A Novel Secure Routing Protocol based on Retina Biometric Authentication

R. Sudha and M. Devapriya

***Abstract*---**The development of the internet in the recent years leads to the security and authentication of users data. It is still a challenging problem in the Wireless Body Sensor Network (WBSN). It is important to protect the personal medical and health information collected by the biosensors. To protect the physiological data biometric authentication is implemented on physical features to provide privacy. Biometric field recently works on reduce in process delay and enhances the level of accuracy. WBSN authenticates systems works based on retina intrinsically of physiological and behavioral characteristics of persons. It provides solutions to network security problems by replacing the authentication component of the traditional systems. The experimental results shows that by implementing BFTASR protocol on retina authentication performance proves that more secure than existing approach.

***Keywords*---**Biometric, Image Acquisition, Image Pre-processing and Wireless Body Sensor Network (WBSN)

I. INTRODUCTION

DUE to increase in global population there is need in developments of new diagnostic techniques and medication discoveries, will place increasing demand on medical and health-care resources. There is a need for technology improvement in Integrated Circuits (ICs) along with wireless technology and physiological sensors. These things provide opportunities to develop efficient and reliable monitoring devices. By using these technological devices Wireless Body Sensor Network (WBSN) can be obtain for physiological measurements and secured monitoring. In general, WBSNs consist of several sensor nodes which can sample, process and communicate wirelessly on environmental parameters. These physiological parameters are typically blood glucose and oxygen levels, pulse rate, blood pressure, circadian rhythm and wake-sleep patterns.

In WBAN, various security problems are arises such as data failure, authentication and access control. It tends to inconsistency in make use of high security system directs to in computational performance. The main problem with these traditional techniques is that there is possible to forget the password and if the password is known to others then the unauthorized user can access the user. It leads to the usage of Biometrics authentication mainly for security. The security of the biometrics which is based on authentication system provides better security and authentication. The biometrics solution is superior in low power consumption and computation complexity. It is different from traditional biometrics, where the patterns used are captured on a specific part of the body surface such as finger prints, eye retinas and irises, voice patterns, facial patterns, and hand measurements. The existing methods deals with iris biometric features for security but can be misused in some applications So this type of authentication measures cannot be implied in military and other fields. Retina provides high level of security due to its original robustness against imposture. Retina as a biometric has certain advantages when compared to other biometrics. This paper deals with the retina biometric authentication for secure and uses a stable physiological feature.

The remainder of this paper is organized as follows. Section 2 discusses related work in association with biometric based network security. Section 3 describes the proposed Retinal biometric authentication. Section 4 demonstrates the performance measures and Section 5 concludes the paper.

II. RELATED WORKS

There are several approaches available in the literature in the field of establishing network security based on biometric features obtained from individual user. Some of the approaches based on the biometric technique are discussed in this section.

Patahnia *et.al* (2014) discussed about wireless body area network collects the parameters of a patient's body and movements by small wearable or implantable sensors. Also, explains about security attacks and requirements in WBAN to provide a robust security system and a part of its authentication. This system provides secured authentication in necessary applications of WBAN technology especially in medical and military. Bursse*et.al* (2015) presented a work to provide solution for provide resilient communication, enhance privacy, and provide anonymity. Saraswathi *et.al* (2011) proposes technique for network security using Retinal biometrics feature works on personal authentication. The techniques in the areas of image processing are reused to extract the bifurcation points of retina biometric image. The paper provides an enhanced preprocessing technique performance of the proposed biometric based network security system. Borah *et.al* (2012) designed a retina based system where the ANN forms a critical decision support system. ANN is configured properly to handle

Manuscript received on August 21, 2017, review completed on August 21, 2017 and revised on August 30, 2017.

R. Sudha is with the Department of Computer Science, PSG College of Arts and Science, Coimbatore, Tamil Nadu, India. E-Mail: sudha279@yahoo.com

M. Devapriya is with the Department of Computer Science, Government Arts College, Coimbatore, Tamil Nadu, India. E-Mail: devapriya_gac@rediffmail.com

Digital Object Identifier: BB082017001.

variations in the retinal images developed a biometric verification system and this system is reliable and efficient. Uludag *et.al* (2004) explains the main challenge in using the stored biometric template of a user in the database whereas the complete biometric authentication is needed to reveal the key. In this framework, releasing a key using common methods based on biometric authentication cannot applicable in many cryptographic applications. In such applications biometric key generation is needed to release the transmitted encrypt message.

