ISSN : 2231-0711

Survey on CPAL: A Conditional Privacy Preservation Authentication with Access Linkability for Roaming Service

S.Sangeetha
P.G. Scholar
Department of Computer Science and Engineering,
SNS College of Engineering,
Sathy main road, Coimbatore-641035, Tamil Nadu, India
geetha0003@gmail.com

D.Jebakumar immnauel
Assistant Professor
Department of Computer Science and Engineering,
SNS College of Engineering,
Sathy main road, Coimbatore-641035, Tamil Nadu, India
jebakumarimmanuel@gmail.com

Abstract – Roaming service helps to enable the wireless device kept connected to a network without breaking connections.With this new emerging technology the requirement of ubiquitous accessing can be successfully achieved,for example IOT(Internet of Things).Main goal of CPAL is to provide access linkability for universal secure roaming and multilevel privacy preservation.Anonymous access linkability not only hide user identity but also authenticate link all the access information of the same user.

Keywords-roaming, IOT, privacy preservation, anonymous access linkability, authentication, ubiquitous access.

I. Introduction

Owing to tremendous development in wireless technology,user mobility has become an important network features.One of the advanced technology in mobile communications is GSM.It is one of the successful digital mobile communication system.This system was named as global system for mobile communications.The primary goal of GSM is to provide a mobile phone system that alloes user to roam globally and provide compactable voice services and data accessing service.Services make a network interesting for customers.It mainly focusing on voice-oriented tele services.Another service provided by GSM focused on emergency number.This service is mandatory for all users and free of charge. One fundamental feature of the GSM system is automatic worldwide localization of user.This system enables the service provider to identify the current user accessing and also checks the same phone number is valid worldwide.To achive above service mentioned GSM provides period location updation even if a user doesnot use the mobile station.The HLR always contains the information about the current location of the user and the VLR is responsible to send the message about the MS(mobile subscriber) moving from one service provider to the another service provider to HLR.Moving from home locationHN) to foreign location(FN) and get service access from FN to connect with network this type is known as roaming service.Roaming can take place within the network of one provider,between two provider in one country but also between different provider in different countries.

II. Related Work

Undertaking different statistical security analysis over conditional privacy preserving authentication with access linkability for roaming service improves secure data sharing while device is on roaming.It also aims to share data while connecting to internet in hetrogenous networking.

A. Group Signature Algorithm:

In CPAL[1] proposed that accessing data in a secure manner made a tedious process.Inorder to achieve data integrity while sharing in roaming service we propose two main algorithm known to be group signature and diffie-hellman key exchange.These two algorithm is used to hide the MS-ID to FN and get authentication from HN.HN only knows the MS-ID.Group signature[2] allows the FN to show some one has been entered to get service but they don’t know their ID.This scheme has set of phases which include the following procedures: Issue/Join, Open, Revoke, Sign and finally Verify. Group Issuing Manager: (IM) is the one responsible for the adding of group members along with the maintenance of the secret database of member certificates. It has a *isk* key used for provisioning new members and implements group signature scheme phases like *Join/Issue*.Group Opening Manager: (GOM) – implemented on the Members List.A key called *omk* that is used to open a signature and reveal the identity of the signing member. Open, actually performs a revocation of subscriber’s identity.Group Revocation Manager: (GRM) – It is used to revocate a member in the case of treachery. GRM uses the Remove procedure computed on the Group Member List.Revoke, used to disable the group member, when necessary.Group Member**:** – any member, implementing the Sign procedure.The members of the group signature scheme, use the Sign procedure to authenticate messages and documents.

B. EAP-based Algorithm:

EAP-based authentication algorithm[3] is an example for symmentric-cryptosystem –based technique.EAP abbrivated as Extensible Authentication Protocol is an authentication framework frequently used in wireless network and point to point connection.It not for a specific authentication mechanism and provide some common function and negotiation of authentication method called EAP.It also suppots multiple authentication methods such as token cards,one-time password,certificate and public key authentication.Using EAP in wireless communication user gives request to WLAN through AP(access point) which request for user ID and transmit that ID to an authentication serversuch as RADIUS.The server asks the AP for proof of ID which the APgets from the user and then send back to the server to complete the authentication.

