An Optimized Secure Communication Using VLR-GS-BU on Wireless Network

M.Saranya
Computer Science and Engineering
Sri Krishna college of Technology
Coimbatore, India
saranmanirajan@gmail.com

P.Dhivya
Computer Science and Engineering
Sri Krishna college of technology
Coimbatore, India
dhivyainfo@gmail.com

***Abstract*— A novel protocol to achieve privacy-preserving universal authentication protocol for wireless communications called Priauth. to secure the communication as the data are sensitive or it requires the users to pay for it. In the algorithms for secure communication a key is shared by H with V and V with users. The key is used to encrypt data transmitted to the servers or users. In privacy based authentication protocols besides the user and its home server, no one including the foreign server can tell the identity of the user; and besides the user and its home server, no one including the foreign server is able to link any past or future protocol runs of the same user. An To revoke multiple users is to associate a key with every nonempty subset of users in the group. Thus, if one or more users are revoked, the VA uses the key associated with the subset of the remaining users to encrypt the new key and transmits the new group key to them. The advantage of this approach is that the communication overhead is only one message for revoking any number of users. However, the number of keys stored by the VA and the users is exponential in the size of the group. The goal of the enhancement is to evaluate trade-off between storage and revocation cost. Storage is computed in terms of keys that each user (respectively, VA) maintains. And revocation cost is computed in terms of the encryptions performed, and the number of messages transmitted, by the VA.**

Keywords- Priauth; hierarchical key management; rekeying and storage trade-offs.

I. Introduction

Wireless communications technologies have undergone rapid development. Small mobile devices within range of a wireless network can transfer data at any place and any time. This is bringing forth the important issue of information security, privacy, and authentication in an open space. Privacy involves ensuring that an eavesdropper cannot intercept the communication information of mobile users. Authentication involves ensuring that the services are not obtained fraudulently. It is very crucial that the identities of wireless users must be authenticated to prevent illegal use of resources. In addition, in order to protect the privacy of users, anonymity characteristic is the focus of consideration. A privacy-preserving user authentication scheme should satisfy the following requirements:

(1) Server Authentication: a user is sure about the identity of the foreign server.

(2) Subscription Validation: a foreign server is sure about the identity of a user's home server.

(3) Provision of user revocation mechanism: due to some reasons user authentication should allow a foreign server to find out whether a roaming user is revoked.

(4) Key establishment: the user and the foreign server establish a random session key which is known only to them and is derived from contributions of both of them. In particular, the home server should not know the session key.

(5) User anonymity: besides the user and its home server, no one including the foreign server can tell the identity of the user;

(6) User untraceablility: besides the user and its home server, no one including the foreign server is able to link any past or future protocol runs of the same user.

The two main contributions: (1) Security- weaknesses of current user authentication protocols in wireless communications. (2) 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 [2] 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.

II. Related Works

G. Yang, Q. Huang, D. S. Wong [2] propose a novel set of solutions to achieve secure roaming. Their solutions only require the roaming user U and the foreign server V to be involved in each protocol execution, and H can be off-line. Furthermore, this protocol is identical to the authenticated key exchange protocol performed between U and H when U is in its home network. All the existing three party protocols require a serving network to separate foreign users from local ones and perform different signaling flows respectively. Their protocols instead, are universal in the sense that the same protocol and signaling flows are used regardless of the domain (home or foreign) U is visiting. They call such kind of authentication protocols Universal Authentication Protocols.As user privacy becomes a notable security issue in wireless communications, it is desirable to keep mobile users' identities and whereabouts anonymous. When U is revoked by H, V is not going to provide services to U. In the weakly-anonymous two-party setting, V knows U, hence the user revocation can be done easily. In the case of two-party roaming with Strong User Anonymity, however, RL cannot be used as V does not know the identity of U. In other words, user revocation for two-party secure roaming with Strong User Anonymity requires that the foreign server can find out whether a visiting roaming user is revoked or not without actually knowing who the roaming user is, and the whole process should be done without any real time involvement of H. In their solution, they achieve this objective efficiently and at the same time, maintain high scalability with respect to large numbers of revoked users.

M. Zhang and Y. Fang[6] they proposed that the protocol 3GPP AKA is vulnerable to a variant of false base station attack. The flaw of 3GPP AKA allows an adversary to redirect user traffic from one network to another. It also allows an adversary to use the authentication vectors corrupted from one network to impersonate other networks; hence the corruption of one network may jeopardize the entire system. The redirection attack represents a real threat since the security levels provided by different networks are not always the same.

Zhu and Ma[3] proposed a new authentication scheme with anonymity for wireless environments. However, this shows that Zhu and Ma's scheme has some security weaknesses. Therefore, in this, a slight modification to their scheme is proposed to improve their shortcomings. As a result, the scheme proposed in this can enhance the security of The first is that it is based on the hash function and smart cards, and mobile users only do symmetric encryption and decryption. The second is that it takes only one round of message exchange between the mobile user and the visited network, and one round of messages exchange between the visited network and the corresponding home network. The third is that one-time use of key between mobile user and visited network is used.

They have pointed out that the Zhu–Ma scheme is not strong enough against some security weaknesses. Therefore, they have proposed a slight modification of the Zhu–Ma scheme. The proposed scheme does not only achieve their advantages but also enhances their security by withstanding the security weaknesses. In addition, the efficiency of their scheme is even higher than that of the original Zhu–Ma scheme.

