

# Improved Security Levels of WLAN through DBSPS

R.S.K.S. Ganesh L

Dept of Computer Science and Engineering  
Swarnandhra College of Engineering and  
Technology, JNTU-K,  
West Godawari, A.P, INDIA

Sudhakar Godi

Dept. of Computer Science and Engineering  
Swarnandhra College of Engineering and  
Technology, JNTU-K,  
West Godawari, A.P, INDIA

## ABSTRACT

Wireless Networks plays a vital role in the field of Information and Communication Technology (ICT). Security to the Wireless networks is a major challenge to the researchers and practitioners. Especially Wireless Local Area Networks are more prone to security threats. This work introduces a novel technique Double Bio-cryptic Security-aware Packet Scheduling (DBSPS) which strengthens security aspects in WLAN's. To strengthen the WLAN security, this work improved the security levels security through double Biometric image encryption. Simulations were performed on Thumb print, Iris, Palm print and Facial databases by using the Matlab and later DBSPS results were compared with the of present Enhanced Bio-Cryptic Security-aware Packet Scheduling (EBSPS) and Bio-Cryptic Security-aware Packet Scheduling (BSPS) algorithms. In order to achieve high Quality-of-Security (QoS) in WLAN, the EBSPS is replaced with the new DBSPS. This DBSPS Algorithm assures the finest performance in increasing the security level to the desirable Wireless Node (WN) applies Double Bio-cryptographic methods in every security level. Finally, simulation outcome proved that proposal mechanism DBSPS is performing well than existing techniques in terms of the security.

## General Terms

Wireless communications and Security

## Keywords

Bio-Cryptography, Quality-of-Security, Biometrics, Security Level, Double Bio-cryptic Security-Aware Packet Scheduling-Algorithm, Enhanced Bio-cryptic Security-Aware Packet Scheduling-Algorithm, Bio-cryptic Security-Aware Packet Scheduling-Algorithm, BSPS, ASPS, DBSPS, EBSPS.

## 1. INTRODUCTION

The usage of Wireless Networks is increasing day-to-day. But Wireless Networks are less attenuated to the security threats, when compared with the Wired Networks like Data Interception, Network Intrusion, Radio Jamming, Denial of Service, Bandwidth Stealing, Masquerade, Litigation Risks, Reputation, Financial Risk, Evil Twins and many more threats. Especially Wireless LAN's are facing severe security risks like Eavesdropping, Illicit entry and Denial of Service [1].

According to recent survey reports by SOPHOS on Security Threat Report 2014 states that 86% of tablets require a WiFi connection to access the internet, while three quarters of Smartphone users will use WiFi on their device on a day-to-

day basis. The truth is far more shocking. It's staggering to note that almost 90% of everyone surveyed have WiFi networks that are either completely open (29%) or where a standard password is given out (57%) [2]. security flaws with WiFi services is a very real issue, as evidenced by this recent article on Hotels in Ireland. Security services (X.800) for both connection less and connection oriented services were categorized into five types those are Authentication, Access Control, Data Confidentiality, Data Integrity and Non-repudiation. A Biometrics refers to metrics related to traits and human characteristics. Realistic authentication or Biometrics authentication is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under examination. Many researches has discussed the problem of AAA(Authentication, Authorization and Accounting) problem and came up with solution in terms of reduction of authentication time, security level improvements and more parameters have considered. A few mechanisms like BSPS and EBSPS were tried to minimize the above specified problem, but their security standards were limited to certain extent. Bio-cryptography refers to the application of cryptography on the biometric data for the user authentication of Wired or Wireless Networks [3]. It is important to guard the biometric samples of a person from illegal access because they are critical to one's identity.

This work discusses mainly on three important aspects. Initially Data Confidentiality which provides a highly secure data transmission over network. This problem can be reduced by encrypting the biometric images. This technique can be popularly called as Bio-cryptography. Next, Access Control can be handled effectively by adopting the both text based and Biometric based credentials. Finally Authentication predicament can be done exactly by double encryption of different security levels. Another important aspect of this paper is to design the new security levels with improved security.

This work comprise of: (1) a analysis and requirements of security for wireless LAN; (2) a novel Double Bio-cryptic Security-aware Packet Scheduling; and (4) a new performance integrating both security and performance; (5) a simulator where the DBSPS algorithm is developed and tested. The rest of this paper is structured as follows. Section 2 discusses previous works in the area of security level and its security improvement, Re-Stenography, Bio-Cryptography and ARAS. Section 3 describes the assumed system blueprint and architecture. In section 4, it is represented with the performance evaluation of proposed algorithm. Lastly, concluded the paper with future work discussed in Section 5.