Panchal *et.al* (2016) proposed a reliable method for retina feature extraction. The input retina image is tracked using the binarization. By using a hybrid method of morphology an improved results are obtained by Scanning Window Analysis (SWA). The validity of this algorithm is calculated by testing the system on retinal image database of RIDB contains a set of 55 retinal images of healthy, glaucoma, and diabetic retinopathy images. Xu*et.al* (2010) provides a method for accurate segmentation of retina blood vessels to overcome the variations in contrast of large and thin vessels. The above method produces a binary image to extract large connected components (large vessels) by using adaptive local thresholding. Then the SVM identifies resulted thin vessel segments which can be lengthened by tracking. This method can avoid heavy computation and manual intervention. Prakash et.al (2014) presents a secure communication in wireless mesh networks by combining with a network coding to multiple layered encryption of onion routing. It provides higher level of security and privacy for network information by avoiding transmission of plain text with decrypted data to its source and destination.

III. PROPOSED METHODOLOGY

Retinal recognition system is very useful compared with other biometric system, the pattern of blood vessel in retina is fixed and not exposed externally all over the life time of an individual. Due to detachment the recognition of retina is hard and the average feature vector size is very small compared to other biometric vectors. The rich and unique features can be extracted from the retinal blood vessels.

The location of retina is in back of the eye and it is precise and difficult to acquire the retinal image. In the human body, part of Retina is invisible in comparison to iris or face, which allows being captured even from longer distances. A suitable optical system is required to focus the whole eye through the pupil and take a picture of the retinal part. It is not possible to find such recognition because the attacker would have to find retinal image from the appropriate person to reproduce an optical system of the eye. A proper biometric function can be carried out in retina. Blood vessel bifurcations pattern consists of up to 400 unique features and is stable for the whole life of an individual.

The retina contains photoreceptor cells called rods and cones. They receive the light and convert it to electrical pulses which are carried to the brain via the optical nerves present in the retina. Basically, the rod system is low spatial resolution with high sensitive to light whereas the cone system is of high spatial resolution but is relatively insensitive to light. The cones are responsible for enabling us to see colors while the rods are responsible for facilitating night vision and peripheral vision.

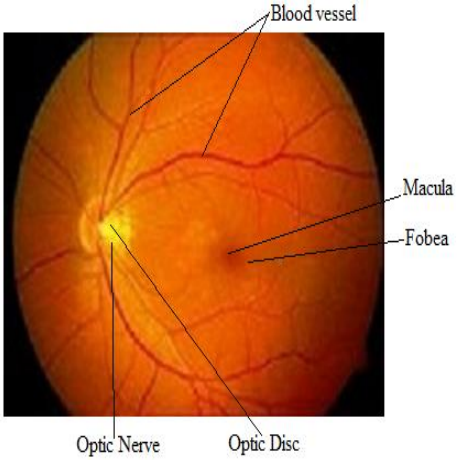

Fig 1 Structure of Retina Image

A new Biometric Fusion Based Trusted Anonymous Secured Routing Protocol (BFTASR) which assures prevention against such attacks is implemented in biometric authentication. Secure routing is necessary because the medical report gives a detailed view for diagnosing. To make it effective there is a need to develop the secure routing technique that converts the extracted features of retina which in the representation of binary data to a DNA based representation string [7]. The process of retina biometric authentication involves three stages such as image acquisition, image pre-processing and feature extraction. The captured retina images are pre-processed for following manipulation. The process of retinal biometric authentication is shown in figure 2 as extraction the minutiae points from biometric feature obtained from the user.