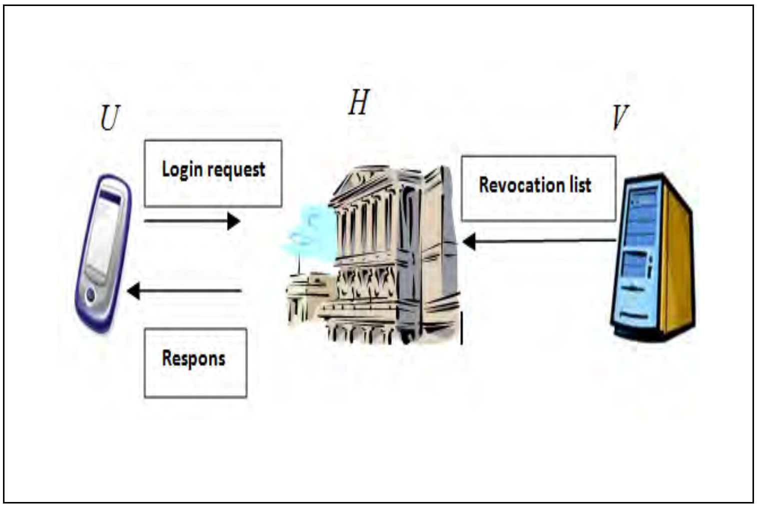


Fig 1: Overall design of the system

D. Boneh and H. Shacham [11] proposed revocation model that is motivated by privacy-preserving attestation. At a high level, one can consider three natural communication models for revoking a user's signing capabilities, without affecting other group members:

1. The simplest method revokes user i by issuing a new signature verification key and giving each signer, except user i, a new signing key. This requires an individual secret message to each signer and a public broadcast message to all verifiers.

2. A better revocation mechanism sends a single short public broadcast message to all signers and verifiers. A recent system by Camenisch and Lysyanskaya, based on dynamic accumulators, provides such a mechanism.

3. Brick all proposes a simpler mechanism where revocation messages are only sent to signature Verifiers, so that there is no need ever to communicate with an end-user machine. A similar mechanism was considered by Ateniese et al. and Kiayias et al. They refer to this as Verifier-Local Revocation (VLR) group signatures. Group signatures have recently become important for enabling privacy-preserving attestation in projects such as Microsoft's ngscb effort (formerly Palladium). Revocation is critical to the security of such systems. They construct a short group signature scheme that supports Verifier- Local Revocation (VLR). In this model, revocation messages are only sent to signature verifiers (as opposed to both signers and verifiers). Consequently there is no need to contact individual signers when some user is revoked. This model is appealing for systems providing attestation capabilities. Their signatures are as short as standard RSA signatures with comparable security. Security of their group signature (in the random oracle model) is based on the Strong Diffie Hellman assumption and the Decision Linear assumption in bilinear groups. They give a precise model for VLR group signatures and discuss its implications. They have described a short group signature scheme where user revocation only requires sending revocation information to signature verifiers, a setup they call verifier-local revocation. Their signatures are short: only 141 bytes for a standard security level. They are shorter than group signatures built from the Strong-RSA assumption and are shorter even than BBS short group signatures, which do not support verifier-local revocation.

III. PROPOSED SCHEME

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

A. Creation of a Wireless networks

The wireless communication network is created by five steps they are as follows Server, Base Station (Visiting Location Register-VLR), GSM Operation Center (Home Location Register – HLR), Gate Way and Client.

Server : Server Side modules consists of VLR and HLR coding of each mobile stations and also modules for different network group.GSM subscribers use the mobile stations to make and receive calls. Mobile stations are the combinations of Subscriber Identity Mobile (SIM) and mobile equipment. Base Station (Visiting Location Register-VLR): Mobile Subscribers communicate with a base transceiver station (BTS) over radio interface. Base station generally takes the up-link radio signals from MS and converts it into data for transmission to other machines within the GSM network and vice versa. GSM Operation Center (Home Location Register – HLR):

The center is responsible for accepting mobile subscribers to the system, route the communications between mobile subscribers. HLR is a main database of subscriber information of the GSM operator. It interacts with mobile switching center, which is a center call and control processing

Gate Way: This is responsible for the user's communications among different networks. This module is the high level mobile switching centre. This provides Multitier Mobile Communication.

Client: Mobile Clients are more sensitive on computation time than PC's, their capacity is restricted both on memory and CPU and also usually their processors are using 16 bit architecture instead of 32 or 64 bit. The mobile client modules are implemented in Java.

B. *Pre Authentication Protocol*

Implementation of pre-authentication of protocol between two devices that wish to communicate with each other at this or a later time. In this phase either a secret key or an authentic copy of a public key are securely shared between the devices. Authentication delay plays an important factor in the overall handover delay[13]. In this paper we assume that delays that constitute handover delay, other than authentication delay, like AP scanning delay and MIP registration delay have an equal effect on all authentication scenarios. Authentication delay is calculated starting from sending *EA*P Request/Identity message and ends by invoking the 4-way handshake protocol. Keys can be shared during pre-authentication using the pre-authentication models:

1) VLR-GS. Keygen (N, T): The group manager runs this algorithm. This algorithm takes as input integers N, $T \epsilon \mathbb{N}$ indicating the number of subscribers (i.e., users) and the number of time intervals, respectively. Its output consists of a master public key mpk, a vector of N subscribers' secret keys usk = (usk[1], . . ., usk[N]) and a vector of N × T revocation tokens urt=(urt[1][1], . . . , urt[1][T], urt[2][1], . . ., urt[2][T], . . . , urt[N][T]), where urt[i][j] denotes the revocation token of user Ui at time interval j.

2) VLR-GS. Sign (mpk, [i], j,): This algorithm takes the master public key mpk, u[i], the current time interval j and a message $M\epsilon\{0, 1\}^*$, and outputs a group signature σ. VLR-GS.Sign (mpk, [i], j,): We assume that a signed message $M\epsilon\{0, 1\}^*$ includes the time interval j in order to bind the signature to the interval. The algorithm is as follows.

- Select random number α, β, δ $\epsilon_R Z^*_p$.
- Compute $T1 = A_i\tilde{}g^{\alpha}$, $T2 = g^{\alpha\tilde{}}g^{\beta}$, $T_3 = (g^{x}{}_i, h_j)$, and $T4 = g^{\delta}$.
- Compute $V = \{(\alpha, \beta, \delta, x_i,) : T1 = A_i\tilde{}g^{\alpha} \wedge T_2 = g^{\alpha\tilde{}}g^{\beta} \wedge T_3 = e(g^{x}{}_i, h_j)^{\delta} \wedge T_4 = g^{\delta} \wedge e(A_i, wg^{x}{}_i) = e(g, g)\}(M)$. For simplicity, the detailed description of the signature from zero-knowledge proofs of knowledge (SPK) is omitted in this paper.
- Output the group signature $\sigma = (T_1, T_2, T_3, T_4,\ )$.

