International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017),e-ISSN:2455-2585
International Conference on
Recent Explorations in Science, Engineering And Technology (ICRESET'19)
Volume-5, Special Issue-March, 2019.

A Review of Fast Mutual Authentication and Key Exchange in Mobile Communications

Suganthi.A[1], Lanitha.B[2]

Department of computer Science and Engineering, KGISL Institute of Technology, Coimbatore, Tamilnadu, India

Abstract— Authentication plays an important role in the entire mobile network system and acts as the first defense against attackers since it ensures the correctness of the identities of distributed communication entities before they engage in any other communication activity. Many security mechanisms for mobile communications have been introduced in the literature and these mechanisms poised several problems. Therefore, in order to provide security service, an efficient and secure authentication scheme is urgently desired. Combining different authentication techniques with other techniques, such as Time-Stamp based authentication and Nonce-based authentication mechanism, has helped to address these problems and forms the basis of future research. The integrated techniques can solve main contradictory problems more precisely. Review work of the literature, specifically that the research on Time-Stamp based authentication, Nonce-based authentication and Nested One-Time secret mechanism, showed that the said techniques have been widely and successfully implemented in several practical applications. This review work provides an in-depth analysis of identifying and finding issues of strengths, weaknesses and outcomes of combined authentication scheme.

Keywords— Information security, mutual authentication, onetime secrets, secure mobile communication

I. INTRODUCTION

Most of the current mobile communications services are based on the Global System for Mobile Communications (GSM) architecture, and based on the third generation (3G) of mobile communication systems have also been deployed. However, the messages transmitted in wireless communication networks are exposed in the air, so malicious parties in these environments have more opportunities than those in wired-line environments to intercept these transmitted messages [2],[3]. It will seriously threaten the security of wireless communication systems if protection mechanism is not considered. Although some security aspects of current mobile communication systems have been concerned, there still exist security problems in some GSM-based systems—for example, the impersonating attack works because of the lack of mutual authentication in the GSM system.

Mutual authentication and other related security issues have been considered in the GSM-based authentication protocols proposed in the literature [4]-[20], but their performance should be improved as much as possible to further meet the low-computation requirement for mobile users and guarantee the quality of the communication services. Among all security mechanisms in the GSM-based systems, authentication schemes are key techniques to ensure the correctness of the identities of all communication entities before they are about to perform other communication activities. These schemes form robust defenses to withstand the replay attack and the impersonating attack in the GSM system.

Several authentication protocols have been introduced in the literature [8],[10],[11],[15]-[20]. In 1997, Suzuki and Nakada [8] proposed an authentication protocol for the global mobility network. However, Buttyan et al. [10] pointed out that Suzuki and Nakada's protocol has some weaknesses, and they proposed an improved scheme based on Suzuki and Nakada's protocol to eliminate the weaknesses. In 2003, Hwang and Chang [11] proposed a mutual authentication mechanism for mobile communications, which is more efficient than the previous scheme of Buttyan et al. [10].

In 2005, Chang et al. [15] proposed an efficient GSM authentication protocol. In 2006, the protocols based on elliptic curve cryptography were proposed. These protocols are based on timestamps, so they are more efficient than Hwang and Chang's scheme. However, the protocols of [15],[19] and [20] must be under the assumption that the clocks of each mobile user and the system are synchronized and the transmission time between them is stable. In fact, it is difficult to satisfy the above assumption in current mobile communication environments. In 2007 and 2008, some schemes [16]-[18] were proposed. They are all based on asymmetric cryptosystems, which are less efficient than symmetric ones, where the scheme of C. Tang et al. also requires the above assumption, i.e., clock synchronization and stable transmission time.