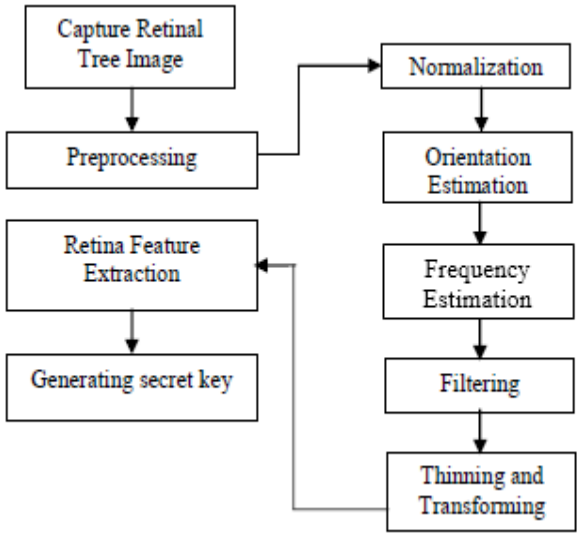

Fig.2 Extraction of Minutiae Features

- Image acquisition: It captures sequence of input images.
- Image preprocessing: It involves various stages for manipulation of image and interpretation by subsequent stages. The steps include removal of noise and variation of intensity recorded, sharpening, improving the contrast and strengthening the texture of the image. Further image restoration extracts information of image in a degraded form to make it suitable for subsequent processing and interpretation.
- Feature extraction: It is a process in which information and details of a retinal image section is captured for analysis. The process of feature extraction involves features extracted from the segmented blood vessels and from the whole retinal image [8]. It involves two steps of feature extraction they are blood vessel segmentation and feature calculation. The blood vessels were segmented using morphological operations. The following steps are involved in the retinal vessel segmentation technique.
- The retinal RGB image is extracted and by applying the histogram equalization technique to improve the contrast of the image.
- Morphological opening for segmentation is performed with a disc structuring element to filter out the image structures
- Classification: This is the main component of the system for generating a key and determines the feature extraction performance. The final retinal image is converted by using a digital representation called a template.

The final retinal image of the user is stored as encrypted binary template for authentication purpose. Feature extracted templates are matched with known patterns in the feature database [13].

A. Key Generation

The generation of keys in eye biometric model has proven to be one of the accurate modes of parameters. The retina biometric features are unique and remain unchanged in lifetime [11]. To extract the retinal features such as blood vessels pattern (vascular tree) which undergoes the thinning process on vascular tree of blood vessels. The extracted features includes identification of the endpoint of each pattern and also the bifurcation points. Thus obtained endpoints are used to generate the key for encryption/ decryption of message. The extracted feature will be thus moved from the origin of an image, pixel by pixel at a time in x and y axis. The output of endpoint (x, y) coordinates values of each endpoint and degree theta. Table 1 indicates the sample end points of thinned image.

TABLE 1
POINTS OF THINNED IMAGE

X	Y	Theta
67	78	230
132	95	154

The above (x, y) coordinate value of each pixel is used in the following algorithm to generate the key.

Step 1- Read the x and y coordinate values of an endpoint from the thinned image
Step 2- Compute the sum using the formula

$$sum = sum + \sum_{i=0}^{n-1} (x_i * y_i) \; mod \; p$$

Where p is a prime number and 'i' is the coordinate value of each endpoint pixel.
Step 3- Find the equivalent binary value of the sum that becomes the key for encryption and decryption of message

As structuring element match with the thinned image pixel, it finds an edge between two pixels and continues this process for the entire image to find the number of endpoints in an image. If the structuring element does not match with the neighbor then bifurcation points set endpoint as with red in color and green color.

IV. EXPERIMENTAL RESULTS

The performance of proposed BFSTR for Retinal biometric authentication is analyzed and simulated by NS2 tool. To perform the retina authentication by configuring the network with an average speed of 4 ms and the sensing area 100m*100m. The result was simulated for 100, 200, 500, 700 and 1000 nodes. The performance of the proposed method was compared with LEACH-E, LEACH-C, LEACH and ECAR. The results have been analyzed using the three performances metric are Packet Delivery Ratio (PDR), throughput and number of dropped packets on comparing with malicious attacks. Table 2 shows the performance comparison of Packet Delivery Ratio (PDR), Throughput and End-to-End delay with increase in number of sensor nodes before Malicious attacks.

