication schemes based on its security model

Authentication Schemes	*Cryptography method*
[9]	Symmetric-key cryptography
[10]	Hash function & XOR operations
[11]	Symmetric & Public-key cryptography
[12]	Symmetric & Public-key cryptography
[13]	Hash function & XOR operations
[8]	Hash function & XOR operations
[7]	Discrete logarithm problem & one way hash function
[6]	Symmetric & Public-key cryptography

III. COMPARATIVE ANALYSIS

Different authentication schemes for satellite communication networks are devised in the past whose comparative analysis is mandate for making use of those schemes in different scenarios. Each authentication scheme has its own way of establishing the security by using different cryptography measures. Comparative analysis of various authentications techniques are conducted whose results are cited in the Table 1, 2 and 3. Table 1 gives a comparison of functionality features like mutual authentication, user privacy, confidentiality, etc. Table 2 illustrates the resistance of the schemes against attacks like impersonate attack, replay attack, insertion attack, etc. Table 3 differentiates the techniques on the basis of principles used to provide authentication. Based on the requirements, any of the authentication schemes can be adopted in the satellite communication environment.

IV. CONCLUSIONS

The modern communication depends on satellite communication mainly for military, telephony, broadcasting and other applications. The security is the main crisis which is unable to tackle all the times. In addition, the first safety equipment in the network is the user authentication. Each scheme has its own security functionalities, advantages and disadvantages. In this paper, various authentication schemes are studied and analyzed in various aspects so that their applications can be defined.

REFERENCES

[1] B. Elbert, “Introduction to Satellite Communication,” 3rd Edition, Artech House, 2008.

[2] D. Roddy, “Satellite Communication,” McGraw Hill, 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 S. P.Tripathi, “Satellite Communication Advancement, Issues, Challenges and Applications,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 4, pp. 1681-1686, 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, pp. 887-900, 2014.

[6] H. S. Cruickshank, “A security system for satellite networks,” Satellite Systems for Mobile Communications and Navigation, UK, 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, vol. 27, no. 10, pp. 1994-2006, 2014.

[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, vol. 30, no. 1, 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, vol. 35, no. 1, pp.41–48, 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, vol. 37, no. 2, pp.160-168, 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, vol. 6, no. 1, pp. 6–13, 2012.

[14] W. Stallings, “Cryptography and Network Security,” Fifth edition, Pearson, 2011.

[15] 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.