In the 3rd Generation Partnership Project (3GPP) authentication and key agreement protocol in 2001 [21], it has to be assumed that there exists a secure channel between each visited location register (VLR) and home location register (HLR). The protocols of [8],[10],[11] and [15]-[18] do not require such an assumption. Besides, in the protocol of 3GPP, HLR transfers a long sequence of authentication vectors to a VLR in the first round of authentication for each mobile user, where the VLR must store these vectors. The vectors will be discarded whenever the corresponding mobile user visits a new VLR, to decrease resources usage, so that to decrease computation and communication cost for the system. Accordingly, among these proposed authentication protocols proposed in [8],[10],[11],[15]-[21] the scheme of K. F. Hwang et al.[11] is the most efficient and practical one for GSM-based systems.

Authors made deep research on the performance of secure mutual authentication schemes and come up with an efficient solution to further simplify and speed up the authentication processes through synchronously changeable secrets, which form a nested structure (containing an outer one-time secret and an inner one), shared by each mobile user and the system. The outer one-time secret is a temporal common key of the user and the HLR for initial authentication or authentication when the user roams around the service area of a new VLR. The inner one-time secret is shared by the user and some VLR for mutual authentication between the user and the same VLR. Compared to Hwang and Chang's scheme of [10], authors found that the proposed scheme greatly reduces the computation cost required for each mobile user by nearly 33%. Furthermore, the proposed scheme is formally demonstrated as being immune to both the replay attack and the impersonating attack.

II. METHODOLOGY FOR MUTUAL AUTHENTICATION

Authors reviewed the Hwang and Chang's scheme (2003) and proposed a novel practical mobile authentication scheme that is much more efficient than Hwang and Chang's scheme in both computation and communication under the same assumption of the scheme reviewed. With a pre-shared secret key, there are two basic approaches to achieve mutual authentication between two entities. One approach is the timestamp-based approach, and the other approach is the nonce-based approach.

A. Time-Stamp based authentication

The assumptions of a timestamp-based authentication scheme:

- The clocks of Alice and Bob must be synchronous.
- The transmission time for the authentication message transmitted from one entity to another must be stable.

The advantages of a timestamp-based authentication scheme:

- The protocol only requires two rounds of transmission to reach the goal of mutual authentication.
- It is efficient in computation and communication. Although timestamp-based authentication schemes are simple and efficient, the above two constraints make them impractical in the Internet and mobile environments since most of the users' clocks are not synchronous with the server's or system's clocks and the transmission time is usually not stable.

B. Nonce-based authentication

The advantages of a nonce-based authentication scheme:

- It is not necessary to synchronize the clocks of two entities.
- The transmission time for the authentication message transmitted from one entity to another can be unstable.

The drawbacks of a nonce-based authentication scheme:

- The protocol requires three rounds of transmission to reach the goal of mutual authentication.
- The scheme is less efficient than a timestamp-based authentication scheme in computation and communication.

A nonce-based authentication scheme is free from the two constraints required in a timestamp- based authentication scheme, but the performance may be a problem in the nonce-based scheme as compared to the timestamp-based one. In addition to the above two authentication mechanisms, Authors introduced another technique for mutual authentication, i.e., one-time secret.

C. One-Time secret mechanism

The assumption of an authentication scheme based on onetime secrets:

- Two entities perform the first time of mutual authentication via the protocol since there is no one-time secret shared by them before the first authentication.

The advantages of an authentication scheme based on onetime secrets:

- The protocol only requires two rounds of transmission to reach the goal of mutual authentication.
- It is more efficient than a nonce-based authentication scheme in computation and communication.

However, it is less efficient than a timestamp-based scheme since an additional string must be computed in the scheme based on a one-time secret.

The drawback of an authentication scheme based on onetime secrets:

- Both entities must store an extra string, i.e., the one-time secret, in their devices or computers.