C. Priauth:

PRIAUTH[4] describes strong user anonymity against both eavesdropper and foreign server.While supporting Strong user untraceability PRIAUTH provides an efficient approach to trackle the problem of user revocation.Inorder to prevent fraudulent use of service user authentication is a mandatory requirement.It only requires the roaming user and the foreign server to be involved in each protocol runs.even though it support authentication function of strong user anonymity it shows some drawbacks such as,not allowing to support new group member joining after system setup and another problem is,a user only to register once at the home network before being able to access the global network.Compared to other authentication method,this protocol can provide a practical user revocation mechanism.

D. Mutual Authentication Protocol:

Mutual authentication is know to be MAP.Main goal of MAP[5] is to provide a muthual authentication mechanism for user U and foreign server V.The following mechanism describes the proposed work of MAP function to enhance security level in roaming service.Mobile user M initially register himself to be a legal subscriber of his home network whenever M enters a new visited network.M generates a secret random number to compute the long term secret key KVH using public one way functionand send ID to visited network.On receriving message1 from M,V forwards PID(Pseudonym identity) and send to H for ID authentication,where KVH is the shared secret key between V and H, timestamp t also calculated.After receiving the message from V,H first decrypts by using KVH.Then H determines whether the timestamp is within some allowable range compared with its current time or else H terminates the execution.Aterwards,H calculates the long-term key KMH by public ID and use it to decrypt KMH using timestamp.If the decrypted secret key KMH is equal to public ID the authenticity of user M is authenticatedof V.Subsequently, H send authentication to V.Message 4 and 5 shows the process of mutual authentication and key negotiation between M and V.On receiving message from H,V frist decrypts.If decrypted message is in KVH is ame as its original then V believes that M is an authorized user.Subsequently V does the following,1.Saving the valu for identifying the identity of user M.2.setting authentication key.3.Forwarding the message to M.M decrypts message using KMH and compute with authentication key.Afterwards ,M sends to V to verify key.Finally V has finished the authentication process with M and established an authentication key.

Message 1. M→V :IDH,PIDM,EKMH(rM_KMH)
Message 2. V→H:PIDM,EKVH(rV _tV _EKMH(rM_KMH))
Message 3.V←H:EKVH(rV _rM_h(IDM)),EKMH(rM_rV _IDV)
Message 4. M←V :EKMH(rM_rV _IDV)
Message 5. M→V :EKauth (Kauth)

E. One-time session key Renewal protocol:

Main goal of SKRP protocol[5] is to establish or renew a session key between M and V.In this section ,a novel mechanism called"One-time session key renewal" is introduce, which allow mobile user M to renew his session key frequently and reduce the risk that he uses a compramized session key to communicate with V.

Message 1. M→V :IDV ,PIDM,i,EKi−1 (rM,i_Ki−1)
Message 2. M←V :EKi−1 (rM,i_rV,i_IDH)
Message 3. M→V :EKi (Ki)

Suppose that M need to renew his session key K with V for the *i*th time,hhe can obtain the new session K according to the steps .The new session K is calculated and K0 is set ass the authentication key , that is, K0 = Kauth. The pseudonym identity PIDM,i for M is computed. Clearly, PIDM,i will vary in each session key negotiation because of rM,i.On receiving the message 1 from *M*, *V*can obtain the original rM,I Then, *V* uses the previous session key Ki−1 to decrypt EKi−1 (rM,i _ Ki−1) and checks whether rM,i and Ki−1 in EKi−1 (rM,i _ Ki−1) are the same as with previous key and the previous key Ki−1 kept by *V*, respectively. If it is not, *V* terminates the execution. Otherwise, PIDM,i of *M* is authenticated. Subsequently, *V* does the following: 1) Generating a random number rV,i; 2) Setting as the next session key Ki = rM,i □ rV,i and keeping it secretly; 3) Sending EKi−1 (rM,i _ rV,i _ IDV) to *M*. Since rM,i and rV,i are generated by *M* and *V*, respectively, Ki = rM,i □ rV,i plays a role of one-time key when *M* accesses *V*. We call this new mechanism "One-time session key renewal".

