IMPACT FACTOR- 4.520 ISSN NO- 2456-7078

Volume-1, Issue-VI, Sept- 2017

Research maGma

An International Multidisciplinary Journal

CONFERENCE

of

Thiruvalluvar University
College of Arts & Science, Arakkonam.

on

"EMERGING TRENDS IN ENGLISH LANGUAGE & LITERATURE”

Research maGma

An International Multidisciplinary Journal

ISSN NO- 2456-7078 IMPACT FACTOR- 4.520 VOLUME-1, ISSUE-7, SEPT-2017

RSA (PUBLIC KEY CRYPTOGRAPHY) ALGORITHM IN WIRELESS SENSOR NETWORKS

[1]D. Thamaraiselvi and [2]Dr. M. Ramakrishnan

[1]CSE Department , SCSVMV University, Kanchipuram

[2]IT Department , Madurai kamarajar University, Madurai

ABSTRACT

User authentication is a crucial service in wireless sensor networks (WSNs) that is becoming *increasingly common in WSNs because wireless sensor nodes are typically deployed in an* unattended environment, leaving them open to possible hostile network attack. The main research goal of the paper is to securely authenticate remote user in a convenient and user friendly manner. In this paper, we propose a RSA (asymmetric Rivest, Shamir, Adleman cryptographic algorithm for encryption based remote user authentication using smart cards in hierarchical wireless sensor networks. Usually, the proposed scheme includes three phases for user authentication such as registration phase, login phase and authentication phase. First an asymmetric Rivest, Shamir, Adleman(RSA) cryptographic algorithm that resolves security weaknesses. The RSA method is suitable for applications with higher security requirements. Finally, we present a comparison of security and computation time for the proposed method. Our proposed scheme achieves better security against attacks and less computational time as compared to those for other existing cryptographic approaches.

KEY WORDS:

Hierarchical wireless sensor networks, Network security, Cryptography, Smart cards, Authentication.

1. INTRODUCTION

Remote user authentication is a method to authenticate remote users to a server over insecure networks [1]. In today's electronic era, smart card based remote user authentication schemes are widely acknowledged as one of the most secure and reliable forms of electronic identification [2]. Wireless sensor networks (WSNs) are applied widely a variety of areas such as military, environmental monitoring, real- time traffic monitoring, measurement of seismic activity, wildlife monitoring, medical, building condition monitoring and so on. Remote User authentication in WSNs is a critical security issue due to their unattended and hostile deployment in the field to deal with secret data over insecure networks. With the help of remote user authentication schemes, people can interact with the server through distributed or portable terminals. In a remote user authentication scheme, the authenticity and integrity of the user and the server are important elements over an insecure network [3]. At their best, the remote user and remote server can securely authenticate each other, processing and protecting the communication in a convenient and user friendly manner.

Smart cards play an important role in our everyday life. We utilize them as credit cards, electronic purses, health cards, and secure tokens for authentication of individual identity. But, since smart cards have low computing capability, lots of authentication schemes using smart cards have been designed without public key cryptosystem technology for computation efficiency [4, 5 and 6]. Under the circumstances, if a smart card is lost or stolen, those schemes are usually weak from the offline password guessing attack, because human-memorable passwords are not long enough to resist the attack. Each user has their unique biometric characteristics, such as voice, fingerprints, iris recognition and so on. These biometric characteristics have irreplaceable advantages: reliability, availability, non-repudiation and less cost. Therefore, biometric authentication has widely used.

There are no proper ad hoc infrastructures in wireless sensor networks where a large number of sensor nodes are deployed by truck or plane on a target field. After deployment of sensor nodes, they communicate to other neighboring nodes within their communication range to form clusters. After that, one cluster head or gateway node is selected by base station or sensor nodes for each cluster on the basis of energy, signal strength, degree, capability, mobility etc. All the sensor nodes sense raw data from environment and send to their nearest cluster head by single-hop or multi-hop communication [7]. Cluster heads gather the raw data and send to nearest base station or sink node by multi-hop or single-hop communication [7]. Finally, data are collected from base station. The collected data is not always real time data because all cluster heads send data to base station after a certain periodic time. If we collect data directly from cluster heads, we can get real time data. This is possible if it is allowed to access those real time data directly from cluster head, when demanded. Hence, it is needed to first authorize the accessors and then allows to access to do secure communication among accessors and cluster heads [8].

In recent years, the main goal is to design authentication scheme in such a manner that the designed protocol is better tread-off among security and communication cost than the previously published scheme. These types of schemes are applicable to the areas such as computer networks, wireless networks, remote login systems, operation systems and database management systems. The goal of a remote user authentication scheme is to identify a valid card holder as having the rights and privileges indicated by the issuer of the card. There exist many user authentication protocols in literature for wireless sensor network [9-18]. We have pointed out that their scheme is insecure against some attacks such as insider attack and session key recovery attack. Further, it is noted that base station uses user's secret parameter in the user's registration phase which is impossible. Additionally, their scheme suffers from dynamic cluster head addition overhead problem, limited number of cluster head access problem and clock synchronization problem.