TABLE 2
PERFORMANCE COMPARISON BEFORE MALICIOUS ATTACKS

Sensor Nodes	Protocols	PDR	Throughput (%)	End-to-End Delay (ms)
100	LEACH-E	45	47	61
	LEACH-C	54	40	54
	LEACH	51	58	58
	EECRA	59	51	47
	BFTASR	63	55	49
200	LEACH-E	55	51	55
	LEACH-C	48	45	47
	LEACH	60	41	49
	EECRA	68	58	35
	BFTASR	72	65	41
500	LEACH-E	41	48	45
	LEACH-C	61	39	41
	LEACH	44	45	55
	EECRA	754	67	49
	BFTASR	81	54	38
700	LEACH-E	55	55	58
	LEACH-C	68	48	38
	LEACH	58	63	42
	EECRA	83	59	54
	BFTASR	88	70	29
1000	LEACH-E	64	61	54
	LEACH-C	72	65	40
	LEACH	79	69	35
	EECRA	90	71	29
	BFTASR	93	79	25

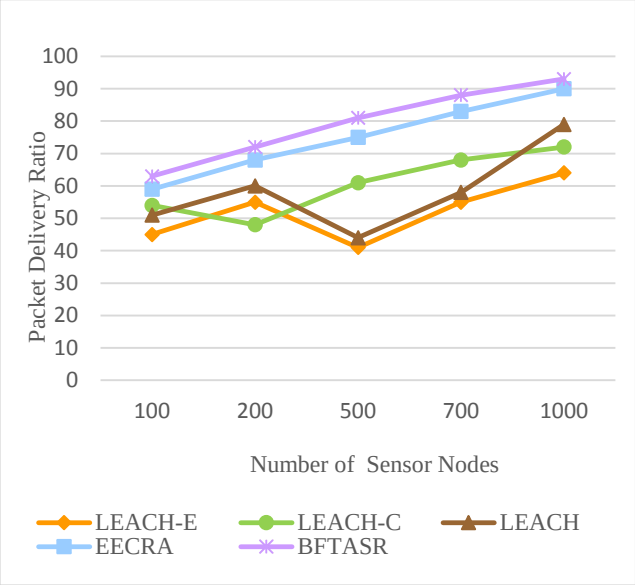

Fig 3 Packet Delivery Ratio before Malicious Attacks

Figure 3shows the proposed BFTASR has highest ability to identify packet dropping attack with the help of its trust management approach and it outperforms the existing techniques.

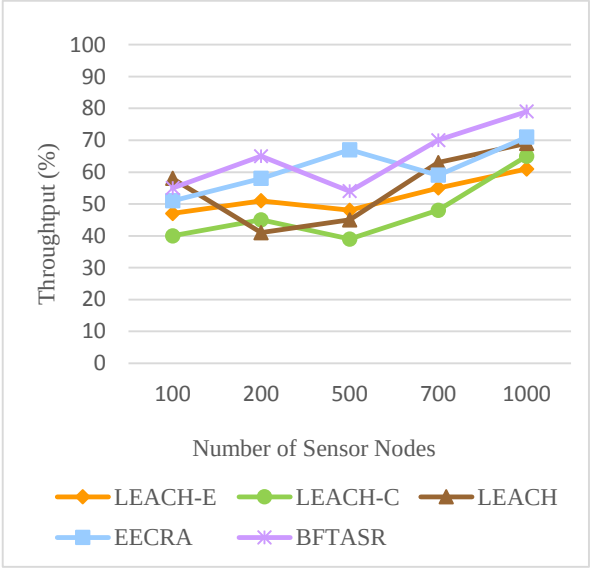

Fig 4 Throughput before Malicious Attacks

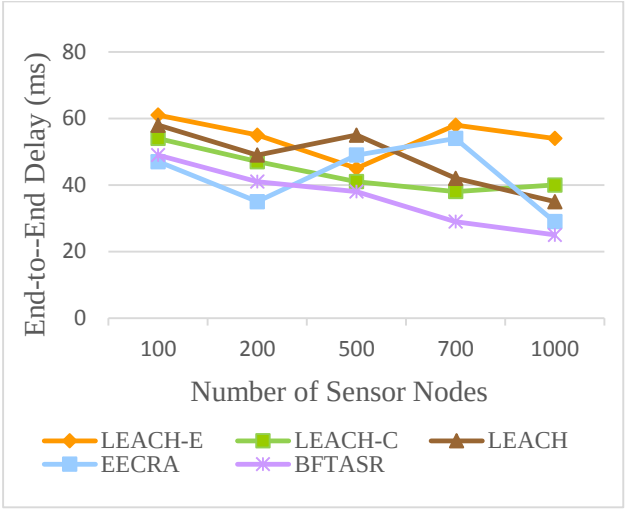

Fig 5 End-to-End Delay before Malicious Attack

Figure 4shows the Throughput of the proposed BFTASR is higher than the remaining existing protocols. Figure 5 the proposed BFTASR reduces the need of re-routing due to its trust based authentication and onion routing which results in 25 ms less of delay in average.

