Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Review: Privacy Preserving Authentication (PPA) Protocols for Wireless Mobile Networks

Abdurahem El Atman Igrair, Dr. Raghav Yadav
Department of Computer Science & Information Technology, Sam Higginbottom Institute of Agriculture, Technology & Sciences, Allahabad, Uttar Pradesh, India

Abstract—Now days' use of mobile handed resources such as smart phone, PDA, notebook etc. is very common and increasing day by day all devices are based on wireless communications. Roaming services is provided by mobile companies for allowing the mobile users to get connected seamlessly. However, security is major concern for such wireless networks as attackers may trying to gain access of others services. Therefore, for preventing such wireless network services fraudulent use, mechanism of user authentication is must. In addition to this, privacy requirement of user is also serious challenge especially under roaming services as the roaming protocols may leak the user's locations and identities information during the phase of user authentication. Hence it's required to have privacy preserving user authentication protocol for wireless mobile communications. Designing user authentication method with privacy preserving for global mobile networks is challenging research task for research communities as wireless mobile networks are different kinds of attacks as well as mobile user's devices is having less energy, storage and processing capabilities. In this paper, we are aiming to present the extensive review of authentication protocols with their pros and cons. We have compared the characteristics of such protocols in this paper.

Keywords—Privacy, Authentication, Wireless mobile Communications, Key Establishment, User Untraceablility.

I. INTRODUCTION

Recently advancement and technology growth in wireless communications resulted into extensive development of mobile communications usage. The tiny mobile resources those are within range of current wireless network can able to transfer information or data at any time and at any place. Therefore, this imposing the challenging problem of privacy, authentication of user and information security for wireless networks. Privacy in wireless communication ensuring that the attacker cannot intercept the mobile user's communication data. The authentication process ensuring attacker cannot able to access the any services fraudulently of any mobile users. For seamless communications, mobile communication networks providing the roaming servicing by deploying roaming protocol so that user can get access of networks. For roaming scenario, basically three different parties considered such as home server S, roaming user R, as well as visiting foreign server F. User R is subscriber of server S. If user R is entered into the foreign network which is monitored by F, then roaming services allows R user to access the services those are subscribed via F. User R and F is having direct communication link, also same between S and F. But there is no direct communication link between user R and S. In order to prevent fraudulent services use, mechanism of authentication is required.

For designing the efficient privacy preserving mobile user authentication, there are different parameters which should be satisfied by this method. We have listed below are main requirements which needs to be satisfied by privacy preserving authentication method. **A. Key establishment:** in this requirement, foreign server and user can establish the random session key which is known to them. It is derived from the combination of foreign server and user. Basically, session key is not known by home server. **B. User Anonymity:** Apart from the home server as well as its subscribed user, no one can inform the identity of user including the foreign server. **C. User Untraceablility**: Apart from the home server and user, anyone cannot able to link to any future or past method including the foreign server for similar user. **D. Authentication of Server:** foreign server identity is ensured by user. **E. Subscription Validation:** A foreign server is ensuring the home server of user identity. **F. User Revocation Scheme Provision:** by considering the related reasons, the process of user authentication should allow the foreign server in order to find whether or not roaming mobile user is revoked.

Therefore, for privacy preserving authentication methods, depending on basic interest of roaming users, it is necessary to keep users anonymous from the all eavesdroppers and the foreign server unless the identity information becomes critical which is known as user anonymity, the examples are special applications or some emergency situations. Mobile devices movement tracking may also disclose the roaming user identity. One single exposure of the identity of a user will lead to the exposure of all other sessions, both past and future, if all the roaming sessions corresponding to the user can be linked. Therefore, it is also important to make sure that no one would be able to tell if two roaming sessions are corresponding to the same mobile unit or not, this is known as user Untraceablility.

Since from last decade, there are number of methods proposed by various researchers over authentication as well as privacy for wireless communications. For wireless communications, the good security method not only providing the

high security but also having the low computation. The authors Zhu and Ma et.al proposed the novel authentication method with anonymity for mobile wireless communications. Below are basic advantages of this scheme.

- This method is based on smart cards and hash function.
- Mobile users in network can only do the symmetric cryptography functions.
- There is only single round of message exchange among the visited network and mobile user.
- There is only single round of message exchange among corresponding home network and visited network.
- There is only one-time key use among mobile user and visited network.

Apart from this advantages, this method is having some listed limitations also:

- The perfect backward secrecy cannot be achieved.
- Mutual authentication cannot be achieved
- Forgery attacks cannot to detected and protected

Similar to above method, there are different methods introduced in literature with their advantages and disadvantages. For authenticating the legitimate users, password based authentication is majorly adopted and simplest approach in network environments. In 1981, it was first remote password based authentication method introduced with password table. In this scheme, table for password verification table must be saved over the server. This paper aiming to discuss comparative study of some recent methods based on their practical results, methodology user, characteristics etc. Section II, the review of different methods for authentication and privacy preserving for mobile wireless communications is presented. Section III, presenting tabular analysis of methods reviewed in this paper with their pros and cons. Section IV is discussing the current problems of existing methods. Finally, section V presenting the conclusion and future work on literature review study of this paper.