The cluster heads in hierarchical wireless sensor networks gather real time data from the other ordinary sensor nodes and send those data to a nearest base station [19]. But, the main important issue is that how a user will get the real time data directly from a cluster head securely. To solve this problem, many user authentication schemes have been proposed in literature. The various cryptographic algorithms are available for network security [20]. The symmetric cryptographic algorithms are high speed compared than asymmetric cryptographic algorithms or public key cryptographic systems like RSA, Elliptic Curve Cryptography. The public key cryptographic algorithms are more secure than symmetric algorithms. Because, it has two keys one for encryption and another one for decryption. The encryption algorithms are more secured depends on the key value and its size. But, the key distribution is major problem. In this hybrid encryption technique we propose symmetric encryption for encryption/decryption and using public key cryptosystems for authentication [21]. The hybrid encryption technique is a combination of both symmetric and asymmetric cryptographic techniques.

The rest of this paper is organized as follows. Section 2 of this paper describes literature review. Then our proposed RSA method is introduced and discussed in section 3. Then the security analysis with various attacks are discussed in Section 4. Section 5, provides performance evaluation of the proposed scheme through analysis and comparative study of simulation results. Finally, Section 6 concludes the paper.

2. RELATED WORK

Some of the recent work related to the remote user authentication is listed below:

Xue-lei Li *et al*. [22] proposed password as an easy-to-remember credential plays an important role in remote user authentication schemes, while drawing from a space so small that an adversary may exhaustively search all possible candidate passwords to guess the correct one. In order to enhance the security of the password authentication scheme, smart card was introduced as the second factor to construct two-factor authentication scheme. However, we find out that two latest smart-card-based password authentication schemes were vulnerable to offline password guessing attacks under the definition of secure two-factor authentication. Furthermore, in order to show the serious consequence of offline password guessing attacks, we illustrate that the password compromise impersonation attacks as further threats were effective to break down the authentication schemes. Finally, we conclude the reasons why these weaknesses exist and present our improved ideas to avoid these problems in the future.

With the growing popularity of network applications, multi-server architectures were becoming an essential part of heterogeneous networks and numerous security mechanisms had been widely studied in recent years. To protect sensitive information and restrict the access of precious services for legal privileged users only, smart card and biometrics based password authentication schemes have been widely utilized for various transaction-oriented environments. In 2014, Chuang and Chen proposed an anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards, password, and biometrics. They claimed that their three-factor scheme achieves better efficiency and security as compared to those for other existing biometrics-based and multi-server schemes. Unfortunately, Chun-Ta Li *et al*. [23] found that the user anonymity of Chuang-Chen's authentication scheme cannot be protected from an eavesdropping attack during authentication phase. Moreover, their scheme was vulnerable to smart card lost problems, many logged-in users' attacks and denial-of-service attacks and was not easily reparable.

The advancement of communication technology resulted in increasing number of security threats over public Internet on remote servers. In 2014, Shipra *et al*. proposed an improved remote user authentication scheme using smart cards with check digits. Shipra et al. claimed that their scheme was secure and efficient against all major cryptographic attacks. Unfortunately, their scheme was vulnerable to some of the cryptographic attacks, particularly “online password guess attack” as discussed in this manuscript. As a part of our contribution, Mrudula Sarvabhatla *et al*. [24] proposed a robust and extra secure authentication scheme for remote users based on smart cards with check digits, with slight increase in the cost. Security was the fundamental compared to complexity, since complexity could be easily manage with improved technology.

Recently, Xue *et al*. proposed a lightweight dynamic pseudonym identity based authentication and key agreement protocol for multi-server architecture (2014). They claimed that their scheme overcomes security flaws of related schemes. In this paper, were analyze the security of Xue *et al*. ’ s scheme and show that their scheme cannot resist password guessing attacks. In addition, their scheme cannot achieve user anonymity and intractability. To conquer these defects, Hao Lin et al. [25] proposed an improved and lightweight pseudonym identity-based authentication scheme for multi-server environment. Compared with Xue *et al*.’s scheme, our protocol not only maintains the merits, but also overcomes the security flaws.

