IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Issue-10 E-ISSN: 2347-2693

An ABC Optimized Biometric based User Authentication in WSN

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

[1*]Department of computer science and Engineering, SCSVMV University ,Kanchipuram, Tamil Nadu,India.
[2]Department of Information Technology,MADURAI KAMARAJAR University,Madurai,Tamil Nadu,India.

e-mail: thamaraiselvi17@gmail.com, ramakrishod@gmail.com

Available online at: www.ijcseonline.org

Received: Oct/23/2016 Revised: Oct/30/2016 Accepted: Nov/17/2016 Published: Nov/30/2016

Abstract— **User authentication is a crucial service in wireless sensor networks (WSNs) because wireless sensor nodes are typically deployed in an unattended environment, leaving them open to possible hostile network attack. The main goal of research is to Authenticate remote user in a convenient and Secured manner. In this paper, we propose a ABC(Artificial Bee Colony optimization algorithm for matching)algorithm for user authentication in hierarchical wireless sensor networks using Biometric (finger print)data. In the proposed scheme ABC algorithm calculates the standard deviation(threshold value) from the biometric data (finger print) which is used for user authentication with maximum fitness in an optimized and secured manner.**

Keywords-Hieriarchical wireless sensor network,Artificial Bee Colony ,User Authentication

I. INTRODUCTION

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 . 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

[*]Corresponding Author:
D.Thamaraiselvi
e-mail: thamaraiselvi17@gmail.com

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.

II. 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.

II. ABC OPTIMIZATION

The procedural flow of the biometric finger print matching is given in fig. 1. The procedure in which first we have to extract the biometric feature of the registrant and the smart card user. This extracted features are given to the ABC algorithm for calculating the maximum of fitness value and then check with the threshold for authorized and unauthorized biometric.

Biometric Minutiae Extraction

Fingerprints are the most used biometrics technique for personal identification. While the purpose of fingerprint verification is to verify the identity of a person. Many fingerprint identification methods have appeared in literature over the years. The most popular matching approach for fingerprint identification is usually based on lower-level features determined by singularities in finger ridge patterns called minutiae. In general, the two most prominent used features are ridge ending and ridge bifurcation. More complex fingerprint features can be expressed as a combination of these two basic features. Ridge-end, which means the end of the ridges and Bifurcation points, which means one single ridge divided into two ridges.

In this paper, each detected minutiae for the finger print biometric BK_i is described as,

$$m_i = (x_i, y_i, t_i) \longrightarrow (1)$$

x_i and y_i are the coordinates of the minutiae point and t_i is the type of minutiae point (ridge ending or ridge bifurcation). The step by procedure to extract the minutiae are as follows:

Step 1: Binarization

This process consist in converting the gray scale image in binary image, i.e, the intensity of the image has only two value: black, representing the ridges and white representing the valleys and the background. A simple method to binarize is to use a global threshold value, however, it is not well suited for noisy images, a more robust method consist of using some rectangular mask, rotate according the orientation of the ridges.

Step 2: Thinning

The objective of thinning is to find the ridges of one pixel width. The process consist in performing successive erosions until a set of connected lines of unit-width is reached. This lines are also called skeletons. An important property of thinning is the preservation of the connectivity and topology which however can lead to generation of small bifurcation artifacts and consequently to detection of false minutiae. Therefore some procedure aiming the elimination of these artifacts must be performed after the thinning

Step 3: Minutiae detection

From the binary thinned image, the minutiae are detected by using nxn pattern masks. Samples of masks used for identifying the ridge ending and bifurcations point. After a successful extraction of minutiae, they are stored in a template, which may contain the minutia position (x,y), and minutia type (bifurcation or termination). After detecting the points, the standard deviation SD of the minutiae points can be calculated as,

$$SD = \sqrt{\frac{1}{N\sum_{i=1}^{N}(m_i - \mu)}} \longrightarrow (2)$$

In which, the mean value $\mu = \frac{\sum_{i=1}^{N} m_i}{N}$ for $i = 1, 2, \cdots, N$ and m_i is the extracted minutiae points.

In the same way the minutiae are detected for the query image and these also stored as template. During the enrolment, the stored standard deviation values will be used in the matching process as reference template or database template. During the verification or identification, the extracted minutia are also stored in a template and are used as query template during the matching.