II. LITERATURE REVIEW

This section presenting different methods for authentication and privacy preserving in mobile wireless communication. We are discussing each method with its methodology used one by one. Below figure 1 is showing the taxonomy of different techniques for privacy preserving and authentication in wireless communications.

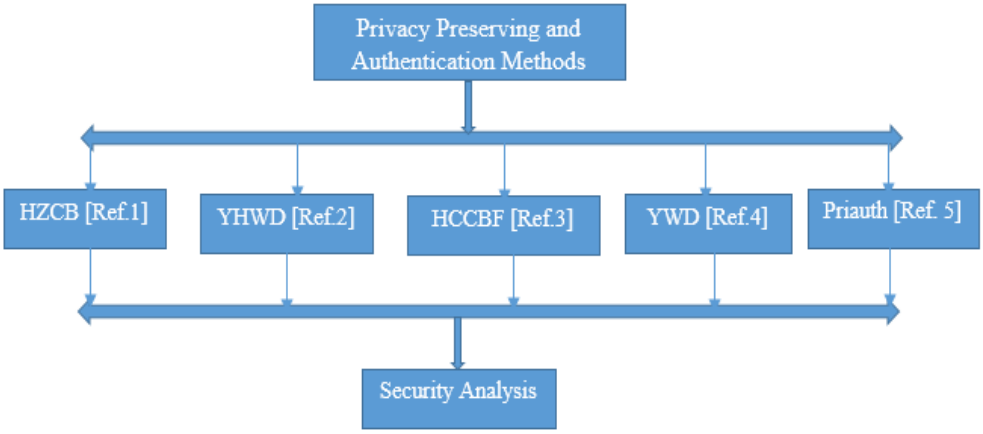

Figure 1: Privacy Preserving and Authentication Methods

2.1. HZCB

In [1], authors prosed the secure and light-weight authentication technique with the user anonymity to overcome the problems of previous methods. At first, author discussed the security weaknesses of previous methods, then proposed new technique to overcome them. From this paper, we studied that this method is simple to implement for mobile user since it only performs a symmetric encryption/decryption operation. Having this feature, it is more suitable for the low-power and resource-limited mobile devices. In addition, it requires four message exchanges between mobile user, foreign agent and home agent. Thus, this protocol enjoys both computation and communication efficiency as compared to the well-known authentication schemes. In special conditions author consider the authentication protocol when a user is located in his/her home network. Also, the session key will be used only once between the mobile user and the visited network. In addition to this, the security analysis demonstrates of this scheme enjoys important security attributes such as preventing the various kinds of attacks, single registration, user anonymity, no password/verifier table, and high efficiency in password authentication, etc. Moreover, one of the new features in our proposal is: it is secure in the case that the information stored in the smart card is disclosed but the user password of the smartcard owner is unknown to the attacker.

Methodology: The method HZCB is composed of five different phases such as the login phase, the registration phase, the session key update phase, the authentication phase, and the password change phase. 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. In the registration phase, the home agent issues a smart card for a mobile user through a secure channel. After a successful validation, an authentication key is established between the foreign agent and the mobile user. The password change phase is invoked whenever a mobile user requests to change his/her password. If 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. This is the working principle of this protocol.

2.2. YHWD

In [2], authors proposed the two new anonymous roaming protocols for wireless communication in which only the roaming user as well as the foreign network are involved in running protocol. Both of the protocols are global and universal such way that both can directly be used as AKE protocols for the home network. In this secure two party roaming protocol, authors adopted the existing efficient method called Identity Based Signature (IBS) which is existentially unforgeable against the message attacks and adaptive selected ID attacks. Author used IBS method introduced by authors Zhu, Yang and Wong in reference number [6] as it is efficient as well as simple enough for resource constrained mobile devices. This technique needs the ECSM (Elliptic Curve Scalar Multiplication) functionality for generating the signature and one Multi-ECSM operation for verifying a signature, and the ECSM operation in the signing algorithm can further be pre-computed. In addition to this, author also introduced the revocation technique as well as billing method. Practical results showing the better performance for security against existing methods.

