Secure Authentication Scheme with User Privacy for Wireless Network Environment

K.Aarthy Meena
Department of Computer Science and Engineering, Sethu Institute of Technology, Virudhunagar, Tamil Nadu, India
aarthymeena@ymail.com

Abstract **- Mobile users enjoy seamless roaming over wireless environment. The wireless network is cumbersome and error prone, thus there is a need for a good and strong authentication scheme which should be designed in such a way that it retains the privacy of the user .It should also be capable of providing minimized communication overhead as most of the exchange of messages in wireless network is found to be the exchange of messages meant for authentication. This results in clumsy environment .The proposed scheme brings out the solution for the above mentioned problems, where the authentication procedure consists of only four messages exchanged between home agent, mobile user and foreign agent. Also the light weight authentication scheme with user anonymity is presented. Apart from that other main issues that are to be solved are prevention of fraud, updating of session key periodically, no need of password verification table and single registration of user to home network. It provides security in protecting the password even if the information is disclosed. The proposed scheme deserves the property of protecting the wireless network from various attacks. And the proposed scheme is simple and user friendly.**

Keywords **- Authentication, Smartcard, Security, Anonymity, Wireless networks**

I Introduction

A. Need for Authentication in Wireless Network Environment

Wireless Networks are increasing in popularity. They are being installed by businesses of all types, educational institutions,governments and the military. The reason is that WLANs provide users the access to their information in many locations, some of which are more conducive to collaboration. The freedom and mobility that WLANs promise also present some serious security challenges.

Before allowing entities to access a network and its associated resources, the general mechanism is to authenticate the entity (a device and/or user) and then allow authorization based on the identity. The most common access control is binary: It either allows access or denies access based on membership in a group. Authentication is a security primitive which enables a node to ensure the identity of the peer node it is communicating with. Authentication is the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true.

A complete information assurance risk assessment requires a focus on the threats against the three key components of assuring information. That is, the information system should protect against confidentiality, integrity, and availability (CIA) attacks. The authentication is based on a three-party model: the supplicant, which requires access; the authenticator, which grants access; and the authentication server, which gives permission. The supplicant has an identity and some credentials to prove that it is who it claims to be. The supplicant is connected to the network through an authenticator's port that is access controlled. The authenticator itself does not know whether an entity can be allowed access; that is the function of the authentication server.Various popular attacks are replay,dictionary attack, man in the middle attack, impersonation of user , impersonation of authenticator , DoS ,Data alteration. Thus the need for authentication is must in wireless environment.

B. Motivation of the Project

Authentication is a security primitive which enables a node to ensure the identity of the peer node it is communicating with. Authentication is the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true. Authenticating an object may mean confirming its provenance, whereas authenticating a person often consists of verifying their identity. Wireless communications technologies are undergoing rapid development, with the potential to provide high-speed and high quality information exchange between mobile devices (e.g., notebook computer, PDA and smart phone) located anywhere in the world. Through universal roaming technology in wireless networks, mobile users can obtain the services provided by the home network when he/she roams into a foreign network. Obviously,before providing services, the foreign agent needs to authenticate the user through the user's home agent.

A strong user authentication scheme in wireless networks should satisfy the following requirements: (1) User anonymity: The disclosure of a mobile user's identity could allow unauthorized entities to track his/her moving history and current location. (2) Low communication cost and computation complexity (3) Single registration (4) Update session key periodically:when a mobile user is always within the same foreign network (or his/her home network), the session key needs to be updated periodically.(5) User friendly: The authentication scheme should be easily used by users. (6) No Password verifier table (7) Update password securely and freely: It allows the card holder to update his/her password

freely after assuring the legality of cardholder. (8) Prevention of fraud (9) Prevention of replay attack

In this project,a secure and light-weight authentication scheme with better security strength while keeping the merits of the previous schemes .In our scheme, the required operations on mobile user are only one symmetric encryption/ decryption operation. Having this feature, it is more suitable for the low-power and resource-limited mobile devices.Also it requires four message exchanges between mobile user, foreign agent and home agent. This feature improves the communicational efficiency. Therefore, it is quite suitable for some lower bandwidth mobile communications. As a result, this protocol enjoys both computation and communication efficiency as compared to the well-known authentication schemes . Security analysis of our scheme will demonstrate that it can resist smart card security breach, fraud, off-line password guessing attack, insider attack and replay threats. In addition, we will show that the proposed protocol is able to provide user anonymity, single registration, user friendly, updating password securely and freely, and high efficiency in password authentication.