ABC optimization algorithm

The Artificial Bee Colony Algorithm is a swarm based optimization algorithm proposed for the first time by Karaboga in 2005. There are three kinds of honey bees in ABC algorithm to forage food source. They are employed bees, onlookers and scouts bees. The tasks of these bees are to collect nectar around the hive. A bee waiting on the dance

area for making decision to choose a food source is called an onlooker and a bee going to the food source previously visited by it is named as an employed bee. A bee carrying out random search is called a scout bee. In ABC, food searching and nectar foraging around the hive are performed by employed, onlooker and scouts bees collectively. In the ABC algorithm, the first half of the colony
consists of employed artificial bees and the second half constitutes the onlookers. For every food source, there is only one employed bee. In other words, the number of employed bees is equal the number of food sources around the hive. The employed bee whose food source is exhausted by the employed and onlooker bees becomes a scout.

$$obj(i) = \min[\gamma \times M] \longrightarrow (3)$$

$$M = \{(x_{\max}(i))^2 + (x_{\min}(i))^2\} \longrightarrow (4)$$

In the above equation (4), $x_{\max}(i)$ is the maximum of the SD and $x_{\min}(i)$ is the minimum of the SD. γ is a random variable in the range [0-1].

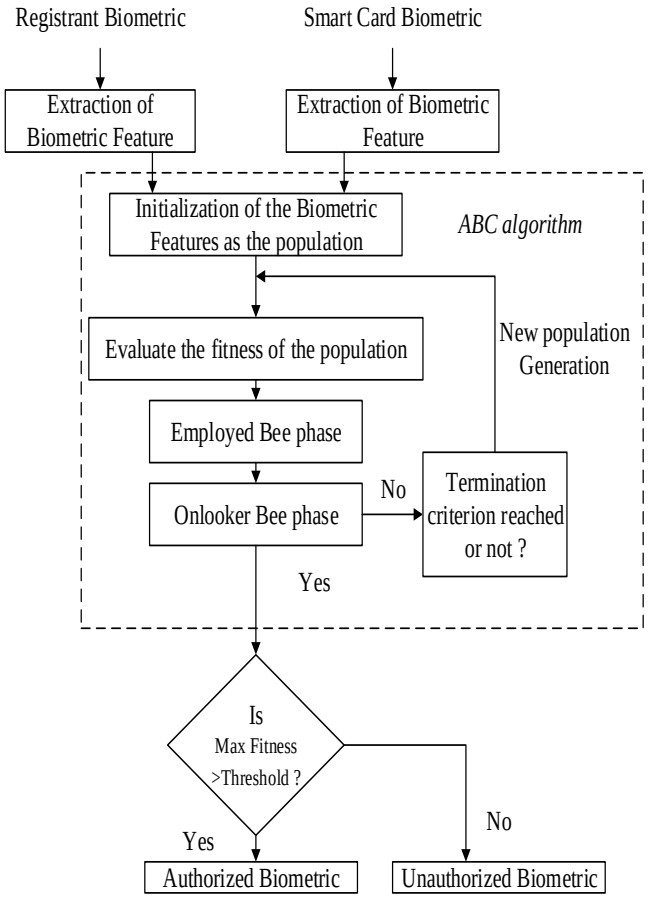


Fig (1):Abc Optimization For Matching

Pseudo code of ABC algorithm:

Step 1: Generate the initial population x_i where $i = 1, 2, 3, \cdots, N$
Step 2: Evaluate the fitness value of the population
Step 3: Gen=1
Step 4: $Gen \le G_{\max}$ (Repeat)
Step 5: For each employed bee produce new solution (food source position)
$v_{ij} = x_{ij} + \psi_{ij}(x_{ij} - x_{kj})$, Calculate the value f_i
Apply greedy selection process between x_i and v_i
Step 6: Calculate the probability value p_i for the solution x_i using their fitness values
Normalize p_i values in to [0, 1]
Step 7: For each onlooker bee select a solution x_i depending on p_i
Generate new solution v_i
Calculate the value f_i
Apply greedy selection process for the onlookers between x_i and v_i
Step 8: If there is an abandoned solution then replace by with a new randomly produced solution x_i for the scout.
Memorize the best food source position
Step 9: Gen=Gen+1
Until cycle= Maximum cycle number
Step 10: End

In the algorithm ABC, for generating an initial solution for i[th] employed bee is generated using the equation (1).

$$x_i^j = x_{\min}^j + rand[0,1] * (x_{\max}^j - x_{\min}^j)$$

Where $i = 1, 2, \cdots, N$ and $j = 1, 2, \cdots, D$. x_i^j is a parameter to be optimized for the i[th] employed bee on the dimension j of the D-dimensional space. N denotes the number of employed bee. $x_{\max}^j$ is the upper bound for x_i^j . $x_{\min}^j$ is the lower bound for x_i^j .