In a recent paper (BioMed Research International, 2013 /491289), Khan *et al*. proposed an improved biometrics-based remote user authentication scheme with user anonymity. The scheme was believed to be secure against password guessing attack, user impersonation attack, server masquerading attack, and provide user anonymity, even if the secret information stored in the smart card was compromised. Fengtong Wen *et al*. [26] analyze the security of Khan *et al*.’s scheme, and demonstrate that their scheme doesn’t provide user anonymity. This also renders that their scheme was insecure against other attacks, such as off-line password guessing attack, user impersonation attacks. Subsequently, they propose a robust biometric-based remote user authentication scheme. Besides, they simulate their scheme for the formal security verification using the wide-accepted BAN logic to ensure our scheme was working correctly by achieving the mutual authentication goals.

3. PROPOSED RSA METHOD

We identify the objectives of our research work is to design a remote user authentication scheme in a hierarchical wireless sensor network which can address all the problems of the former schemes, make the scheme secure against all possible attacks and compare the scheme in terms computational time with other related schemes. In this proposed design methodology, a smart-card based user authentication scheme in hierarchical wireless sensor network using RSA method is proposed. In the proposed Scheme, the process flow consists of three phases: Registration phase, login phase, Verification phase. In security analysis, we consider various attacks like privileged insider attack, guessing attack, stolen verifier attack, man-in-the-middle attack, DoS attack, many logged-in users with same login-id attack, and smart card breach attack.

a) RSA cryptography

The concatenated user name and password of the user is encrypted and decrypted using the RSA cryptographic algorithm to secure the communication from an unauthorized access. RSA (Rivest, Shamir, Adleman) operates on the decimal value of the message and its robustness is based on the impossibility to factorize very large numbers (of at least 300 digits). The RSA algorithm is based on the assumption that integer factorization is a difficult problem. This means that given a large value n, it is difficult to find the prime factors that make up n. It is a most popular asymmetric key algorithm.

1) Key Generation

The following procedure is carried out for the key generation:

(i) Choose two very large random prime integers and .

(ii) Compute n and : $\phi(n)$; $n = pq$; $\phi(n) = (p-1)(q-1)$

(iii) Choose an integer , $1 < e < \phi(n)$ such that: $\gcd(e, \phi(n)) = 1$(where means greatest common denominator).

(iv) Compute , $1 < d < \varphi(n)$ such that: . $e * d \equiv 1(\bmod \phi(n))$

The encryption public key is $K_E = (n, e)$ and the decryption private key is $K_D = (n, d)$. The values of , *p* , *q* and $\varphi(n)$ are private; *e* is the public or encryption exponent; *d* is the private or decryption exponent. In our experiment, the information we have to encrypt is the masked password

2) Encryption

The masked password MP_i of the registrant user is encrypted as,

$$E_i(MP_i) = MP_i^e (\bmod n) \quad (1)$$

In the login phase, the masked password SMP_i of the smart card user is encrypted as,

$$E_i(SMP_i) = SMP_i^e (\bmod n) \quad (2)$$

The encrypted masked password of the registrant user and the login smart card user is stored in the base station Y_i.

3) Decryption:

The encrypted information is decrypted and store in the base station. The decrypted masked password of the registrant user is given as,

$$D_i(MP_i) = E_i^d (\bmod n) \quad (3)$$

The decrypted login smart card user masked password is taken as,

$$D_i(SMP_i) = E_i^d (\bmod n)$$

The encrypted and the decrypted information of the registrant user and the login user is stored in the base station for user authentication.

b) Authentication Scheme

1.Registration phase

Initially, a new registrant user register his/her identity at the remote server in the Registration phase. Registrant X_i send his/her user name IX_i , password P_i and personal biometrics BK_i on the smart card reader. Before sending this details the user concatenate the user name and password.

$$MP_i = (P_i \| IX_i)$$

Smart card reader SM_i receives the registrant message <MP_i, BK_i> from the registrant user . Smart card reader send the details of the user to the corresponding cluster head CH and then CH forward to the base station Y_i. If the above request is accepted, the base station receives the masked password MP_i. Then the masked password will get encrypted as specified in eqn. 1 and the encrypted message is decrypted using eqn. 3. The encryption and decryption D_i details are stored in the base station. At the same time, base station will extract the minutiae from the biometric BK_i and calculate the standard deviation *SD* using eqn. 6.The evaluated details are stored in the Y_i . After registering, the base station send a smart card to the registered user.

2.Login phase

After registration, access the real-time data from the WSNs by the user SX_i in the login phase. First user SX_i insert the smart card into the smart card reader then inputs his/her identity SIX_i and password Sp_i into the reader terminal. The login user also concatenate the user name and password before sending to the base station.

$$SMP_i = (SP_i \| SIX_i)$$

If the login message <SMP_i> is received by the base station Y_i ,as mentioned in the registration phase, the base station will encrypt the masked password as in eqn. 2 and then decrypt the masked password as in eqn. 4. After decryption Base station verify the user with the registered user. Check SMP_i is equal to the stored MP_i . If not, then report wrong password P_i to the user. This process performs up to some predefined number of times so that it can withstand password guessing attack by using stolen or lost smart card. If the user name and password of the user is same, then it will ask the biometric SBK_i of the entered user SX_i. If the user enters the biometrics SBK_i, the Base station Y_i extracts the minutiae of the biometrics and calculate the SD using eqn. 2.In order to verify the biometric of the user, the standard deviation of the user SX_i and the corresponding SD of the registered user X_i is given as input to the matching ABC optimization algorithm.