II Related Work

Lee [3] overcomes the drawback of Zhu et al.'s scheme which failed to provide anonymity and Lee et al.'s scheme which failed to possess the property of backward secrecy. It is very crucial that the identities of wireless users must be authenticated to prevent illegal use of resources.

Lee [3] tells that a good security protocol for wireless communications must not only provide high security but also low computation. Recently, Zhu and Ma proposed a new authentication scheme with anonymity for wireless environments . The scheme has some advantages as follows. 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. However, the Zhu–Ma scheme has three security weaknesses as follows.

a. It cannot achieve perfect backward secrecy.
b. It cannot achieve mutual authentication.
c. It cannot protect against a forgery attack.

Park [1] proposed a scheme that requires several hashing operations in both the smart card side and the server side, and it requires a very small quantity of transmission data. Because the efficiency of the smart card is mostly concerned, only the details of the smart-card efficiency are given. In the login phase, the smart card only performs one hashing operation.

Lee [4] proposed a method of integrating user authentication with anonymity and untraceability is presented based on the secret-key certificate and the algebraic structure of error-correcting codes. Authentication protocol proposed here provides a means for the authentication server to avoid the requirement of maintaining a secure database of user secrets.

III. Existing System

To provide an anonymity service for wireless communications, Zhu and Ma proposed a new authentication scheme. Lately, [4] pointed out that the scheme of Zhu and Ma has some security issues and then improved it. However, the original scheme of Zhu and Ma as well as the enhanced scheme fail to provide anonymity, and subsequently expose the identity of a mobile user to foreign agents. Besides, we find that [4] definition of perfect backward secrecy is actually backward secrecy, but their scheme does not possess this property. In this paper, both security issues will first be demonstrated before an effective remedy will be proposed.

Security analysis in existing system is discussed as follows, and the way how the system achieves anonymity and backward secrecy are mentioned below. Proposition 1: Existing system can achieve anonymity Proof: In this scheme, FA obtains $h(h(N||ID_{MU}))$ instead of $h(ID_{MU})$. Therefore, FA has no way of verifying whether the guessed identity is correct or not without the secret value N. Besides, deriving the $h(N||ID_{MU})$ from $h(h(N||ID_{MU}))$ is also intractable if h(.) is a secure hash function such as SHA-256.Thus, the off-line guessing attack cannot succeed.Proposition2: Existing system can accomplish backward secrecy Proof: In this system , the value $h(PW_{MU})||x$ is fixed for every session. If an attacker knows the session keys ki−1 and ki, then x_{i-1} will be obtained. Thus, he/ she can try to compute $h(PW_{MU})||x$ from .However, ki is an output value of a hash function h(.), and therefore deriving $h(PW_{MU})||x||x_{i-1}$ is intractable. That is, even though x_{i-1} is known by the attacker, $h(PW_{MU})||x$ will not be obtained by him/her.

IV Proposed Scheme

The protocol is divided into five phases: the registration phase, the login phase, the authentication phase, the session key update phase and the password change phase. In the registration phase, the home agent issues a smart card for a mobile user through a secure channel. In the login phase, a roaming user sends a login request message to a foreign agent. In the authentication phase, the visited foreign agent authenticates the mobile user through his/her home agent. After a validation, an authentication key is established between the foreign agent and the mobile user. If a mobile user is always within the same foreign network (or his/her

home network), the session key update phase can ensure the freshness of the session key. [4].

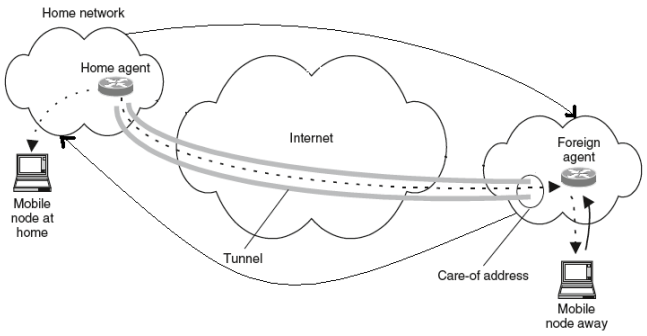

Fig. 1 Overall architecture

A. Registration Phase

Once the user enters into the network,the network to which a mobile user is associated with is called Home Agent(HA).The Mobile User(MU) must get registered to the Home Agent.For doing so ,it submits its identity which is the hashed value of a password and a randomly generated number.Then the HA computes necessary information ans it issues a smart card. .the contents of a smart card are $\{TK_{MU}, SK_{MU}, h(.),r\}$.