The food position (weight) of both onlooker bee and employed bee in the j[th] dimension is given in the equation (10).

$$v_i^j = x_i^j + \varphi_i^j (x_i^j - x_k^j)$$

Where, $j = 1, 2, \cdots, D$ and $k = 1, 2, \cdots, N$. x_i^j is the i[th] employed bee, v_i^j is the new solution for x_i^j , x_k^j is the

neighbor bee of x_i^j in employed bee population, φ is randomly selected in the range [-1, 1], D is the dimension of the problem and N denotes the number of employed bee. In the above equation j and k values are selected randomly.

In order to generate the new food source position every onlooker bee memorizes the solution of n employed bee based on the fitness values of the employed bee. The probability pi of the onlooker bee will select the solution of the i[th] employed bee.

$$P_i = F(i) \Big/ \sum_{i=1}^{n} F(i) \longrightarrow (5)$$

In the above equation (6) the fitness value of the i[th] employed bee is given using the formula,

$$F(i) = \begin{cases} \dfrac{1}{(1+obj(1))} & if\ (obj(i) \geq 0) \\ 1+abs(obj(i)) & if\ (obj(i) < 0) \end{cases}$$

$obj(i)$ is the objective function specific for the problem.

Onlooker bees produce new solutions from the selected solutions depending on p_i and evaluate them. If the new solution has equal or better fitness than the old solution, then it is changed with the old one in the memory. Else, the old is retained. If a solution is not improved over a prearranged number of cycles, then that food source is assumed to be abandoned. The abandoned food source is replaced by new food source generated by scout bees. This procedure is continued until the termination criterion is reached.The optimum weight set is determined using the implementation of the above said ABC optimization algorithm.

c) Authentication Scheme

Table 1: List of notations used in the proposed scheme

Registrant	Xi
Registrant User name	IXi
Registrant Password	Pi
Registrant Biometric	BKi
Registrant Masked Password	MPi
Smart card User	SXi
Login User name	SIXi
Login Password	SPi
Login Biometric	SBKi
Login Masked Password	SMPi
Smart card reader	SMi
Base station	Yi
String Concatenation operator	‖

In Table 1, the list of notations used in this proposed scheme is given.

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.

$$MP_i = (P_i \| IX_i) \longrightarrow (6)$$

Smart card reader SM_i receives the registrant message $< MP_i, BK_i >$ from the registrant user X_i . 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 .Ifthe above request is accepted, the base station receives the masked password MP_i .Then the masked password will get encrypted E_i as specified in eqn. 1 and the encrypted message is decrypted D_i using eqn. 3. The encryption and decryption 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.

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.

$$SMP_i = (SP_i \| SIX_i) \longrightarrow (7)$$

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 passwordas in eqn. 2 and then decrypt the masked password as in eqn. 4. After decryptionBase

station Yi verify the user with the registered user. Check SMP_i is equal to the stored MP_i. If not, then report wrong password Pi 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 Yi 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 Yi receives login message $< SIX_i, SP_i >$ from the user SX_i, Yi first checks whether received SMP_i is equal to the stored MP_i. If not, then report wrong password Pi 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.

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. This attacks are explained below:

Privileged insider attack

In this scheme, the user does not send his/her password in plain text during registration. Here the user name IX_i and the password P_i is first masked to produce MP_i, which is $MP_i = (P_i \| IX_i)$. It is computationally infeasible to find P_i from MP_i because the base station encrypt only the MP_i, but not the original user name and password. So the privileged insider of the base station cannot know the password Pi. Thus he/she cannot impersonate the user in thoseservers where the user might have registered himself/herself with the same password. So this proposed scheme is resistance to the privileged insider attack.

Password Guessing attack

Consider the situation where a user lost his/her smart card, and it is found by an attacker or is stolen by an attacker. In that case, the attacker cannot impersonate that user by using the smart card because if the login message $< SMP_i >$ is received by the base station Y_i ,it verify the user with the registered user. Check SMP_i is equal to the stored MP_i. If not, then report wrong password Pi 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.So this scheme is resistance to guessing attack.