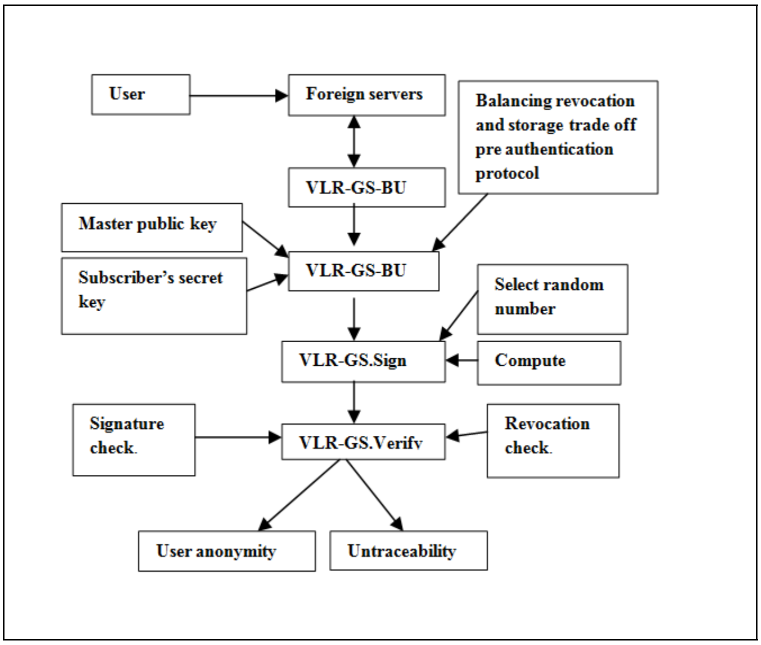


Fig 2: Overall design of Priauth

3) VLR-GS.Verify (mpk, j, RL_j, σ,): It takes as input mpk, the interval j, a set of revocation tokens RLj for interval j, a signature σ, and the message M. It outputs either "valid" or "invalid". The former output denotes that σ is a correct signature on M at interval j with respect to mpk, and the signer is not revoked at interval j.

VLR-GS.Verify (mpk, j, RL_j, σ, M): The inputs are $mpk = (g, \tilde{}g, h_1, . . ., h_T, w)$, the current time interval j, the revocation list RL_j that consists of $urt[i][j]$ for all revoked U_i at interval j, a target signature $\sigma = (T_1, T_2, T_3, T_4, V)$, and the message $M\epsilon\{0, 1\}^*$. This algorithm can perform two functions:

- Signature check. Check that σ is valid, by checking the .
- Revocation check. Check that the signer is not revoked at interval j, by checking $T_3 \neq (T_4, B_{ij})$ for all $B_i \in RL_j$.

4) Hierarchical Key Management Algorithm: In hierarchical algorithm, smaller basic structures in a hierarchical fashion are composed. The parameter d is the number of elements in a basic structure and can be considered as the degree of the hierarchy. We note that the degree can be different for different nodes in the hierarchy. However, for the sake of simplicity, the nodes in the hierarchical structures have auniform degree d. the basic structures of the form <R,R_1,R_2,R_d> is associated with the shared keys. The structure at next higher level,The personal key associated with $R_{i,}$1<i<d in structure <R_i,u_{i1},u_{i2},u_{id}>is the same as the group key of the structure hRi; ui1; ui2; . . . ; uidi. Furthermore, the structure is <R,R_1,R_2,R_d> associated with shared keys. Now, each user in the basic structure <R_i,u_{i1},u_{i2},u_{id}>is provided with any shared key that is provided to Ri in the structure <R,R_1,R_2,R_d>. For example, d = N, 2, 3, 4. In the hierarchical structure, the key associated with a subset {a, b, . . . , z} is denoted by $k_{ab...z}$.

C. Elliptic Curve Parameter Selection

An implementation of an elliptic curve cryptosystem requires a number of decisions to be taken at different hierarchy levels depending on the underlying hardware and implementation goals that need to be achieved.

At the field level:

- Selection of the underlying eld (could be F $_2$m, Fp or $F_p{}^m$).
- Choosing the ¯eld representation (e.g., polynomial basis or normal basis).
- Field arithmetic algorithms for ¯eld addition (subtraction), multiplication, reduction and inverse.

At the elliptic curve level:

- Choosing the type of representation for the points (affine or projective co-ordinates).
- Choosing a point addition and doubling algorithm.

At the protocol level:

- Choosing the appropriate protocol (key-exchange or signature).
- Choosing the algorithm for scalar multiplication k ¢ P.

Elliptic Curve Digital Signature Algorithm is implemented over elliptic curve P-192 as mandated by ANSI X9.62 in C language. The Project contains necessary modules for domain parameters generation, key generation, signature generation, and signature verification over the elliptic curve. ECDSA has three phases, key generation, signature generation, and signature verification.