2.3. HCCBF

In [3], author proposed secure and lightweight user authentication protocol with anonymity for roaming service in the global mobility network (GLOMONET). Author claimed that their approach is having more advantages as compared to related methods. Firstly, it uses low-cost functions such as one-way hash functions and exclusive-OR operations to achieve security goals. Having this feature, it is more suitable for battery-powered mobile devices. Secondly, it uses nonce instead of timestamps to avoid the clock synchronization problem. Therefore, an additional clock synchronization mechanism is not needed. Thirdly, it only requires four message exchanges between the user, foreign agent and home agent. Further, the security properties of this method are formally validated by a model checking tool called AVISPA. Author also demonstrate that this protocol enjoys important security attributes including prevention of various attacks, single registration, user anonymity, no password table, and high efficiency in password authentication. Security and performance analyses show that compared with other related authentication schemes, the proposed scheme is more secure and efficient.

Methodology: The design of this method consisting of three different entities such as home agent, mobile user as well as foreign agent. This protocol functionality is basically divided into three different phases such as Registration phase, Authentication phase and Login phase. In the registration phase, the home agent issues a personalized 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 home agent. Author verified the security properties of this protocol. Also evaluated the performance of this approach in terms of computation cost and communication cost.

2.4. YWD

In [4], author proposed the method of construction of anonymous as well as authenticated key exchange protocols for a *roaming* user and a visiting server in order to establish a random session key in such a way that the visiting server authenticates the user's home server without knowing exactly who the user is. A network eaves dropper cannot find out the user's identity either which is known as *user anonymity*. In addition, visited servers cannot track the roaming user's movements and whereabouts even they collude with each other this is known as *user Untraceablility*. This construction approach is generic and built upon provably secure two-party key establishment protocols. The advantage of this generic protocol construction include eliminating alias synchronization between the user and the home server, supporting joint key control, and not relying on any special security assumptions on the communication channel between the visiting server and the user's home server. This protocol can also be implemented efficiently. By piggybacking some message flows, the number of message flows between the roaming user and the visiting server is only three.

Methodology: Author aimed to present the novel authenticated key exchange protocol called AAKE-R. There are three parties involved for designing this protocol such as home server foreign server and user. Home server may be offline or online. If the home server is online, we mean that the home server is involved in a protocol run and hence the protocol is a three-party one. Otherwise, it is a two-party protocol between the user and the foreign server. Below listed properties are achieved by this mechanism:

- Server authentication: The mobile user is sure about the identity of the foreign server.
- Subscription Validation: The foreign server is sure about the identity of the home server of the user.
- 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 obtain the session key.
- User Anonymity: Besides the user and the home server, no one including the foreign server can tell the identity of the user.
- User Untraceablility: Besides the user and the home server, no one including the foreign server is able to identify any previous protocol runs which have the same user involved.

2.5. Priauth

In [5], author proposed novel method for privacy-preserving universal authentication protocol which is named as Priauth. This protocol delivers the strong user anonymity against both foreign servers and eavesdroppers. Also providing the efficient session key establishment and achieves efficiency. In addition to this, this approach providing the efficient method to handle the user revocation problem at the same time strong user Untraceablility supporting. This method

considering the four different types of threats to the user authentication such as DoS attack, false mobile user attack, message env route attack and deposit case attack. There are two main contributions such as first is related to showing the weaknesses of present authentication methods in mobile wireless communications. The second is contribution is that they proposed the privacy-preserving universal authentication protocol called *Priauth*.

Methodology:

- By introducing Verifier-Local Revocation Group Signature with Backward Unsinkability (VLR-GS-BU), this approach solving the six requirements such as server authentication, subscription validation, provision user revocation, user anonymity, key establishment, and user Untraceablility.
- In addition to this, 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.
- Also Priauth belongs to the class of *Universal Authentication Protocols* in which same protocol and signalling 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.

III. COMPARATIVE ANALYSIS

In this section, we will present the study over comparative analysis for above methods in different aspect. Below table 1 is showing the details about methods reviewed in above section with their features.

Table 1: Comparative Analysis of Features of Related Methods

Year	Title	Authors	Journal	Features
2010	A strong user authentication scheme with smart cards for wireless communications	Daojing He, Maode Ma, Yan Zhang, Chun Chen, Jiajun Bu	2010 Published by Elsevier B.V. All rights reserved.	Smart card based secure and light-weight user authentication scheme has been proposed.
2010	Universal Authentication Protocols forAnonymous Wireless Communications	Guomin Yang, Qiong Huang, Duncan S. Wong, and Xiaotie Deng	IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 9, NO. 1, JANUARY 2010	Two novel anonymous roaming protocols proposed for authentication process. Proposed a revocation mechanism and a billing scheme.
2011	Design and Validation of an Efficient Authentication Scheme with Anonymity for Roaming Service in Global Mobility Networks	Daojing He, Sammy Chan, Chun Chen, Jiajun Bu, Rong Fan	Wireless Pers Commun (2011) 61:465–476 DOI 10.1007/s11277-010-0033-5	Secure and lightweight user authentication protocol with anonymity for roaming service in the global wireless communication networks.
2007	Anonymous and Authenticated Key Exchange forRoaming Networks	Guomin Yang, Duncan S. Wong, and Xiaotie Deng	IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 6, NO. 9, SEPTEMBER 2007	The novel construction approach of anonymous and authenticated key exchange protocols for a *roaming* user and a visiting server to establish a random session key is introduced in this paper.