## 2. RELATED WORK

User authentication is typically based on many factors. Nevertheless, the development of social engineering attacks and various malwares convert the user's PC in an untrusted device and thereby making user authentication vulnerable. Aude Plateux and his team made a successful attempt in providing the one-time authentication for electronic payment authentication and online banking [4]. In India AADHAR brought more popularity for the Biometric authentication. AADHAR is a unique Identification Proof for all Indians. This AADHAR card is issued by the Unique Identification Authority of India (UIDAI) [5]. Avala Ramesh and S.P. Setty worked on different edge detection technique which will be best suited for encryption of Biometric images. The analysis states that Canny Edge operator suits best for feature extraction for Biometric Images [6]. Sulakshana Bhariya et al. illustrated the significance of the bio-cryptography and discussed the Improving the Security of Image Encryption and Decryption [7]. Rajesh Duvvuru and Pradeep M implemented the concept of Re-Stenography on images, which resulted the strongest form of stenographic image [8].

Initially Xiao Qin et al. found the concept of Security level for the real-time Wireless Networks and they proposed Security aware Packet Scheduling (SPSS) algorithms with designated security to the different users. The SPSS results were compared with two standard algorithms namely MIN and MAX. The result clearly shows that SPSS performs better than rest of the algorithms with respect to Security Level (SL) and Guarantee Ratio (GR) [9]. Later Rajesh Duvvuru et al. extended the work of SPSS with specific constraint and certain specified SL for the better usage of SL and introduced Automated ASPS for the better utilization of network. Proper designations of SL's were resulted well in terms of Load-on-Network Switch (LNS). In ASPS, the SL designation avoided the confusion in assignment of SL dynamically. The results of ASPS were compared with the MIN, MAX and SPSS algorithms. The overall performance of ASPS performed better than all three algorithms [10]. But ASPS and SPSS were limited to the only Text based authentication.

Next, the Rajesh Duvvuru and team continued with the ASPS extension. The Text based authentication was strengthening by adding Bio-cryptic security level to it, which resulted in introducing BPS algorithm. But BPS mechanism comprises of Text, Thumb print and Iris three level Bio-cryptic security only. It means that three levels of ASPS plus Bio-cryptic security is equal to BPS [11]. The same team added two more SL for the BPS algorithm and improved the SL in WLAN. This change resulted in bringing EBSPS mechanism for the enhanced security [12].

Then many researchers have concentrated on the speedy authentication by using the Bio-cryptic security. But existing algorithms have concentrated with speedy authentication mechanism only, not improving any security [13][14][15]. Security levels were compared on different algorithms in detailed [16].

Presently the system for designed for the and simulated for different security levels using Double Bio-cryptic to strengthen the authentication in WLAN through Advanced Radius Server Authentication (ARSA) [10].

## 3. DOUBLE BIOCRYPTED SECURITY-AWARE PACKET SCHEDULING ALGORITHM (DBSPS)

### 3.1 Notations and Assumptions

Fixed numbers of security levels were assumed in DBSPS (only five levels of security were assumed). The network model contains some Source Wireless Node (SWN), Destination Wireless Node (DWN), ARAS and Network Switch (NS). Data is communicated through (NS) from SWN to DWN. Where the network data traffic between SWN and DWN is assumed using Random Probability Distribution (RPD) [10].

New security levels authentication data packets were assumed and designed. Request IP Address packet (RIA), Response Authentication Packet (RsA) and Response authentication status (RsAS) packets were inherited from previous works [9]. Whereas, Guarantee Ratio (GR) and Security Levels (SL) were assumed using Uniform probability distribution. The presumed architecture is best suited for research laboratories and highly confidential WLAN's. The rest of the newly designed packets and SL's are as follows.

#### 3.1.1 Request Double Authentication Packets (RDA)

Once the RsA packet receives from the ARAS, the SWN responds and act accordingly by sending different RDA packets. They are (1) Request Double Authentication packet for security level 1 (RDA1) (2) Request Double Authentication packet for security level 2 (RDA2) (3) Request Double Authentication packet for security level 3 (RDA3) (4) Request Double Authentication packet for security level 4 (RDA4) (5) Request Double Authentication packet for security level 5 (RDA5). The detailed novel RDA packets are described below:

- RDA1 is a tuple of three fields (1, Double-cryptic-text Password, ARASIP). 1 specifies security level 1 and cryptic password.
- RDA2 comprises a set of four fields (2, Double-cryptic-text Password, Double-cryptic thumb print, ARASIP). 2 specify security level 2 and double Bio-cryptic thumb print.
- RDA3 contains a record of five fields (3, Double-cryptic-text Password, Double-cryptic thumb print, Double-cryptic Iris, ARASIP). 3 specifies security level 3, double Bio-cryptic thumb print and double Bio-cryptic Iris.
- RDA4 contains a record of six fields (4, Double-cryptic-text Password, Double-cryptic thumb print, Double-cryptic Iris, Double-cryptic Palm print, ARASIP). 4 specifies security level 4, double Bio-cryptic thumb print, double Bio-cryptic Iris and double Bio-cryptic Palm print .
- RDA5 contains a record of seven fields (5, Double-cryptic-text Password, Double-cryptic thumb print, Double-cryptic Iris, Double-cryptic face, ARASIP). 5 specify security level 5, double Bio-cryptic thumb print, double Bio-cryptic Iris, double Bio-cryptic Palm print and Double-cryptic face.

ARASIP represents the address of Advanced Radius Authentication Server. This is a common field in the RDA packets.

Figure 1 explains the network architecture Admission Controller (ADC) for admitting packets into the NS, Security Level for incrementing and decrementing Security Levels (SLC) and Earliest Deadline First Scheduler (EDFS) for scheduling data packets. The details about architecture were explained well in the literature of Bio-cryptography [10]. But architecture is modified with the replacement of RqA packets with RDA packets.

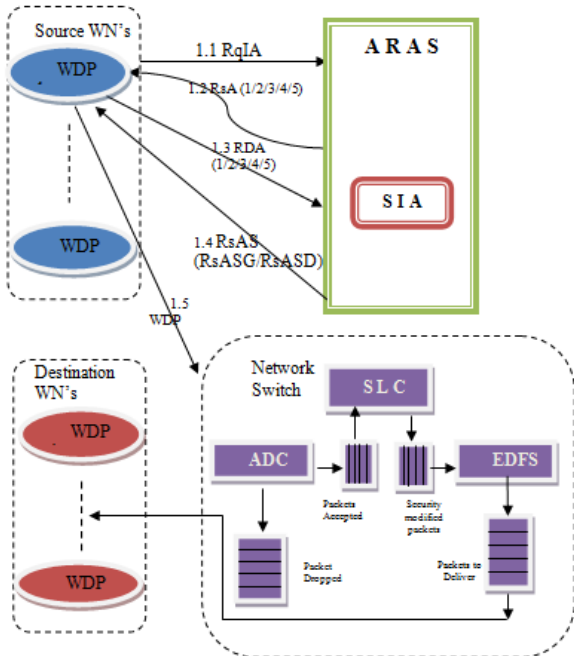


Figure 1: Schematic Diagram of Wireless LAN Model

### 3.2 The Blueprint of Wireless Data Packet

The Wireless data packet (WDP) standard model was inherited from the literature. The WDP comprises with a tuple of related attributes (AT<sub>i</sub>, PT<sub>i</sub>, SL<sub>i</sub>, Di)<sub>[9]</sub>. Where, AT<sub>i</sub> and PT<sub>i</sub> represents arrival time and processing time of packet i and SL<sub>i</sub> and Di is denoted as security level and deadline of the packet i.

Deadline (DL<sub>i</sub>) of ith packet can be calculated using Eq-1.

$$DL_i \geq IT_i - FT_i \quad -- (1)$$

Where IT and FT are WDP initial time and finished time of packet i. where i is a finite decimal number. Here network input network traffic to NS and output NS network traffic is taken using Random probability distribution.

The ARAS total authentication time is computed as

$$ARASTAT_i = ARASTRqAi + ARASTRsAi \quad -- (2)$$

Here ARASTRqAi is represented as Total requests time by the ARAS and ARASTRsAi is represented as Total response time by the ARAS. Equation-2 has discussed clearly in the previous works [12].

Thus, is the total authentication time (TAT<sub>i</sub>) is expressed in equation-3.

$$TAT_i = WNTAT_i + ARASTAT_i \quad -- (3)$$

### 3.3 Double Bio-cryptic algorithm (DBcA)

The DBcA protects the Biometric images from the security risks with double protection. Figure 2 illustration simulation procedure of the DBcA. This algorithm is used for incorporated in RDP packet according to the need and importance of the user. The algorithmic steps are as follows:

*Step1:* Read the Biometric sample image from human in SWN.

*Step2:* Apply the Canny edge detection on Biometric samples and extract the features and edges.