Stolen verifier attack

In registration phase, user does not send the user name and password directly to the BS. It is masked and sent to the base station to produce smart card. So it is resistance to stolen verifier attack.

Man-in-the-middle attack

Suppose an attacker intercept a login request message $< SMP_i >$. However, it cannot secretly relay and alter the communication because first the base station verify the masked password SMP_i of the login user in the registered users. If the user is valid, then only base station ask the biometrics of the login user. Also the base station will check whether the login user biometric is matched with the registered biometric. So, the intruder can't interrupt the communication between two parties. Thus, man-in-the-middle attack is not possible in this proposed scheme.

DoS attack

Suppose an adversary has found or stole the smart card of a legitimate user Xi. However, in this proposed scheme, the base station verify the masked password SMP_i of the login user or smart card user. If the user is valid, then base station ask the biometrics of the smart card user. If the finger print is not matched, the intruder can't access the real time data. Thus the proposed scheme is secure against denial of service attack.

Many logged-in users with same login-id attack

This scheme can prevent the risk of many logged-in users with the same login ID. Here login process starts only when the user inserts his/her card into the card reader, and all computations is performed only during the period when the card is still inside the card reader. Once the card is removed the login process is terminated.

Smart card breach attack

Suppose a smart card is lost or stolen. Although it is assumed that a smart card cannot be cracked, an adversary may perform side channel attacks, including differential power analysis and invasive attack. Here, adversary cannot find MPi as he does not have knowledge of Pi. Thus, the proposed scheme can resist smart card breach attack.

5 Experimental results

The proposed methodology will be implemented using Matlab and validated by comparing with the conventional techniques. The database we use in our experiments is the NIST Special Database 4 (NIST-4) [27], which is a publicly available fingerprint database. The size of the fingerprint images is 388×374 pixels with a resolution of 96×96 DPI.

The Computational time for various existing methods for the registration, login and authentication phase compared with our proposed approach is given in Figs. 2-4. The proposed system will provide less computation time than the existing methods.

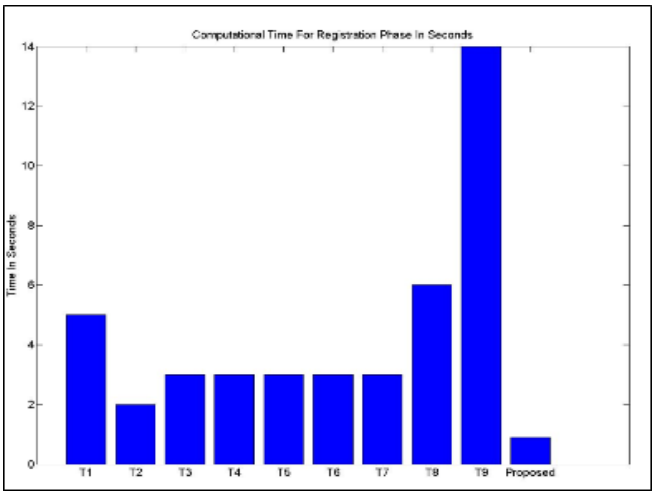


Fig 2: Comparison of Computational time in registration phase

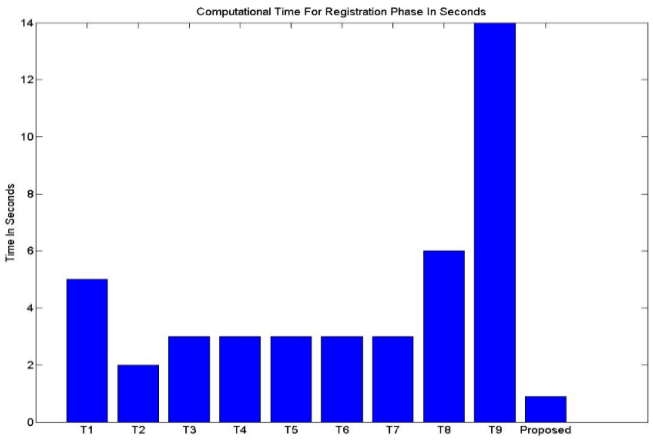


Fig 3: Comparison of Computational time in login phase

ACKNOWLEDGMENT

I Pay my sincere thanks to my Guide for providing me a proper guidance to do the research work.

REFERENCES

[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.