Table 3 shows the performance comparison of Packet Delivery Ratio (PDR), Throughput and End-to-End delay with increase in number of sensor nodes after Malicious attacks

TABLE 3
PERFORMANCE COMPARISON AFTER MALICIOUS ATTACKS

Sensor nodes	Protocols	PDR	Throughput (%)	End-to-End Delay (ms)
100	LEACH-E	57	47.5	61
	LEACH-C	46	39	57
	LEACH	39	54	47
	EECRA	72	65	68
	BFTASR	63	54	51
200	LEACH-E	48	35	52
	LEACH-C	54	42.8	65
	LEACH	61	49	35
	EECRA	69	57.8	58
	BFTASR	76	65	41
500	LEACH-E	64	50	40
	LEACH-C	69	35	59
	LEACH	48	59.5	51
	EECRA	74	65	45
	BFTASR	85	72.5	35
700	LEACH-E	58	59.4	58
	LEACH-C	65	51.5	51
	LEACH	72	65	47
	EECRA	85	72	37
	BFTASR	92	80.5	24
1000	LEACH-E	71	62.3	49
	LEACH-C	78	69	35
	LEACH	82	73.5	22
	EECRA	90	80	28
	BFTASR	97.5	84	19

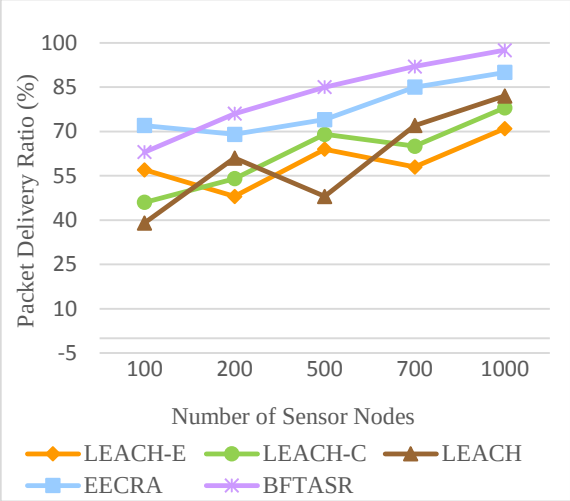

Fig 6 Packet Delivery Ratio after Malicious Attacks

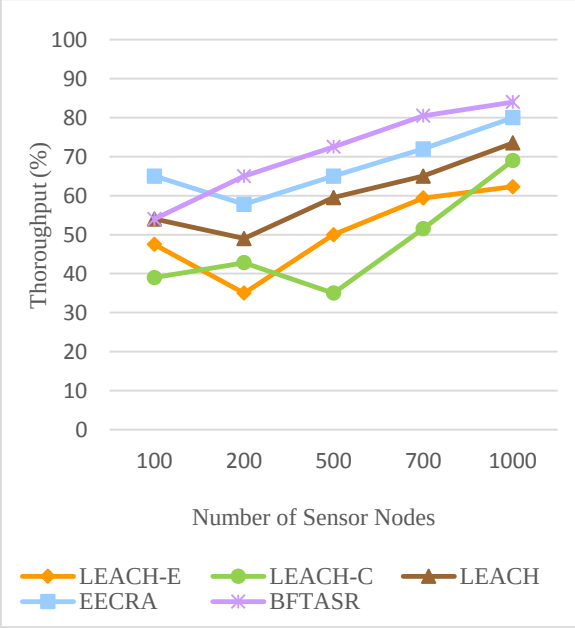

Fig 7 Throughput after Malicious Attacks

Figure 6-8 shows the of Packet Delivery Ratio (PDR), Throughput and End-to-End delay after malicious attacks of BFTASR protocol using retina authentication requires less processing delays than the other protocol. If the protocol is under a heavy attack, it will launch new route discoveries for the broken routes, which introduce more delays in average. Compared to the attacked LEACH-E, LEACH-E, LEACH and EECRA the proposed BFTASR reduces the need of re-routing, resulting in 19 ms less of delay in average. The simulation results confirm that BFTASR is very effective in delivering data packets to their intended destinations even in the presence of large proportion of malicious entities.