*Step3:* Encrypt the edge detected Biometric images using RSA algorithm using and save the image as E1.

*Step4:* Read the E1 image and apply Selective encryption algorithm on E1 and save it E2. Incorporating the resultant E2 image in to RDA packet.

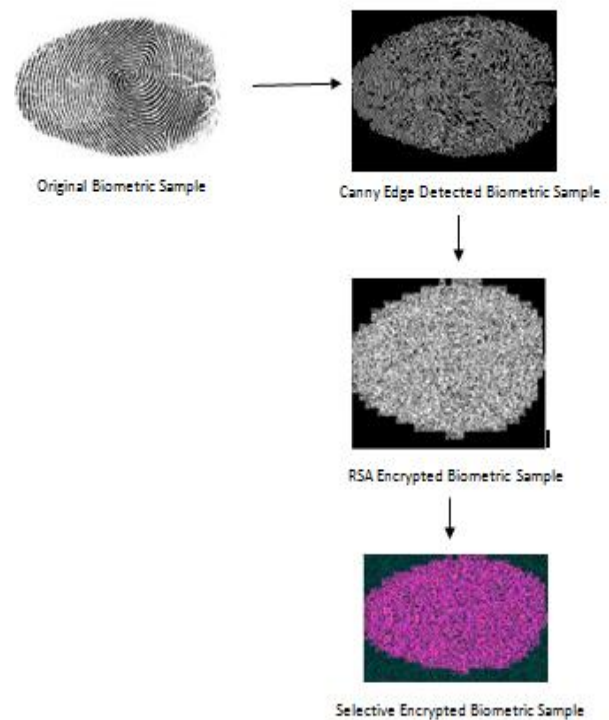


Figure 2: Simulation diagram of Double Bio-cryptic procedure

The biometric data was success fully encrypted with two algorithm that they specified above. Figure 2 explains it clearly the procedure of DBSPS.

### 3.4 The DBSPS algorithm

The DBSPS algorithm is a combination of DBcA and EBSPS algorithms. The algorithm can be described in the following steps.

Step 1: the node i sends RqP containing the IP address(IP<sub>i</sub>), requesting access for network to ARSA(Advanced Radius Server Authentication).

Step 2: ARSA selects an suitable security level and replies by RSP containing information about designated security level (SLi) and requesting for authentication data.

Step 3: The user's system on receiving RsP generates the respective RDA (1/2/3/4/5) packets for designated security level containing the required authentication data. RDA packets were incorporated with DBcA. These RDA packets are sent back to the network for the authentication.

Step4: The ARAS receives RDA packets and checks the credentials and issues RsAS packets accordingly.

Step5: IF RsASG, GOTO step 7 else GOTO step6. Step6 : User asked for re-verification of the credentials Step7: Follows the procedure of BSPS algorithm (From Step7 to 15).

## 4. SIMULATION OF DBSPS

### 4.1 Double Bio-Cryptography Simulations using Matlab

Double Bio-cryptography follows three important steps. Initially canny edge operator is applied for feature extraction on biometric images. Later the detected images are subjected for the image encryption with RSA and Selective encryption algorithms and lastly the images are combined together and incorporated in RDA. The simulations were performed on the IIT Delhi and IIT Delhi Biometric Research Laborites databases [17] [18] [19] [20].

#### 4.1.1 Feature Extraction of Biometric Images

Feature extraction operation is initial and very vital step for encryption of images. Especially this step plays a crucial role for Biometric images. In this we used Canny operator for edge detection. In this work, threshold value were not taken into consideration. For Matlab software an inbuilt function for the feature extraction using CED. i.e., `edge(fin_his_eq,'canny')`; is used.

#### 4.1.2 RSA Algorithm on Edge Detected Biometric Images

In first stage of encryption RSA algorithm is used for the protection of Biometric samples. In this algorithm two distinct prime numbers p and q considered, then computed the prime numbers p and q for the key generation. [11]. Given m, can recover the original message M by reversing the padding scheme. Where, C and D use the pre-computed values. In Matlab image tool kit we applied the above equation used i.e.  $cipher(j,k) = \text{mod}(M(j,k)^e, n)$ ; where M is the feature extracted biometric image. Using `imread()`, we read the image M ( Image is already stored in WN).

#### 4.1.3 Selective Encryption Algorithm on Edge Detected Biometric Images

In the second stage of encryption were applied on the RSA encrypted image and resultant image is considered as strong Bio-cryptic sample. In the implementation of Selective encryption three procedure calls were taken into considered, they are `hudungen()`, `Keygen()` and lastly `Selctive_encryption()`.