In the GSM system, two authentication actions must be performed. (i) The mutual authentication between a VLR and the HLR. (ii) The mutual authentication between the system (VLR and HLR) and each user. In order to guarantee the quality of mobile communication, the authentication mechanisms they adopted should be as efficient as possible. Each VLR and the HLR are both located in the interior wired network of the GSM system, so authentication between these two registers can be achieved through the timestamp-based authentication mechanism without suffering from the problem of clock synchronization. Since the clocks of each VLR and the HLR can be easily synchronized and the time consumed by transmitting a message between them is stable, the timestamp-based solution can be used to build up the mutual authentication protocol between each VLR and the HLR. On the other hand, it is not easy to synchronize the clocks of the system (VLRs and the HLR) and all mobile users. Hence, the author cannot utilize the timestamp-based solution to construct the authentication protocol between the system and every mobile user even though the solution is the most efficient one among the three authentication mechanisms. The assumption of the mechanism based on one-time secrets cannot form the authentication protocol for the initial authentication between the system and each mobile user. Thus, authors adopted the nonce-based mechanism to establish the authentication protocol for the initial authentication between the system and every user (shown in Fig.1) and the following authentication processes will be accomplished through the techniques of one-time secrets.

TABLE I

DEFINITION OF NOTATION USED IN NEW SYSTEM

Notation	Definition
U_i	The identity of user i
V	The identity of some VLR
H	The identity of the HLR
K_{uh}	A common secret key kept by U_i and H
K_{vh}	A common secret key kept by V and H
K_{auth}	An authentication key kept by U_i and V
E_{Kx}	A symmetric encryption function with a secret key K_x

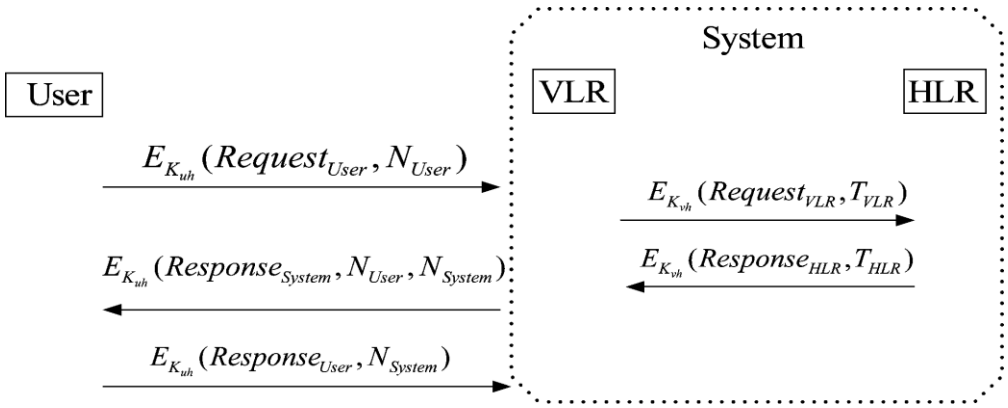

Fig. 1 Initial authentication between a mobile user and the system (VLR and HLR).

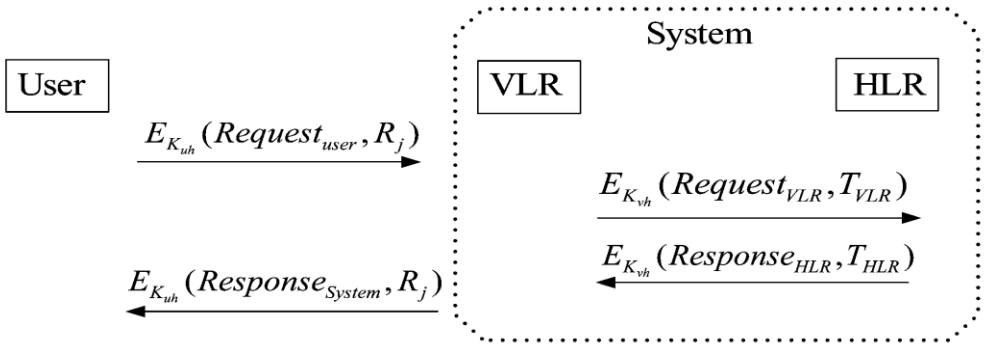

Fig. 2 jth authentication between a mobile user and the system (VLR and HLR) after the initial one, where $j \geq 1$