VERIFICATION PHASE

After receiving the authentication request message, execute a mutual authentication process between the user and the remote system in the Verification phase. When Y_i receives login message <SIX_i, SP_i> from the user SX_i , Y_i first checks whether received SMP_i is equal to the stored MP_i. If not, then report wrong password P_i to the user. If the user name and password of the user is same, then it will ask the biometric SBK_i of the entered user SX_i. If the user enters the biometrics SBK_i , base station verify the biometric of the user SBK_i matches with the registered biometric BK_i using the ABC optimization algorithm. If the maximum fitness value obtained from the algorithm is less than or equal to the threshold means the user is authorized to access the real time information. Otherwise, the user is declared as the unauthorized and he/she not have the permission to access the real time information.

6 CONCLUSION

In this paper, a proposed secure RSA for remote user authentication in WSNs. The proposed method is compared in terms of computational time and various attacks. Since WSNs needs more efficient methods to perform mutual authentication in an insecure network environment, we use an RSA-based mechanism to accomplish this. The proposed method can prevent all the problems of the former schemes and provide mutual authentication to protect inside security and outside security. Furthermore, it not only inherits the merits of RSA-based mechanism but also enhances the WSN authentication with higher security than other methods. Therefore, the proposed method is more suited to WSNs environments in terms of user authentication.

REFERENCE

1. Awasthi A. K. and Lal S, "A remote user authentication scheme using smarts cards with forward secrecy," IEEE Trans. Consumer Electronic, vol. 49, no. 4, pp. 1246-1248, 2003.

2. Chan C. K. and Cheng L. M, "Cryptanalysis of a remote user authentication scheme using smart

cards," IEEE Trans. Consumer Electronic, 46, pp. 992-993, 2000.
3. Leung K. C., Cheng L. M., Fong A. S. and Chen C. K, "Cryptanalysis of a remote user authentication scheme using smart cards," IEEE Trans. Consumer Electronic, 49-3, pp.1243-1245, 2003.
4. Lee S. W., Kim H. S. and Yoo K. Y, "Comment on a remote user authentication scheme using smart cards with forward secrecy," IEEE Trans. Consumer Electronic, 50, 2: pp. 576-577, 2004.
5. Liaw H.T., Lin J.F. and Wu W.C., "An efficient and complete remote user authentication scheme using smart cards," Mathematical and Computer Modelling, 44, pp. 223-228, 2006.
6. Shen Z. H, "A new modified remote user authentication scheme using smart cards," Applied Mathematics, Volume 23-3, 371-376, 2008.
7. M. T. Thai, F. Wang, D. Liu, S. Zhu, and D. Z. Du, "Connected dominating sets in wireless networks with different transmission ranges," IEEE Transactions on Mobile Computing, vol. 6, no. 7, pp. 721– 730, 2007.
8. F. Dressler, "Authenticated reliable and semi-reliable communication in wireless sensor networks," International Journal of Network Security, vol. 7, no. 1, pp. 61–68, 2008.
9. R. Fan, L. di Ping, J. Q. Fu, and X. Z. Pan, "A secure and efficient user authentication protocol for two tiered wireless sensor networks," in Second Pacific Asia Conference on Circuits, Communications and System (PACCS'10), vol. 1, pp. 425–428, 2010.
10. D. He, Yi Gao, S. Chan, C. Chen, and J. Bu, "An enhanced two-factor user authentication scheme in wireless sensor networks," Ad Hoc & Sensor Wireless Networks, vol. 10, no. 4, pp. 361–371, 2010.
11. M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks," Sensors, vol. 10, no. 3, pp. 2450–2459, 2010.
12. P. Kumar and H. J. Lee, "Cryptanalysis on two user authentication protocols using smart card for wireless sensor networks," in Wireless Advanced (WiAd'11), pp. 241–245, 2011.
13. H. Ru Tseng, R. H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in IEEE Global Telecommunications Conference (GLOBECOM'07), pp. 986–990, 2007.
14. B. Vaidya, D. Makrakis, and H. T. Mouftah, "Improved two-factor user authentication in wireless sensor networks," in IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'10), pp. 600–606, 2010.
15. B. Vaidya, J. Silva, and J. J. P. C. Rodrigues, "Robust dynamic user authentication scheme for wireless sensor networks," in Proceedings of the 5th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet'09), pp. 88–91, 2009.