Artificial Bee Colony Algorithm Role in The Field of Authentication

Dr. D.Thamaraiselvi
Asst.professor, Dept of CSE
SCSVMV

Abstract- *Authenticating a user is very important in un attended environment like wireless sensor network. Wireless sensor networks are used to monitor physical or environmental conditions. authenticating a user in wireless sensor networks is more difficult than in traditional networks owing to sensor network characteristics such as unreliable communication networks, resource limitation, and unattended operation. As a result, various authentication schemes have been proposed to provide secure and efficient communication. In this proposed paper biometric based remote user authentication using ABC ALGORITHIM is used for optimization .*

Keywords- user authentication, Biometric ,ABC, OPTIMIZATION

I. INTRODUCTION

A wireless sensor networks consist of a set of nodes deployed in large numbers to collect and transmit environmental data to a collection point named Base Station (BS).These networks have a particular interest for military applications, environmental, home automation, medical, and many of the applications related to the monitoring of critical infrastructures. A user can access to the collected data either directly or remotely . In the first case, user with mobile device communicates directly with the sensor nodes. For security reasons, access to the sensor networks should be controlled. We take into consideration that authenticating remote users in WSNs is an important security issue due to their unattended and hostile deployments. Moreover, sensor nodes are usually equipped with limited computing power, storage, and communication modules. Thus, authenticating remote users in such resource-constrained environment is a challenge security concern. Accessing this data will, in general, not be for free since the deployment of a WSN induces some costs. This means that the deployment agencies of some of these services will make them available only to subscribers. In this case, a WSN must be able to distinguish legitimate users from illegitimate ones, resulting in the problem of access control. The customer of this company must pass an authentication protocol for each new session and take data arding to his privileges described in the database system.

In this paper, we propose a user authentication scheme based on (BIOMETRIC) finger print of the user . It provide authentication of the user in wsn. WSN deployed by a commercial company over a large geographical area to capture the physical phenomena of the environment such as temperature, humidity, etc. Accessing this data will, in general, not be for free since the deployment of a WSN induces some costs. This means that the deployment agencies of some of these services will make them available only to subscribers. In this case, a WSN must be able to distinguish legitimate users from illegitimate ones, resulting in the problem of access control.

II. RELATED WORK

This paper extracts the features of fingerprint and the standard deviation is calculated and stored in base station. Artificial bee colony alg is used for optimized matching of the finger print.

A. Fingerprint Enhancement

This is an usually required process in creating a security system with the help of biometrics. This process includes subsequent processing on the gathered fingerprint image. Fingerprint consists of sequence of ridges and furrows on the finger surface. This provides the individuality of the users fingerprint. No two fingerprints can have the similar existence of ridges and furrows. Minutiae points are local ridge features that appear at either a ridge bifurcation or a ridge ending. The ridges hold the information of features mandatory for minutiae extraction. Hence the clarity of the ridge occurrences in a fingerprint image must be very important. The gathered image is then enhanced with the help of image enhancement methods in order to diminish the noise in the image. The image enhancement methods used to enhance fingerprint image are normalization, orientation estimation, local frequency estimation, Gabor filtering, and thinning.

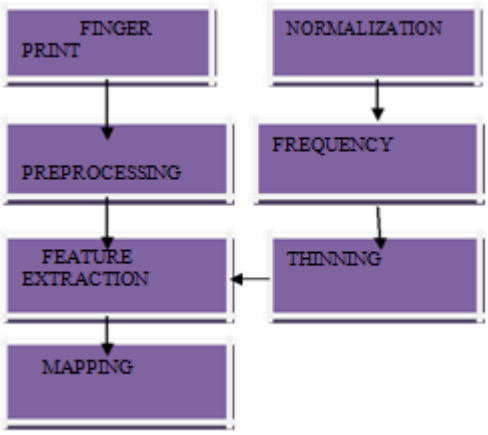


FIG:1 extracting miniature points

B. Normalization

Normalization technique is nothing but the standardization Dof. Minutiaethe The n xt step is to obtain the minutiae from the thinned intensity values in an image by altering the range of gray-level values with the intention that it occurs within a preferred range of image values. The most commonly used technique of minutiae extraction is the Crossing Number (CN) model. This Additionally the ridge structure in the fingerprint does not undergo any alterations in its structure because of this process involves the utilization of the skeleton image in processing. This process is which the ridge flow pattern is eight-connected. The performed in order to standardize the dynamic levels of dissimilarity in gray-level values that assist the processing of subsequent minutiaemage improvement processes. neighborhood of every ridge pixel in the image by means of calculated which is defined as partially the addition of the differences among the pairs of neighboring pixels in the eight-neighborhood. Figure 6 indicates the list of minutiae in a fingerprint image. Figure 6. Minutiae extraction on a fingerprint image.