Table 2: Performance Parameters Comparative Study for Literature Methods

Performance Characteristics	**HZCB**	**YHWD**	**HCCBF**	**YWD**	**Priauth**
Communication Overhead	Medium	Low	Medium	High	Low
Global	No	Yes	No	No	Yes
Single Registration	Yes	No	Yes	Yes	Yes
DoS Resistance	No	No	No	No	Yes
User Untraceablility	Yes	No	Yes	Yes	Yes
Key Establishment	No	Yes	No	Yes	Yes
User Revocation Provision	No	No	No	No	Yes

Above tabular analysis showing the comparative study for most important features and performance parameters of privacy preserving authentication protocol for wireless communications. This study helps to select appropriate protocol

for wireless communications based on its advantages and limitations. The method Priauth achieving the better performance as compared to other methods. This method satisfying all the requirements of efficient protocol.

IV. CURRENT LIMITATIONS

The methods we studied in this paper are proposed for user authentication processing and privacy preserving in mobile communication networks. There are some more areas in mobile communication networks in which still security is concern such as mobile cloud computing in which most of mobile users want to access the cloud data with high security. The cloud mobile computing is not addressed above discussed methods. Also, there are some more recent attacks to which above methods are not evaluated such as replay attack, stolen verifier attack, modification attack, server spoofing attack.

V. CONCLUSION AND FUTURE WORK

There are different wireless and mobile networks for communication deployed since from last five years with rapid development and enhancement in wireless technology. Networks like mobile telecommunication networks for example 2G, 3G and recently 4G, wireless local area networks based on 802.11, WiMAX networks, roadside to vehicle communication networks etc. With rapid growth of this networks, security challenges also increase such as privacy preserving, legitimate user authentication especially in roaming networks. In this paper we presented the survey over different privacy preserving and user authentication methods with goal of present the comparative study of methodologies used, features and performance metrics for this methods. For future work, we will suggest to work on designing improved method for mobile cloud communication systems.

REFERENCES

[1] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A strong user authentication scheme with smart cards for wireless communications," *ComputerCommun.*, 2010, 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.WirelessCommun.*, vol. 9, no. 1, pp. 168-174, 2010.

[3] 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/s11277-010-0033-5

[4] 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.

[5] Daojing He, Jiajun Bu, Sammy Chan, Chun Chen, and Mingjian Yin, "Privacy-Preserving Universal Authentication Protocol for Wireless Communications", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 10, NO. 2, FEBRUARY 2011.

[6] R. W. Zhu, G. Yang, and D. S. Wong, "An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices, "theory. Compute. Sci., vol. 378, no. 2, pp. 198-207, 2007.

[7] C. C. Lee, M. S. Hwang, and I. E. Liao, "Security enhancement on anew 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] Daojing He, Chun Chen, Sammy Chan and Jiajun Bu, "Strong roaming authentication technique for wireless and mobile networks", INTERNATIONAL JOURNAL OF COMMUNICATION Systemising. J. Commun. Syst. (2012), Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/dac.1387.

[10] Yoon, E. J., and Jeon, I. S., "An Efficient and SecureDiffie–Hellman Key Agreement Protocol Based on Chebyshev Chaotic Map," Communications in Nonlinear Science and Numerical Simulation, vol. 16, no. 6, pp.2383-2389, 2011.

[11] Zhang, L., "Cryptanalysis of the Public Key Encryption Based on Multiple Chaotic Systems," Chaos, Solitons Fractals, vol. 37, no. 3, pp. 669-674, 2008.

ABOUT AUTHOR

Abdurahem el atman igrair He is presently doing Ph.D. in computer science and information technology at SHIATS institute, Allahabad, India, he has received his M. Tech degree in computer network and information security from (JNTU) Hyderabad, India in year of 2012, and (BSc) in year of 2004 from computer science department Sebha University, Libya.

Dr. Raghav Yadav He is presently an assistant professor at Sam Higginbottom Institute of Agriculture, Technology and Sciences (SHIATS), Allahabad, India, he is received the Ph.D. degree from the Motilal Nehru National Institute of Technology (MNNIT), Allahabad, India. He received his M.Tech. Degree in computer science and engineering from MNNIT, Allahabad. And B.E. degree in electronics engineering from Nagpur University Dr. Yadav has authored more than 20 research papers in national/international conferences and refereed journals. His research interests are in the field of optical network survivability, ad-hoc networks, and fault tolerance systems.