F. VLR-GS-BU:

VLR-GS-BU[6] contributes two main functions: (1) We show some security weaknesses of current user authentication protocols in wireless communications. (2) We propose a privacy- preserving universal authentication protocol called Priauth. By introducing Verifier-Local Revocation Group Signature with Backward Unlinkability (VLR-GS-BU), it can satisfy all requirements described above. Also, Priauth only requires the roaming user and the foreign server to be involved in each protocol run, and the home server can be off-line. Additionally, Priauth belongs to the class of Universal Authentication Protocols in which same protocol and signaling flows are used regardless of the domain (home or foreign) a roaming user is visiting. This helps reducing the system complexity in practice. Furthermore, Priauth supports verifier-local revocation, which means that verifiers (i.e., foreign servers) can, based on the revocation list (RL) sent from the home server, check locally whether a roaming user is revoked. Note that VLRGS- BU is not originally designed for authentication purpose and a direct application of it imposes two problems in Priauth. Firstly, it does not allow Priauth to support new group member joining after system setup. Secondly, it does not provide Priauth the single registration property commonly available in most existing authentication protocols, which requires a user only to register once at the home network before being able to access the global network. We will provide solutions to these two problems to make Priauth practical.

G. Three-Party Roaming Protocols:

The conventional roaming authentication approaches [7, 8] follow the three-party structure.Simple cryptographic techniques (i.e., hash function operation, symmetric and public key cryptography) are usually used for this type of systems. The typical authentication procedures are as follows. A user *U* sends a login request ({*ID*,*h*(*key*ÍÍ*ID*ÍÍ*nonce*ÍÍ…)}, {*ID*,*Ekey*(*ID*ÍÍ *nonce*ÍÍ…)}, or {*Cert*,*sign*(*nonce*ÍÍ…)}) to the visited foreign server *V*, where the notations *ID*, *h*(*key*ÍÍ*data*), *Ekey*(.), and *sign*(.) represent the user identity, keyed-hash-function with a session key, encryption with a symmetric key, and digital signature using public key cryptography, respectively. Additionally, ÍÍ denotes the bit concatenation operator. Also, *nonce* is a random number included in the *beacon messages*, which are periodically broadcast by *V* to declare service existence. Upon receiving this login request message, server *V* transmits the message to *U*'s home server *H* for authentication. Since these approaches only require low-cost cryptographic operations on mobile users and network servers, they are suitable for resource-limited application scenarios. For example, our implementations show that Advanced Encryption Standard (AES) encryption (with a 128-bit plaintext and a 128-bit key) and an ECC-160 digital signature just take 0.6 ms and 102 ms on a 1.2-GHz laptop PC, respectively. One example is wireless LAN (WLAN) secure roaming. The IEEE 802.1x standard provides an authentication framework that is based on the Extensible Authentication Protocol (EAP). In the EAP framework, some authentication methods including EAP-MD5 (Internet Engineering Task Force [IETF] RFC 1321), EAP-TLS, EAP-TTLS, and EAP-GPSK have been proposed. As one of the most popular EAP types, EAP-MD5 is primarily based on a oneway hash function. When using EAP-MD5, a subscriber computes the hash value with the password as input, and the hash value is transmitted through the visited server to the home server for subscriber validation. The main weakness is that EAP-MD5 cannot support user anonymity and non-traceability, and server authentication. Although the other EAP solutions (e.g., EAP TLS, EAP-TTLS, and EAPGPSK) can achieve mutual authentication between mobile users and the visited networks, recent studies [9] have shown that they cannot provide basic user anonymity and non-traceability, session key security, or attack resistance.