ECC is a relative of discrete logarithm cryptography. An elliptic curve E over Zp as in Figure 1 is defined in the Cartesian coordinate system by an equation of the form:

$$y2 = x3 + ax + b \quad (1)$$

1) ECDSA Key Generation: An entity A’s key pair is associated with a particular set of ECdomain parameters D= (q, FR,a, b, G, n, h). E is an elliptic curve defined over Fq , and P is a point of prime order n in E(Fq),q is a prime. Each entity A does the following:

1. Select a random integer d in the interval [1, n- 1].
2. Compute Q = dP.
3. A’s public key is Q, A’s private key is d.

2) ECDSA Signature Generation:To sign a message m, an entity A with domain parameters D= (q,FR, a, b, G, n, h) does the following:

```
Input: Public point $P$ in $E(K)$ of order $n$, private key $d$ and message $m$.
Output: Signature $(r; s)$
Select a $k$ 2 [1; $n$ ¡ 1].
Compute $kP = (x1; y1)$ and convert $x1$ to an integer ^$x1$.
Compute $r$ = ^$x1$ mod $n$. If $r = 0$ then repeat from step 1.
Compute $e = H(m)$.
Compute $s = k$¡1$(e + dr)$ mod $n$. If $s = 0$ then repeat from step 1.
Return $((r; s))$
```

3) ECDSA Signature Verification: To verify A’s signature (r, s) on m, B obtains an authenticated copy of A’s domain parameters D = (q, FR, a, b, G, n, h) and public key Q and do the following

```
Input: Public point $P$ in $E(K)$ of order $n$, public key $Q$, message $m$ and
signature $(r; s)$.
```

```
 Output: Accept or Reject signature
Verify if $r; s\ 2\ [1; n\ ¡\ 1]$; else Return("Reject signature").
Compute $e = H(m)$.
Compute $w = s¡1 \bmod n$.
Compute $u1 = ew \bmod n$ and $u2 = rw \bmod n$.
Compute $X = u1P + u2Q = (x1; y1)$.
If $X = O$ then Return("Reject signature");
 Convert $x1$ to an integer $\hat{}x1$; Compute $v = \hat{}x1 \bmod n$.
If $v = r$ then Return("Accept signature"); Else Return("Reject signature");
```

D. User Join & Leave Mechanisms

A new user joining is about allowing a new user to register to a server after system setup. To support dynamic participation, an authentication scheme should support new user joining. For the above protocol, however, this new user joining mechanism no longer works. A feasible new user joining mechanism is added into Priauth as follows. We assume a user U_n hopes to register to a server H during interval j_n. After verifying U_n's information, as the group manager of an independent VLR-GS-BU system, H selects $x_n є_R Z^*_p$ and computes $A_n = g_1/(\gamma+x_n)$. After that, it computes $B_{nj} = h_{xn}\ j$ for all $jє[j_n, T\ ]$. The master public key mpk is still $(g,\ \tilde{}g,\ h_1, \ldots, h_T, w)$. Un's secret key $[n]$ is (A_n, x_n). The revocation token at interval j of user Un is $[n][j] = B_{nj}$, where $jє[j_n, T\ ]$. The length of the master public key of H but also the number of revocation tokens is linear to . The master key of H is stored on every subscriber of H while the revocation tokens are stored on H.

The probability that the bounding box of a new user u overlaps with some active user u' is given by equation 1. Therefore, the key update cost is N*Proverlap. For every user u0 whose subscription range overlaps with user u, the key server has to break up the bounding box into an average of 2_d sub-boxes.

$$P_{r\ overlap} = \frac{\prod_{i=1}^{d}(2x_i)}{\prod_{i=1}^{d} i_{max}} = 2^d \prod_{i=1}^{d} \frac{x^i}{x^i_{max}} \tag{1}$$

Figure 3 illustrates the creation of new sub-boxes are new users join the system for a d=2 dimensional domain. The
size of the average key update message for every overlapping user u ' is 2d keys. Therefore, the total cost of a new user join using the group key management is given by Equation 2.

$$Cost_{gkm} = 2^d * N * 2^d \prod_{i=1}^{d} \frac{x^i}{x^i_{max}} \tag{2}$$

The cost of a new user join in our key management protocol is $Cost_{our} = 2^{d-1} * \frac{\sum_{i=i}^{d} log x^i}{d}$ The ratio of the costs is given by Equation 3.

$$cost_{gkm} : Cost_{our} = \frac{2^{d+1} * N * d}{\sum_{i=i}^{d} log x^i} \prod_{i=1}^{d} \frac{x^i}{x^i_{max}} \tag{3}$$

Let us suppose that the subscription range along each dimension x_i = x and the maximum subscription range along each dimension X $^{i}{}_{max}$ = Xmax.

Let us suppose that the subscription range along each dimension x_i = x and the maximum subscription range along each dimension X $^{i}{}_{max}$ = Xmax.

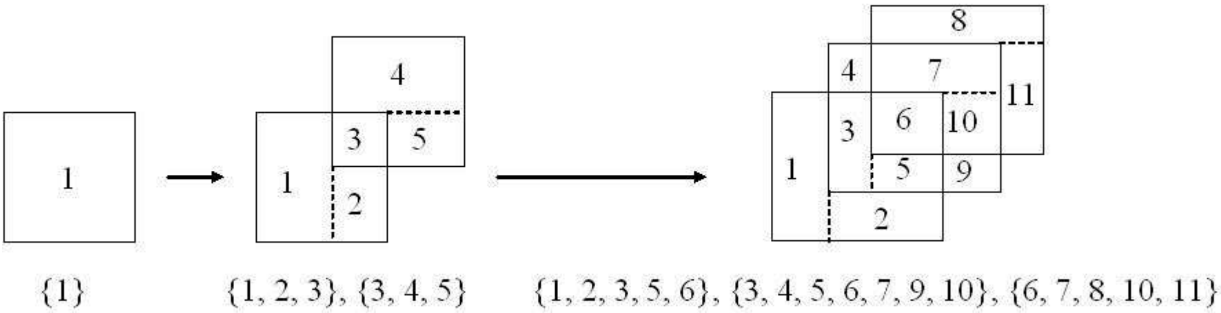


Fig 3: User Join: Group Key Management

E. *Balancing Revocation and Storage Trade-off*

The protocol VA needs to interrupt the communication during the rekeying; the resulting delay can be unreasonable for many applications. Thus, efficient distribution of the new key for multiple membership changes is a critical problem in secure group communication. One approach to revoke multiple users is to associate a key with every nonempty subset of users in the group. Thus, if one or more users are revoked, the VA uses the key associated with the subset of the remaining users to encrypt the new key and transmits the new group key to them. The advantage of this approach is that the communication overhead is only one message for revoking any number of users. In a hierarchical structure like a tree, we have some auxiliary keys, which divide a group into several subgroups. We call these auxiliary keys as Administrative keys. The administrative keys are used only for rekeying operations that take place when group membership changes. An authorization key Ka,b to the user u. This ensures that:

- Given Ka,b a user u can efficiently derive Kt,t if a _ t _b.
- Given Ka,b it is computationally infeasible for a user u toguess Kt,t if t < a or t > b.