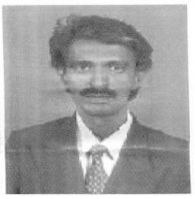
[13] H. Ru Tseng, R. H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in IEEE Global Telecommunications Conference (GLOBECOM'07), pp. 986–990, 2007.

[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.
[16] R. Watro, D. Kong, S. F. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Tinypk: Securing sensor networks with public key technology," in Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04), pp. 59–64, 2004.
[17] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), pp. 244–251, 2006.
[18] J. Yuan, C. Jiang, and Z. Jiang, "A biometric based user authentication for wireless sensor networks," Wuhan University Journal of Natural Sciences, vol. 15, no. 3, pp. 272–276, 2010.
[19] A. K. Das, "Improving identity-based random key establishment scheme for large-scale hierarchical wireless sensor networks," International Journal of Network Security, vol. 14, no. 1, pp. 1–21, 2012.
[20] M. L. Das, "Two-factor user authentication in wireless sensor networks," IEEE Transactions on Wireless Communications, vol. 8, no. 3, pp. 1086–1090, 2009.
[21] William Stallings, "Cryptography and Network Security-Principles and Practices," 3rd Edition, Pearson Education Asia, 2003.
[22] Xue-lei Li, Qiao-yan Wen, Hua Zhang, Zheng-ping Jin and Wen-min Li, "Offline Password Guessing Attacks on Smart-Card-Based Remote User Authentication Schemes," In Proceedings of the 6th International Asia Conference on Industrial Engineering and Management Innovation, Atlantis Press, pp. 81-89, 2016.
[23] Chun-Ta Li, Hua-Hsuan Chen, Min-Jie Syu, Chun-Cheng Wang and Cheng-Chi Lee, "Cryptanalysis of an anonymous multi-server authenticated key agreement scheme using smart cards and biometrics," In Information Networking (ICOIN), IEEE International Conference, pp. 498-502, 2015.
[24] Mrudula Sarvabhatla, Kodavali Lakshmi Narayana and Chandra Sekhar Vorugunti, "An improved secure remote user authentication scheme using smart cards with check digits," Signal Processing, Informatics, Communication and Energy Systems (SPICES), IEEE International Conference, PP. 1 - 5, 2015.
[25] Hao Lin, Fengtong Wen and Chunxia Du, "An Improved Lightweight Pseudonym Identity Based Authentication Scheme on Multi-server Environment," In Wireless Communications, Networking and Applications, Springer India, pp. 1115-1126, 2016.
[26] Fengtong Wen, Willy Susilo, Guomin Yang, "Analysis and Improvement on a Biometric-Based Remote User Authentication Scheme Using Smart Cards," Wireless Personal Communications, pp.1747-60, 2015.
[27] C.I. Watson, C.L. Wilson, NIST special database 4, fingerprint database, U.S. National Institute of Standards and Technology, 1992.
[28] E. J. Yoon, K. Y. Yoo, "Robust biometrics based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," The Journal of Supercomputing, vol. 63, no. 1, pp. 235–255, 2013.
[29] Watro, R., Kong, D., Cuti, S., Gardiner, C., Lynn, C.,Kruus, P. "TinyPK: securing sensor networks with public key technology". In: Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks, SASN 2004, Washington, DC, USA; October 2004. p. 59–64
[30] Das, M. L. "Two-factor user authentication in wireless sensor networks". IEEE Transactions on Wireless Communications 2009; 8(3):1086–90.
[31] Wong, K., Zheng, Y., Cao, J., Wang, S. "A dynamic user authentication scheme for wireless sensor networks". In: Proceedings of IEEE international conference on sensor networks, ubiquitous, and trustworthy computing, IEEE Computer Society; 2006. p. 244–51.

Authors Profile

Ms.D.Thamaraiselvi Received herM.tech Degree from SATHYABAMA UNIVERSITY ,T.N ,India, in the year 2010. She is Pursuing her Ph.D and working as Assitant Professor in the Department of Computer Science and Engg in SCSVMV UNIVERSITY Kanchipuram,,T.N,India. She is having more than five years .she is a member in IANG .Her research interest is Network security, Datamining .



Dr. M. Ramakrishnan, Received his Doctorate degree from Anna university Coimbatore ,T.N ,India. Currently he is working as Professor in Madurai Kamar ajar University, Madurai, T.N, India. He has published more than 20 research articles in a referred journals and having more than 15 years of teaching expereince. His Research interest is Network security.