H. Two-Party Roaming Protocols:

Compared with the three-party approach, the advantages of the two-party technique include the following. First, it avoids some problems such as the connection loss between the foreign server and the home server, and the single point of failure due to the home server, which are possible in the three-party structure. Second, one drawback of the three-party roaming structure is that these protocols require a foreign server to unconditionally forward any login request, valid or invalid, to the home server [7, 8]. Therefore, an adversary can easily launch DoS attacks on a home server through a foreign server. However, the two-party structure only requires the roaming user and the foreign server to be involved in each protocol run; the DoS attack on home servers is thus not applicable. Third, it requires fewer communication rounds. In the three-party roaming structure, a communication round between the foreign server and the home server is required. Especially when the home server is many network hops away from the foreign server, this communication delay becomes more crucial. These advantages together have led to the recent increasing popularity of the two-party roaming authentication [10-14].The typical authentication procedure of the two-party technique is: A user *U* sends a login request {*alias*, *signkey*(*alias*ÍÍ*nonce*ÍÍ...)} to the visited foreign server *V*, where the notations *alias* and *signkey*(.) represent a pseudo-ID (i.e.,unused pseudonym) and digital signature using some complex cryptographic techniques (e.g., group signature), respectively. With public key materials, *V* checks whether *U* is a legitimate subscriber of the claimed server *H*. While the two-party structure ensures more robust and fault-tolerant roaming authentication, such a structure also poses some security challenges. First, in order to enable the foreign server to locally check the validity of roaming users, some complex cryptographic techniques (e.g., identity-based signature, group signature) must be used, which usually result in high computation overhead on mobile users and the foreign server. For example, our implementations show that as a common operation of these techniques, pairing computation takes 3.8 ms on a 1.2-GHz laptop PC.

I. Non-Cryptographic Roaming Authentication Technique:

All existing roaming authentication approaches resort to cryptography. However, cryptographic exchange mechanisms are complex and therefore induce potential vulnerabilities in themselves. As reported in [15], lower/physical layer characteristics(e.g., MAC behavior, clock skew, signal strength) have been considered as potential alternatives/complements to provide security in wireless networks. We expect that some progress can be made by using these non-cryptographic techniques to achieve an effective roaming authentication. Here, we use clock skew and Requirement (1) (i.e., server authentication) as an example.Clock skews are the inherent tiny drifts in the clocks of hardware devices due to variations in the manufacturing process. It has been demonstrated that the measurement of clock skews can provide the fingerprints of the devices (e.g., access points). To meet Requirement home network and uses this information to establish the first point of trust with a legitimate foreign server. This method does not require any additional hardware to realize as it exploits the already existing defects in the clock crystals.

III. APPLICATIONS

Recent advances in wireless communication technology have motivated new application domains for wireless networks.Some of them are listed below,

1.The term "roaming" originates from the Global System for Mobile Communications (GSM), referring to the extension of connectivity service in a location that is different from the home location where the service was registered. In particular, roaming

2.Roaming is the ability for a cellular user to automatically make and receive voice calls, send and receive data, or access other services, including home data services,when traveling outside the geographical coverage area of the HN, by means of using a visited network.

3. With the development of wireless communications, the concept of roaming can be extended to the emerging paradigm of networking, e.g., IoT, VANET, and e-Health.

4.When these users want to access an FN, which is different from the HN where the service was registered, CPAL can be applied to the access process to provide security and privacy preservations.

IV. COMPARATIVE ANALYSIS

Scheme	TOC	SRR	UNI	NOP	SUA	JRD
GroupSignature Algirithm	Public	Yes	Yes	2	Yes	Yes
EAP-Based Algorithm	Symmentric	Partially	No	3	No	No
PRIAUTH	Public	Yes	Yes	2	Yes	No
Mutual Authentication Protocol	Symmentric	Partially	Yes	3	Yes	No
One-time Session key renewal protocol	Symmentric	Partially	Yes	3	Yes	No
VLR-GS-BU	Public	Yes	Yes	2	Yes	No
Three-party roaming protocol	Both	Yes	Yes	3	No	No
Two-party roaming protocol	Both	Yes	Yes	2	Yes	No
Non cryptographic roaming authentication technique	Clock Skew	Yes	No	2	No	No

TOC, type of cryptosystem; SRR, security requirements of roaming service; UNI, universality; NOP, the number of parties;SUA, strong user anonymity;JRD, efficient joining and revocation function for dynamic membership.