The primitive described above helps us to construct a very simpleand efficient protocol for temporal access control on broadcast services.At any given time instant t, the service provider broadcastsa packet P (of say, audio/video data) as follows:

- Get current time instant t and compute Kt,t.
- Broadcast ht, EKt,t (P), MACtt,t (P)i.EK(x) and MACK(x) denote an encryption and a message authenticationcode of a string x respectively. Note that all users

can potentially receive the broadcast message. An authorized subscriberdecrypts the payload P as follows:

- Receive the broadcast message ht, EKt,t (P),MACKt,t (P)i.Note that the time instant t is in plain-text.
- A subscriber is authorized if it has a temporal authorizationfor some time period (a, b) such that a _ t _ b. An authorized subscriber can compute the decryption key Kt,t from Ka,b, decrypts the broadcast message to obtain the payload P and checks its integrity.

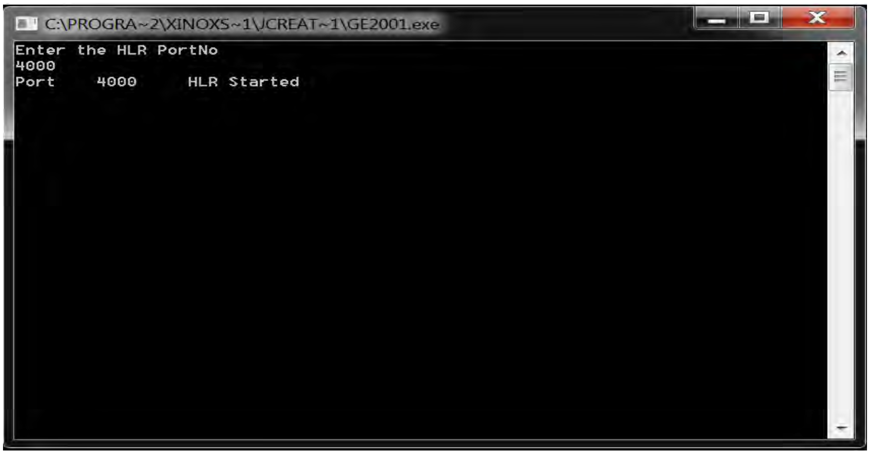
The property of the authorization key Ka,b ensures that one canefficiently compute Kt,t from Ka,b if and only if a _ t _ b. In the following section, we present an algorithm to efficiently and securely construct such keys using hierarchical key graphs.

```
Algorithm 1: Key Derivation
Input: t, K $_{a,b}$
Output: K t,t
          DERIVE(t, K $_{a,b}$)
if t < a or t > b
 return ?
          mid   a+b
 if t = mid
return K $_{a,b}$
 if t < mid
          Ka,mid   H(K $_{a,b}$, 0)
 return DERIVE(t, K$_a$,mid)
 else
           Kmid+1,b   H(Ka,b, 1)
return DERIVE(t, Kmid+1,b)
```

Identify the Headings

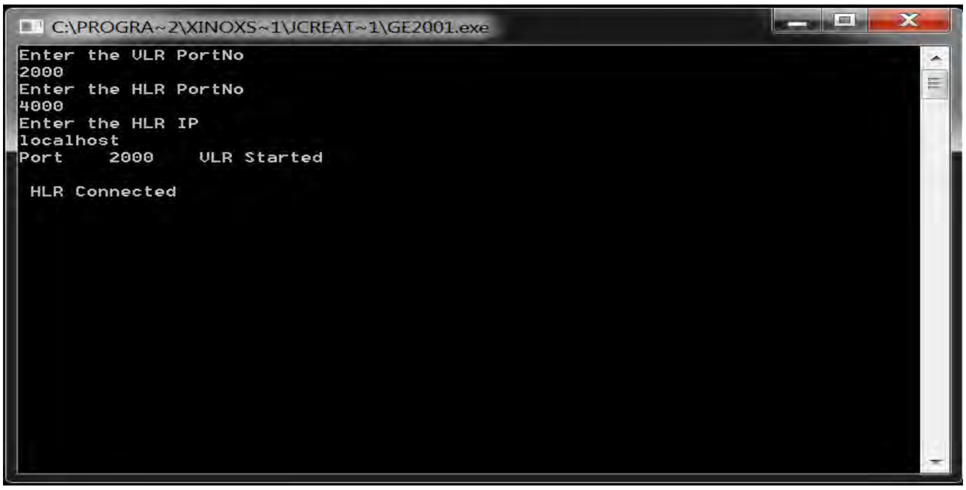
IV. EXPERIMENTAL RESULTS

Fig3,4,5 shows the home location register, visitor location register and user. It also shows how it get stated using the port number and the local host by VLR-GS-BU algorithm. The user is login by the user name. Fig6.shows the message authentication operations such as ECDSA Elliptic Curve Scalar Multiplication (ECSM) operation for signing, Multi-ECSM operation for verifications are very high. Fig6.shows the message authentication operations such as ECDSA Elliptic Curve Scalar Multiplication (ECSM) operation for signing, Multi-ECSM operation for verifications are very high. Fig .7,8 shows key generated in the home location and visitor location and the session is also generated. For evaluating the effectiveness of proposed system we calculate key generation complexity for both systems and prove that