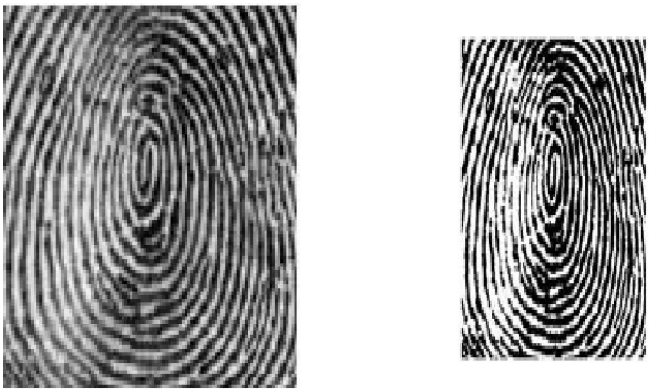
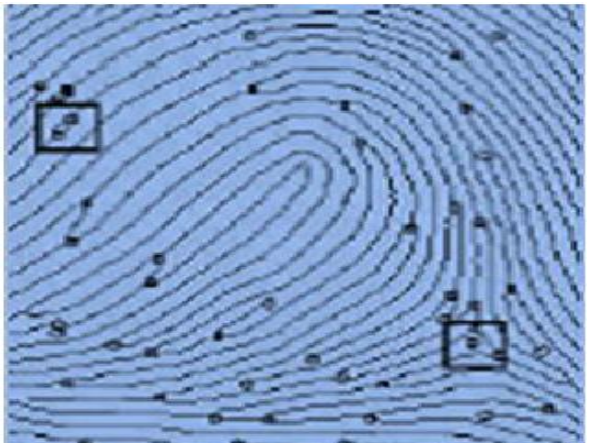


Figure 2 represents an image of the fingerprint before and after normalization

C. Thinng:

The final image improvement pace normally performed before minutiae extraction is thinning [14]. Thinning is a morphological process that consecutively takes away the foreground pixels till they are one pixel apart. By applying the thinning technique to a fingerprint image maintains the connectivity of the ridge structures during the formation of a skeleton stage of the binary image. This skeleton image is subsequently utilized in the following extraction of minutiae.

calculated which is defined as partially the addition of the differences among the pairs of neighboring pixels in the eight-neighborhood. Figure 6 indicates the list of minutiae in a fingerprint image. Figure 6. Minutiae extraction on a fingerprint image.



3.1 ABC OPTIMIZATION ALG:

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.

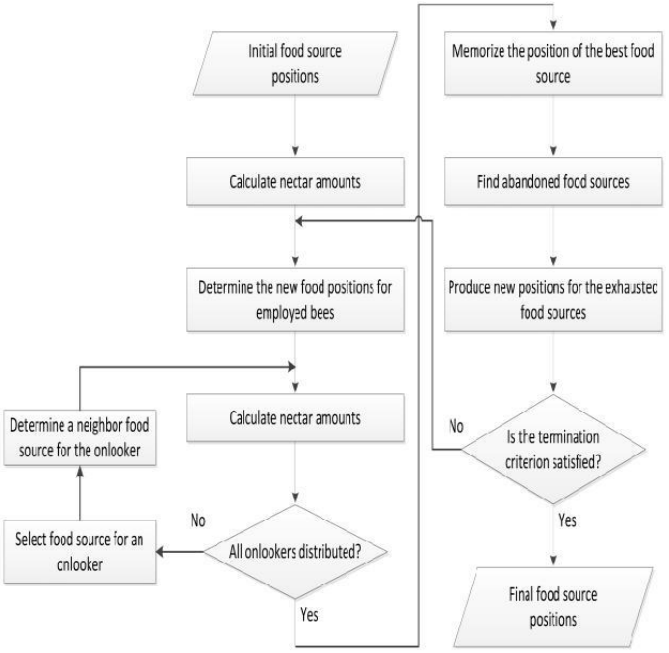


FIG5: ABC ALG

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

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.

$$P_i = F(i) \Big/ \sum_{i=1}^{s} F(i)$$

In the above equation (11) the fitness value of the i^{th} employed bee is given using the formula,

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

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

3.2 USER AUTHENTICATION SCHEME:

Table1: Notations

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	‖

3.2 A.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 Pi and personal biometrics BKi 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 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 Yi .Ifthe above request is accepted, the base station receives the masked password MPi .Then the masked password will get encrypted Ei as specified in eqn. 1 and the encrypted message is decrypted Di 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 calculatethe standard deviation SD using eqn. 6.The evaluated details are stored in the Yi . After registering, the base station send a smart card to the registered user.

3.2 B. 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 SPi 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 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.

3.2.C.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.

IV. 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:

4.1 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.

4.2Password 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 *SMPi* is received by the base station *Yi* ,it verify the user with the registered user. Check *SMPi* is equal to the stored *MPi* . 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.

V. CONCLUSIONS

In this paper user is authenticated using biometric finger print data where the features are extracted and stored in base station when a user wants to access the data he has to insert smart card and the finger .The standard deviation is calculated using artificial bee colony algorithim for searching in an optimized way.

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, b“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.