V. CONCLUSION

In modern environment over 6.8billon people uses roaming internet(mobile usage) i.e equal to 96% of population.Because of this evolvation, mobile frequent usage is easy to access.It is necessary to increase security over the community in mobile network.Normally we know many internet connection eg., Ethernet,TCP/IP,etc.So whatever technique used we have more method to hack the data so were are in need of security mechanism to protect our data from attackers.Likewise that some of the security algorithm and protocols has been mentioned in above works to have attain its security levels.

REFERENCES

[1]. Chengzhe Lai, Student Member, IEEE, Hui Li, Member, IEEE, Xiaohui Liang, Member, IEEE, Rongxing Lu, Member, IEEE, Kuan Zhang, Student Member, IEEE, and Xuemin Shen, Fellow, IEEE," CPAL: A Conditional Privacy-Preserving Authentication With Access Linkability for Roaming Service," IEEE internet of things journal, vol. 1, no. 1, february 2014.

[2]. J. Y. Hwang, S. Lee, B. . Chung, H. S. Cho, and D. Nyang. Group signatures with controllable linkability for dynamic membership. Information Sciences, 222:761-778, 2013.

[3]. C. Fan, Y. Lin, and R. Hsu, "Complete EAP method: User efficient and forward secure authentication protocol for IEEE 802.11 wireless LANs," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 4, pp. 672–680,Apr. 2013.

[4]. D. He, J. Bu, S. Chan, C. Chen, and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications," IEEE Trans. Wireless Commun., vol. 10, no. 2, pp. 431–436, Feb. 2011.

[5]. Y. Jiang, C. Lin, X. Shen, and M. Shi, "Mutual authentication and key exchange protocols for roaming services in wireless mobile networks," IEEE Trans. Wireless Commun., vol. 5, no. 9, pp. 2569–2577, Sep. 2006.

[6]. Savitha S.V * * M.Phil Research Scholar, Sree Narayana Guru college, K.G .Chavadi, Coimbatore 6411 05, Jisha K ** **M.Phil Research Scholar, Sree Narayana Guru college, K.G .Chavadi, Coimbatore 6411 05,"Session key Authentication Mechanism For Wireless Sensor Network users,International Journal for Scientific and Research Publication,Volume 4, Issue 6, June 2014 ISSN 2250-3153.

[7]. D. Samfat, R. Molva, and N. Asokan, "Non-Traceability in Mobile Networks," *Proc. MobiCom '95*, 1995, pp. 26–36.

[8] G. Yang, D. S. Wong, and X. Deng, "Anonymous and Authenticated Key Exchange for Roaming Networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, Sept. 2007, pp. 3461–72.

[9]. K. Hoeper and L. Chen, "Where EAP Security Claims Fail," *Proc. Qshine '07*, 2007.

[10]. Z. Wan, K. Ren, and B. Preneel, "A Secure Privacy-Preserving Roaming Protocol based on Hierarchical Identity- based Encryption for Mobile Networks," *Proc. ACM WiSec '08*, 2008, pp. 62–67.

[11]. G. Yang et al, "Universal Authentication Protocols for Anonymous Wireless Communications,"IEEE Trans.Wireless Commun,vol. 9,no. 1,Jan. 2010,pp. 168-74.

[12]. D.He et al, "Privacy-Preserving Universal Authentication Protocol for Wireless Communications," *IEEE Trans. Wireless Commun.*, vol.10,no. 2,Feb.2011,pp. 431-36.

[13] D.He et al, "Secure and Efficient Handover Authentication based on Bilinear Pairing Functions," *IEEE Trans. Wireless Commun.*, vol. 11,no. 1,Jan. 2012,pp.48-53

[14] D. He *et al.*, "Handauth: Efficient Handover Authentication with Conditional Privacy for Wireless Networks," *IEEE Trans. Computers*, published online 27 Dec. 2011.

[15]. K. Zeng, K. Govindan, and P. Mohapatra, "Non-Cryptographic Authentication and Identification in Wireless Networks," *IEEE Wireless Commun.*, vol. 17, no. 5, Oct. 2010, pp. 56–62.