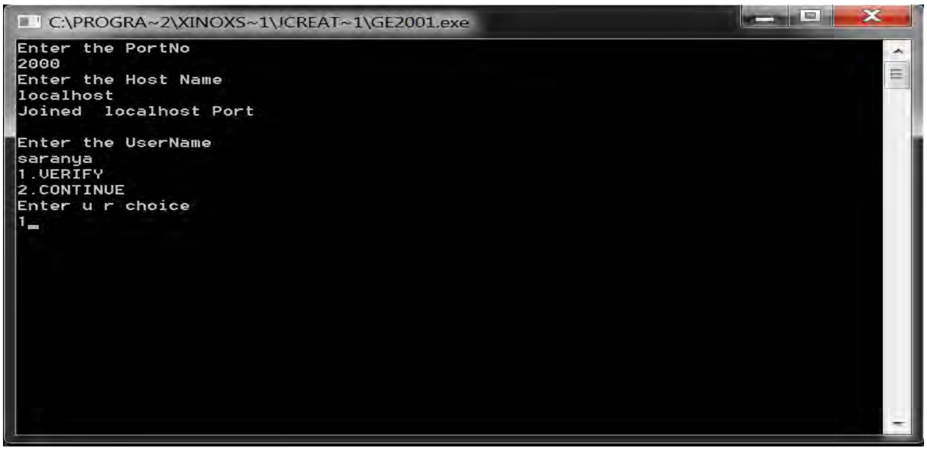
```
Enter the HLR PortNo
4000
Port    4000     HLR Started
```

Fig 4: HLR image



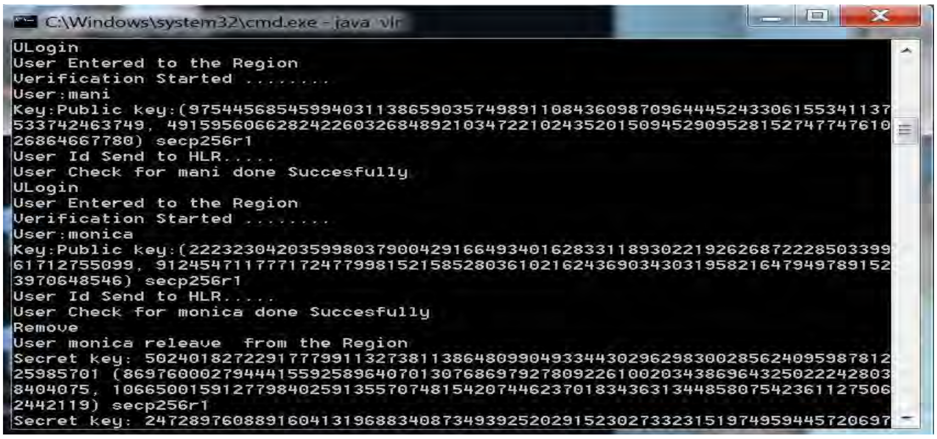
```
Enter the VLR PortNo
2000
Enter the HLR PortNo
4000
Enter the HLR IP
localhost
Port    2000     VLR Started

 HLR Connected
```

Fig 5: VLR image



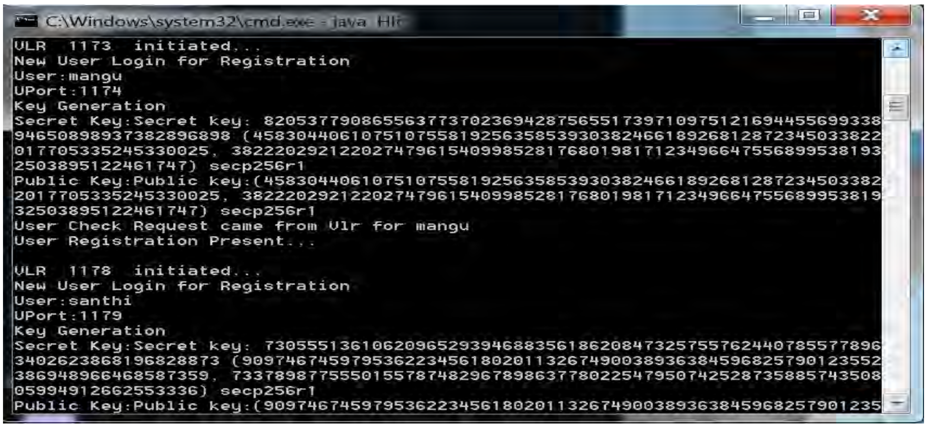
```
Enter the PortNo
2000
Enter the Host Name
localhost
Joined  localhost Port

Enter the UserName
saranya
1.VERIFY
2.CONTINUE
Enter u r choice
1_
```

Fig 6: User login using VLR-GS-BU



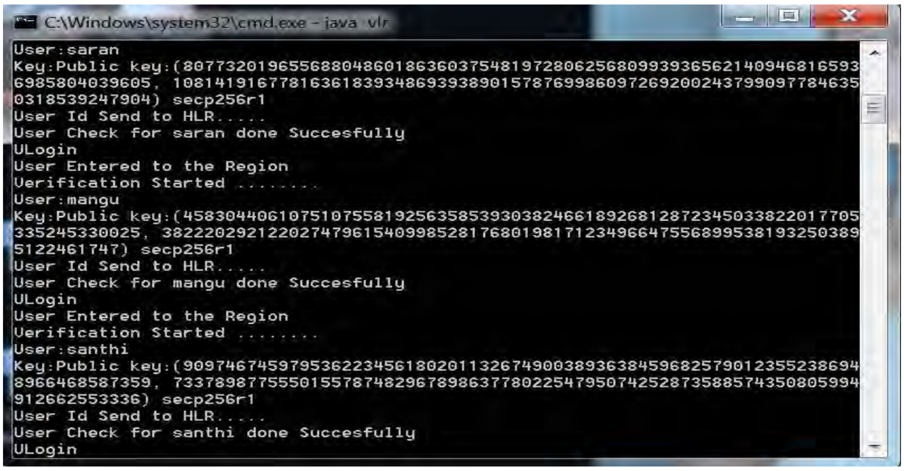
```
ULogin
User Entered to the Region
Verification Started .........
User:mani
Key:Public key:(97544568545994031138659035749891108436098709644452433061553411137
533742463749, 4915956066282422603268489210347221024352015094529095281527477476 10
26864667780) secp256r1
User Id Send to HLR.....
User Check for mani done Succesfully
ULogin
User Entered to the Region
Verification Started .........
User:monica
Key:Public key:(22232304203599803790042916649340162833118930221926268722285033 99
61712755099, 9124547117771724779981521585280361021624369034303195821647949789152
3970648546) secp256r1
User Id Send to HLR.....
User Check for monica done Succesfully
Remove
User monica releave  from the Region
Secret key: 502401827229177799113273811386480990493344302962983002856240959878 12
25985701 (869760002794441559258964070130768697927809226100203438696432502224 2803
8404075, 106650015912779840259135570748154207446237018343631344858075423611275 06
2442119) secp256r1
Secret key: 247289760889160413196883408734939252029152302733231519749594457206 97
```