Where,

$$TK = h(ID_{MU}||x_{HA}) \quad (1)$$

$$SK = h(ID_{MU}||N) \quad (2)$$

$$r = TK_{MU}+ID_{HA}+(ID_{MU}||m)_n \quad (3)$$

Then MU computes SK_{MU}, V_{MU}, H_{MU}, and then it replaces TKMU with (V_{MU}, H_{MU}) and then it enters the entry in the smart card which is finally $\{V_{MU}, H_{MU}, SK*_{MU}, h(),r,d\}$. These are the steps that involve in Registration Module.

B. Service Requisition Phase

MU roams into the foreign network and tries to access service. Before providing services, the FA needs to authenticate the MU through HA. If the MU is a legal user of HA, the FA will issue a temporary certificate TCertMU to the MU, which will be used in the session key update phase when the MU communicates with this FA. As is shown in Fig 1. the steps of this phase are described as follows. For authentication, the MU inserts his/her smart card into the device and enters his/her identity IDMU and password PWMU. The card performs the following operations:

1.If $H_{MU} == H*_{MU}$ the request is initiated, where,$H*_{MU}=h(TK*)$,$TK*=V_{MU}+h(ID_{MU}||h(PW_{MU}+d)$.

2.Computation of E and N,Where $E=(h(ID_{MU})||ID_{FA}||x_O||x)_L$, $n=ID_{HA}+(ID_{HA}||M)_N$, x0 and x are two l-bits secret random numbers, and IDFA is the identity of the foreign agent which MU wants to login.A timestamp TMU is also selected by the MU to resist replay attacks. Note that the bit length of a timestamp is assumed to be 64 throughout this paper. The symmetric encryption algorithm used throughout the proposed scheme is DES. Under the DES algorithm, the bit length of plaintext is assumed to be X, thus the bit length of ciphertext should be [x/64]*64.Finally message M1 is sent which contains $M_1=\{n,E,ID_{HA},T_{MU}\}$ to FA as a service requisition message.

C. Verification Request Phase

On receiving message from the MU, the FA checks whether the timestamp T_{MU} is valid. If it is valid, the FA generates a random number b and computes its signature using the private key SFA. Afterwards, the FA sends the message M2 $=\{b,n,E,T_{MU},T_{FA},ES_{FA}(h(b,n,E,T_{MU},Cert_{FA}))$ to HA. After receiving the message from the FA, HA decides whether the certificate CertFA and timestamp TFA are valid. If they are not valid, HA terminates the execution. Otherwise, HA verifies the signature using FA's public key PFA. If the signature is invalid, HA rejects this message; otherwise, HA computes as follows: Then, HA decrypts the value by using the secret value N to obtain the MU's real identity IDMU. Subsequently, HA verifies whether the MU is a legal user. If it is not a legal user, HA sends the message"This user is an illegal user." to FA. Otherwise, HA decrypts E to obtain ID_{FA}; x and x0. After the operations above, HA compares ID_{FA} from E with the identity of the FA derived from the certificate $Cert_{FA}$. Note that as is described above, the certificate $Cert_A$ of entity A contains the identity ID_A of entity A, the public key PA of entity A, etc. If it does not hold, the HA sends the message "This user does not match FA". Otherwise, HA identifies the MU to be a legal user and then computes W as follows and its signature $ES_{fa}(h(b,n,E,T_{MU},Cert_{FA}))$, where c is a random number generated by HA.

D. Verification Response Phase

HA sends the message m3 $\{c,W,T_{HA},ES_{HA}(h(b,c,W,T_{MU},Cert_{HA})),Cert_{HA})$ to FA. With the message from HA, FA first checks whether the timestamp T_{HA} is extinct. If THA is invalid, FA will reject this message. Otherwise, FA verifies the signature using HA's public key PHA. If the signature is invalid, FA rejects this message; otherwise, FA decrypts W with its private key SFA. to obtain $h(h(N||ID_{MU}))$; x0 and x. Thus, the session key $k =h(h(h(N||ID_{MU}))||x||x_0)$ between FA and the MU can be derived. Then FA gives a response $(TCert_{MU}(h(x_0||x))_k$ to the MU. Here TCertMU includes lifetime and other information. Here the bit length of TCertMU is assumed to be 256.Cert And T_{FA} are validated and the signature is validated using the private key of HA which is Es_{HA}.Then the decryption of n is done from which ID_{MU} is obtained. MU is verified and the decrypted value is $E=(h(ID_{MU})||ID_{FA}||x_O||x)_L$.once the value is decrypted, Comparision Of ID_{FA} on E and ID_{FA} on $Cert_{FA}$ id

one if the result is same in both cases the computation of W is done, $W=EP_{FA}(h(h(N||ID_{MU}))||x_0||x)$. Message M_3 is sent from HA to FA. $M_3=\{c,W,T_{HA},ES_{HA}(h(b,c,W,T_{MU},Cert_{HA})), Cert_{HA}\}$.