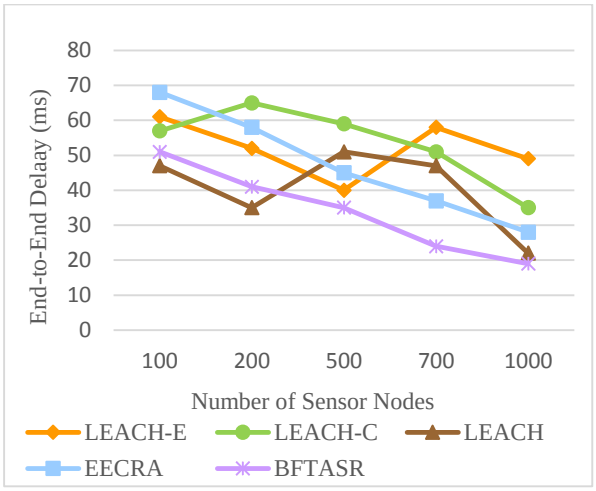

Fig 8 End-to-End Delay after Malicious Attacks

V. Conclusion

Securing information across the network is one of the key challenges. This paper is proposed to generate a secure key by using retina biometric technique since retina is unique and reduces the duplication. A system designed to provide by means of verification BFTASR routing protocol is a more feasible and providing a high security than other techniques. The overall performance shows that proposed scheme achieves high throughput and packet delivery ratio is provided by authorized node of WBAN and decreases the average end to end delay.

References

[1] Pathania, S. and Bilandi, N., 2014. Security issues in Wireless Body area network. Int J ComputSci Mobile Comput, 3(4), pp.1171-1178.
[2] Brussee, P.W.G. and Pouwelse, J.A., 2015. Survey of robust and resilient social media tools on Android. arXiv preprint arXiv:1512.00071.
[3] Saraswathi, K., Jayaram, B. and Balasubramanian, R., 2011. Retinal biometrics based authentication and key exchange system. International Journal of Computer Application, 19(1).
[4] Borah, T.R., Sarma, K.K. And Talukdar, P.H., Retina Based Biometric Identification System In 2012.
[5] Uludag U, Pankanti S, Prabhakar S, Jain AK. Biometric cryptosystems: issues and challenges. Proceedings of the IEEE. 2004 Jun; 92(6):948-60.
[6] Panchal, P., Bhojani, R. and Panchal, T., 2016. An Algorithm for Retinal Feature Extraction Using Hybrid Approach. Procedia Computer Science, 79, pp.61-68.
[7] Choraś, R.S., 2012, August. Retina recognition for biometrics. In Digital Information Management (ICDIM), 2012 Seventh International Conference on (pp. 177-180). IEEE.
[8] Kirbas, C. and Quek, F., 2004. A review of vessel extraction techniques and algorithms. ACM Computing Surveys (CSUR), 36(2), pp.81-121.
[9] Xu, L. and Luo, S., 2010. A novel method for blood vessel detection from retinal images. Biomedical engineering online, 9(1), p.14.
[10] Farzin, H., Abrishami-Moghaddam, H. and Moin, M.S., 2008. A novel retinal identification system. EURASIP Journal on Advances in Signal Processing, 2008(1), p.280635.
[11] Tajuddin, M. and Nandini, C., 2013. Cryptographic Key Generation using Retina Biometric Parameter. International Journal of Engineering and Innovative Technology (IJEIT) Volume, 3.
[12] Borah, T.R., Sarma, K.K. and Talukdar, P.H., 2013. Retina and fingerprint based biometric identification system. International Journal of Computer Applications (IJCA), 74.
[13] Barkhoda, W., Tab, F.A. and Amiri, M.D., 2009, October. Rotation invariant retina identification based on the sketch of vessels using angular partitioning. In Computer Science and Information Technology, 2009. IMCSIT'09. International Multiconference on (pp. 3-6). IEEE.