Fig 7: User Releave



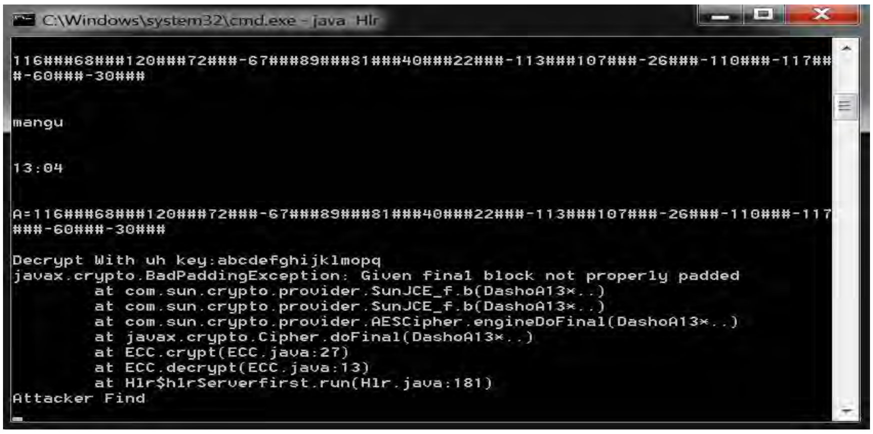
```
VLR  1173  initiated...
New User Login for Registration
User:mangu
UPort:1174
Key Generation
Secret Key:Secret key: 820537790865563773702369428756551739710975121694455699338
9465089893738289 6898 (4583044061075107558192563585393038246618926812872345033822
0177053352453300 25, 382220292122027479615409985281768019817123496647556899538193
2503895122461747) secp256r1
Public Key:Public key:(4583044061075107558192563585393038246618926812872345033 82
2017705335245330025, 382220292122027479615409985281768019817123496647556899538 19
32503895122461747) secp256r1
User Check Request came from Vlr for mangu
User Registration Present...

VLR  1178  initiated...
New User Login for Registration
User:santhi
UPort:1179
Key Generation
Secret Key:Secret key: 7305551361062096529394688356186208473257557624407855778 96
340262386819682887 3 (9097467459795362234561802011326749003893638459682579012 3552
3869489664685873 59, 7337898775550155787482967898637780225479507425287358857435 08
05994912662553336) secp256r1
Public Key:Public key:(9097467459795362234561802011326749003893638459682579012 35
```

Fig 8: HLR Database



```
User:saran
Key:Public key:(80773201965568804860186360375481972806256809939365621409468165936985804039605, 108141916778163618393486939389015787699860972692002437990977846350318539247904) secp256r1
User Id Send to HLR.....
User Check for saran done Succesfully
ULogin
User Entered to the Region
Verification Started ........
User:mangu
Key:Public key:(45830440610751075581925635853930382466189268128723450338220177053352453300025, 38222029212202747961540998528176801981712349664755689953819325038951224617477) secp256r1
User Id Send to HLR.....
User Check for mangu done Succesfully
ULogin
User Entered to the Region
Verification Started ........
User:santhi
Key:Public key:(90974674597953622345618020113267490038936384596825790123552386948966468587359, 73378987755501557874829678986377802254795074252873588574350805994912662553336) secp256r1
User Id Send to HLR.....
User Check for santhi done Succesfully
ULogin
```

Fig 9: VLR Database



```
116###68###120###72###-67###89###81###40###22###-113###107###-26###-110###-117##
#-60###-30###


mangu


13:04


A=116###68###120###72###-67###89###81###40###22###-113###107###-26###-110###-117
###-60###-30###

Decrypt With uh key:abcdefghijklmopq
javax.crypto.BadPaddingException: Given final block not properly padded
        at com.sun.crypto.provider.SunJCE_f.b(DashoA13*..)
        at com.sun.crypto.provider.SunJCE_f.b(DashoA13*..)
        at com.sun.crypto.provider.AESCipher.engineDoFinal(DashoA13*..)
        at javax.crypto.Cipher.doFinal(DashoA13*..)
        at ECC.crypt(ECC.java:27)
        at ECC.decrypt(ECC.java:13)
        at Hlr$hlrServerfirst.run(Hlr.java:181)
Attacker Find
```

Fig10: Attacker node

Fig. 7,8 shows key generated in the home location and visitor location and the session is also generated. For evaluating the effectiveness of proposed system we calculate key generation complexity for both systems and prove that proposed system is less complex than existing.

Table I
Comparison between YHWD, YWD, Priauth and Balancing Revocation

Protocols	Numbers of Parties	Universal	Resistance to DOS attack	Perfect Forward Secrecy	User Untraceability	Revocation cost
YHWD	2	Yes	No	No	No	No
YWD	3	No	No	No	Yes	No
PRIAUTH	2	Yes	Yes	Yes	Yes	No
BALANCING REVOCATION	3	Yes	Yes	Yes	Yes	Yes

SSL specification, has been introduced into the implementation of Priauth. The same experiment is performed ten thousand times and average is taken over them. Table-I, shows the comparison between YHWD, YWD and Priauth We assume the access device of a roaming user runs on a 798 MHz processor, thus it takes 39.7 ms (plus 35.7 ms pre-computed). For new user joining, it just takes ($T-jn$+2) ECSM computations on H while the new user does not need to do any computations.