E. Service Response and Session Establishment Phase

After receiving the message from FA, the MU computes the session key k and then decrypts $(TCert_{MU}(h(x_0||x)_k$ to obtain the temporary certificate $TCert_{MU}$. Besides, the MU can perform authentication to FA. He can compute $h(x_0||x)$ and compare the value with the received h(x0||x). If the two results are identical, the MU confirms that FA is authenticated by HA.Therefore, the MU can make sure that it is communicating with a legitimate FA. So far, FA has finished the authentication to the MU and established session keys.$M4=Cert_{MU}(h(x_0||x)_k$.

V. Experimental Results

On implementing the above mentioned scheme,the computation complexity could be reduced and the cost of communication overhead is also reduced.

Apart from this, the wireless environment is protected from replay and impersonation attack.

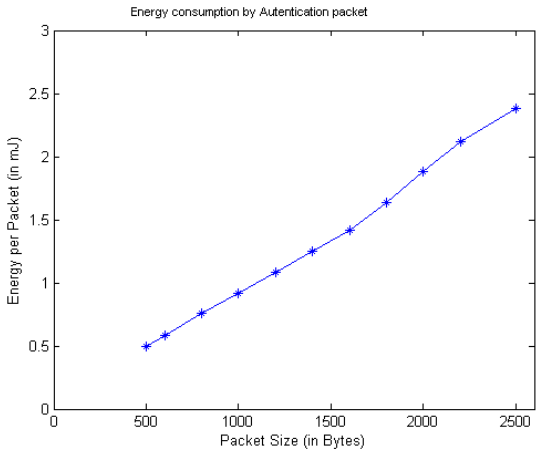

Fig 5.1 Graph showing energy consumption

VI. Conclusion And Future Enhancement

This work has revealed that some security weaknesses in some recently proposed smart card based authentication schemes for wireless environments. Moreover, a secure and light-weight user authentication scheme has been proposed. Security analysis has demonstrated that our protocol is able to provide mutual authentication with user anonymity and is effective in protecting from various attacks. There are number of ways in extending this project.One among them is to reduce the number of computations involved and to introduce a new algorithm called ECC algorithm instead of DES algorithm that is used for the purpose of encryption and decryption.

References

[1] C.-S. Park, Authentication protocol providing user anonymity and untraceability in wireless mobile communication systems, *Computer Networks* 44 (2004) 267–273.

[2] H.-Y. Chien, J.-K. Jan, Y.-M. Tseng, An efficient and practical solution to remote authentication: smart card, Computers & Security 21 (4) (2002) 372–375.

[3] C.C. Lee, M.S. Hwang, I.E. Liao, Security enhancement on a new authentication schemewith anonymity for wireless environments, *IEEE Transactions on Consumer Electronics* 53 (5) (2006) 1683–1687.

[4] C.C. Wu, W.B. Lee, W.J. Tsaur, A secure authentication scheme with anonymity for wireless communications, *IEEE Communication Letter* 12 (10) (2008) 722–723.

[5] P. Zeng, Z. Cao, K.-K.R. Choo, S. Wang, On the anonymity of some authentication schemes for wireless communications, *IEEE Communication Letter* 13 (3) (2009) 170–171.

[6] J.-S. Lee, J.H. Chang, D.H. Lee, Security flaw of authentication scheme with anonymity for wireless communications, *IEEE Communication Letter* 13 (5) (2009) 292–293.

[7] J. Xu, D. Feng, Security flaws in authentication protocols with anonymity for wireless environments, *ETRI Journal* 31 (4) (2009) 460–462.

[8] J.-L. Tsai, Efficient multi-server authentication scheme based on one-way hash function without verification table, Computers & Security 27 (3-4) (2008) 115–121.

[9] Y.-P. Liao, S.-S. Wang, A secure dynamic ID based remote user authentication scheme for multi- server environment, *Computer Standards & Interfaces* 31 (1) (2009) 24–29.

[10] H.-C. Hsiang, W.-K. Shih, Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment, *Computer Standards & Interfaces* 31 (6) (2009).

[11] T.S. Messerges, E.A. Dabbish, R.H. Sloan, Examining smart-card security under the threat of power analysis attacks, *IEEE Transactions on Computer* 51 (5) (2002) 541–552.

[12] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: *Proceeding of the Advances in Cryptology* (CRYPTO'99), 1999, pp. 388–397.

[13] National Institute of Standards and Technology, US Department of Commerce, Secure Hash Standard, US Federal Information Processing Standard Publication 180-2, 2002.