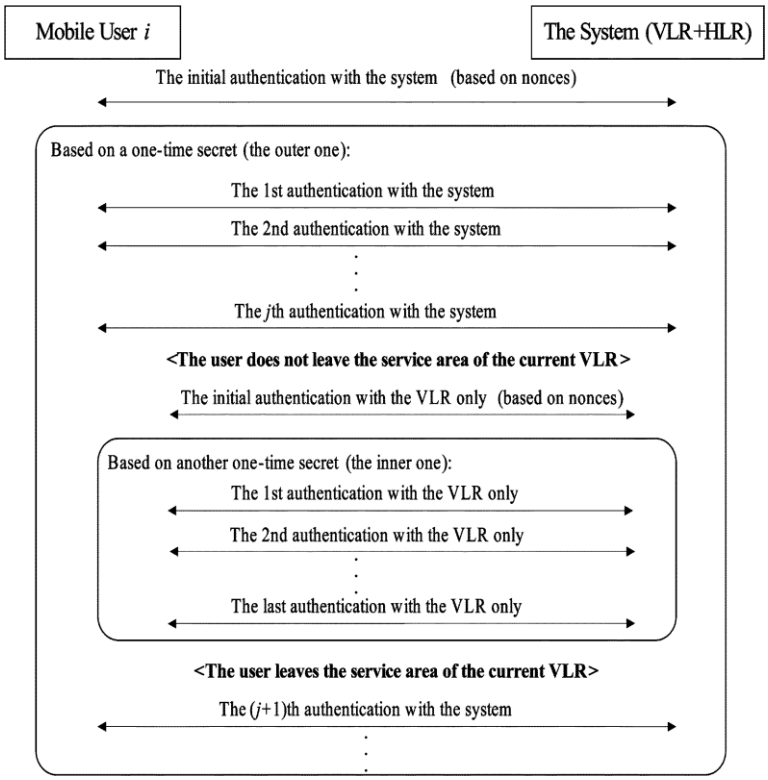

Fig. 3 The proposed nested one-time secret mechanism

III. PROPOSED SYSTEM - NESTED ONE-TIME SECRET MECHANISMS

A sequence of mutual authentication processes based on hybrid mechanism between mobile user and the system (a VLR and the HLR) is as follows. In the initial authentication, the user and the system authenticate each other by performing a nonce-based authentication protocol, and then they negotiate an initial value of a one-time secret. Thus, they make use of the one-time secret, called the outer one-time secret, to complete the following authentication processes. Even, the cost of the authentication can be further reduced again if the user does not leave the service area of the current VLR. In this case, the user performs an initial mutual authentication protocol only with the VLR and set an initial value of another one-time secret, called the inner one-time secret, shared by them. They can perform the following authentication actions via the inner one-time secret until the user leaves the service area of the VLR. Once the user enters the service area of another VLR, the outer one-time secret will be resumed to serve as the key parameter for the next round of authentication between the user and the system. Mobile user shares the outer one-time secret with the HLR and shares the inner one-time secret with the current VLR. This is referred to as the nested one-time secret mechanism.(shown in Fig. 3)

IV. CONCLUSION

The main objective of this work was to analyze and review several work in the literature on a secure mutual authentication and key exchange scheme for mobile communications in combination with other techniques that were aimed to improve security in mobile communication. The analysis focused on the combined use of three established mechanisms of Time-Stamp based authentication, Nonce-based authentication, and One-Time secret mechanism.

The proposed scheme can be solved the problem of replay attack and the impersonating attack on mobile communications and speed up authentication. Compared to Hwang and Chang's scheme, not only does the proposed scheme reduce the communication and computation cost, but also the security of our scheme has been formally proved.

REFERENCES

[1] Chun-I Fan, Pei-Hsiu Ho, and Ruei-Hau Hsu , "*Provably Secure Nested One-Time Secret Mechanisms for Fast Mutual Authentication and Key Exchange in Mobile Communications," IEEE/ACM Trans.Networking.*, vol. 18, no.3, JUNE 2010,pp.996-1009.