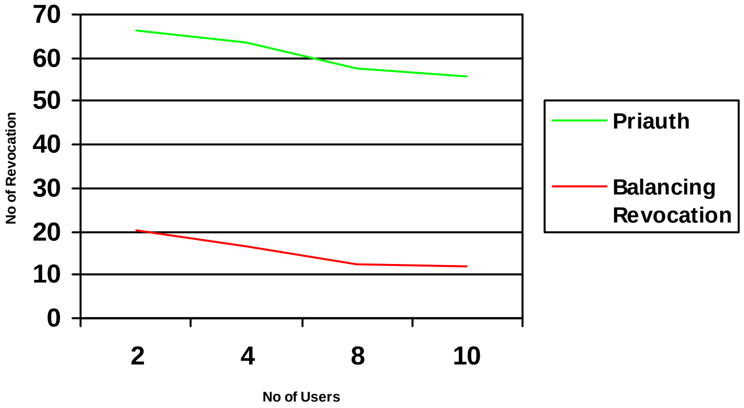


Fig 11: Number of users revoked

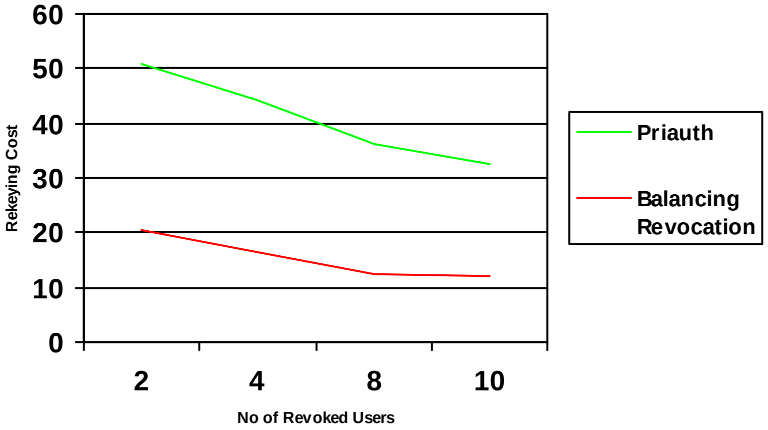


Fig 12: Rekeying Cost

Fig. 10 &11 shows the number of users Vs revocation varying in priauth and balancing revocation using the hierarchical key management for reducing the complexity. The number of users vs rekeying cost is varied between the pre-authentication and balancing revocation in order to reduce the rekeying.

V. CONCLUSION

The proposed a novel protocol to achieve privacy-preserving universal authentication for wireless communications. Thus provide a trade-off between the number of keys maintained by the users and the time required for rekeying due to the revocation of multiple users. This enables the group controller to deal with heterogeneous set of users that have different capabilities. With this capability, users with high capability can benefit from it (by reducing the rekeying cost), while users with low capability can still participate. We also showed that our algorithm can provide differential service to users that are long term versus those that are short term. Such hybrid schemes provide additional options for the group controller to adapt to heterogeneous systems where users have varying requirements and capabilities. Thus for the future work the maximum Distance Separable code(MDS) cryptography can be used to improve the complexity in the enhancements.

REFERENCES

[1] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A strong user authentication scheme with smart cards for wireless communications , "Computer Commun., 010,doi:10.1016/j. comcom.2010.02.031.

[2] G. Yang, Q. Huang, D. S. Wong, and X. Deng,"Universal authentication protocols for anonymous wireless communications," IEEE Trans. Wireless Commun., vol. 9, no. 1, pp. 168-174, 2010.

[3] G. Yang, D. S. Wong, and X. Deng, "Anonymous and authenticated key exchange for roaming networks," IEEE Trans. Wireless Commun., vol. 6, no. 9, pp. 3461-3472, 2007.

[4] G. Yang, D. Wong, and X. Deng, "Deposit-case attack against secure roaming," in Proc. ACISP'05, 2005.

[5] D. He and S. Chan, "Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks," Wireless Personal Commun., 2010, doi: 10.1007/s11277-010- 0033-5M.

[6] Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," IEEE Trans. Wireless Commun., vol. 4, no. 2, pp. 734-742, 2005

[7] C. C. Lee, M. S. Hwang, and I. E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," IEEE Trans. Consumer Electron., vol. 53, no. 5, pp 1683-1687, 2006.

[8] C. C. Wu, W. B. Lee, and W. J. Tsaur, "A secure authentication scheme with anonymity for wireless communications," IEEE Commun. Lett. vol. 12, no. 10, pp. 722-723, 2008.

[9] J.-L. Tsai, "Efficient multi-server authentication scheme based on one way hash function without verification table," Computers & Security, vol. 27, no. 3-4, pp. 115-121, 2008.

[10] H.-C. Hsiang and W.-K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment," Computer Standards & Interfaces, vol. 31, no. 6, pp. 1118-1123, 2009.

[11] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in Proc. ACM CCS'04, pp. 168-177, 2004.

[12] T. Nakanishi and N. Funabiki, "Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps," in Proc. ASIACRYPT'05, LNCS, vol. 3788, pp. 533-548, 2005.

[13] ANSI X9.62 "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)," 1999.

[14] "Pairing based cryptography benchmarks." [Online]. Available: http://crypto.stanford.edu/pbc/.

AUTHORS PROFILE

Ms.M.Saranya has received Bachelor of Technology degree in Information Technology under Anna University, Chennai in 2010. She is currently pursuing Master of Engineering degree in Computer Science and Engineering under Anna University, Coimbatore, India. Her areas of interest are wireless networks.

Ms.P.Dhivya received B.Tech (CSE), M.Tech (CSE) in 2006 and 2009 respectively from Anna university. Since 2010, she has been working as faculty in reputed Engineering Colleges. At Present, she is working as Assistant Professor(SG) in the department of Computer Science & Engineering, Sri Krishna College of Technology, Coimbatore. Her interests include Image Processing, Data Mining.