[2] Brown, *"Techniques for privacy and authentication in personal com-munication systems,"IEEE Personal Commun*., vol. 2, no. 4, pp. 6–10,Aug. 1995.

[3] N. Jefferies, *"Security in third-generation mobile systems," IEE Coll.Security Netw.*, pp. 8/1–8/5, 1995.

[4] M. Rahnema, "*Overview of the GSM system and protocol architecture,"IEEE Commun. Mag.*, vol. 31, no. 4, pp. 92–100, Apr. 1993.

[5] B. Mallinder, "*An overview of the GSM system," in Proc. 3rd NordicSeminar Digital Land Mobile Radio Commun., Copenhagen, Denmark,1998*, pp. 12–15.

[6] Aziz and W. Diffie, "*Privacy and authentication for wireless localarea networks," IEEE Personal Commun*., vol. 1, no. 1, pp. 24–31,1993.

[7] M. S. Hwang, Y. L. Tang, and C. C. Lee, *"An efficient authenticationprotocol for GSM networks," in Proc. AFCEA/IEEE Euro-Comm,2000*, pp. 326–329.

[8] S. Suzuki and K. Nakada, "*An authentication technique based on distributed security management for the global mobility network," IEEE J. Sel. Areas Commun.*, vol. 15, no. 8, pp. 1608–1617, Oct. 1997.

[9] H. Lee, M. S. Hwang, and W. P. Yang, "*Enhanced privacy and authenticationfor the global system for mobile communications," Wireless Netw.*, vol. 5, no. 4, pp. 231–243, 1999.

[10] L. Buttyan, C. Gbaguidi, S. Staamann, and U. Wilhelm, *"Extensions to an authentication technique proposed for the global mobility network," IEEE Trans. Commun.*, vol. 48, no. 3, pp. 373–376, Mar., 2000.

[11] K. F. Hwang and C. C. Chang, "*A self-encryption mechanism for authentication of roaming and teleconference services," IEEE Trans.Wireless Commun.*, vol. 2, no. 2, pp. 400–407, Mar. 2003.

[12] C. C. Lee, M. S. Hwang, and W. P. Yang, "*Extension of authentication protocol for GSM," IEE Proc., Commun.*, vol. 150, no. 2, pp. 91–95,2003.

[13] L. Harn and W. J. Hsin, "*On the security of wireless network access with enhancements," in Proc. ACM Workshop Wireless Security, 2003*,pp. 88–95.

[14] Peinado, "*Privacy and authentication protocol providing anonymous channels in GSM," Comput. Commun.*, vol. 27, no. 17, pp. 1709–1715,2004.

[15] C. Chang, J. S. Lee, and Y. F. Chang, "*Efficient authentication pro-tocol of GSM," Comput. Commun.*, vol. 28, no. 8, pp. 921–928, 2005.

[16] Tang and D. O. Wu, "*An efficient mobile authentication scheme for wireless networks," IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp.1408–1416, Apr. 2008.

[17] M. Al-Fayoumi, S. Nashwan, S. Yousef, and A. R. Alzoubaidi, "*A newhybrid approach of symmetric/asymmetric authentication protocol for future mobile networks," in Proc. Wireless Mobile Comput., Netw.Commun., 2007*, pp. 29–29.

[18] Kalaichelvi and R. M. Chandrasekaran, "*Secure authentication protocol for mobile," Proc. Comput., Commun. Netw*., pp. 1–4, 2008.

[19] K. P. Kumar, G. Shailaja, A. Kavitha, and A. Saxena, "*Mutual authentication and key agreement for GSM," in Proc. ICMB, 2006*, p. 25.

[20] K. Ammayappan, A. Saxena, and A. Negi, "*Mutual authentication and key agreement based on elliptic curve cryptography for GSM," in Proc.ADCOM, 2006*, pp. 183–186.

[21] 3rd Generation Partnership Project; Technical Specification Group SA;3G Security, "*Security architecture, version 4.2.0, release 4," 3GPP, TS 33.102, 2001.*