## 5. RESULTS AND DISCUSSIONS

### 5.1 Result and Analysis of Crypto-Biometrics

#### 5.1.1 Impact of Authentication Time at each Biometric Sample

Computation time of DBSPS is high when compared with the EBSPS. Even though computation time is high is the secured with the double encryption. Figure 3 shows this difference between DBSPS and EBSPS. The results clarify the computation time of DBSPS on an average 50% more than EBSPS. Figure 3 shows the comparison of DBSPS and EBSPS at security level-5. The Y-axis represents the encryption time and encryption at SWN and X-axis represents Biometric templates.

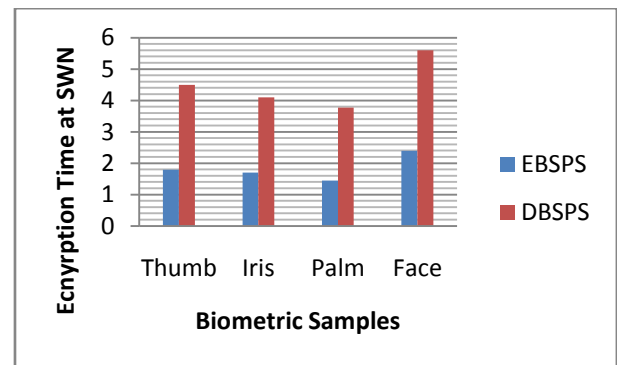


Figure 3: Authentication time at SWN of each Biometric sample

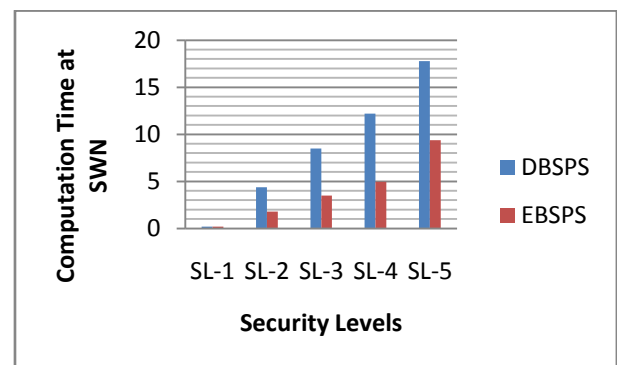


Figure 4: Computation time at SWN at each Security Levels

Figure 4 shows the comparison between DBSPS and EBSPS algorithm by considering computation at SWN at each security level. In this analysis the computation time of DBSPS will consume more time than EBSPS algorithm.

#### 5.1.2 Impact of Key Size on LNS

Load-on Network Switch is one of the important parameter that is considered. In Literature LNS explains that, if encrypted key size it reflects in increment in authentication packet size. This was a big load on Network switch. If LNS is more the performance of the network is poor. The encryption size of RSA algorithms is 1024 bits and whereas Selective encryption key size is 128 bits. Figure 4 show the key sizes of DBSPS and EBSPS algorithms. LOS is directly proportional to the SL. It is observed that, key size is similar in all the security levels. Figure 5 demonstrates the results analysis of key size at each security level. The key size of DBSPS is larger than EBSPS mechanism.

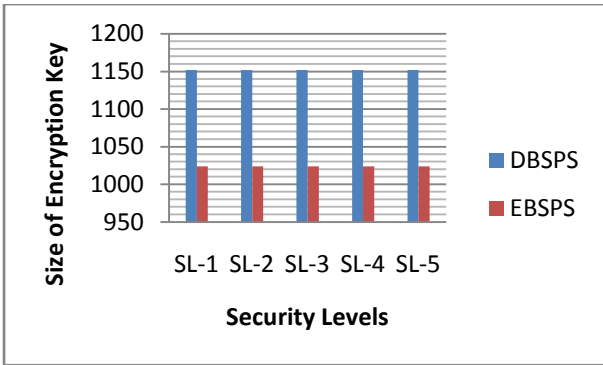


Figure 5: Comparison between DBSPS and EBSPS based on key size

### 5.2 Overall Performance

The overall performance of DBSPS is better than EBSPS because enhancement in the security level. The overall performance is articulated in our previous work [6].

Performance measurement is based on mainly five parameters they are Guarantee ratio (GR), level of security (LS), overall performance (OP), Load-on-Switch (LNS) and total

authentication time (TATi). Overall performance can be designed by following Eq-4:

$$OP = (GR * LS) + LNS + TATi \quad \text{-- (4)}$$

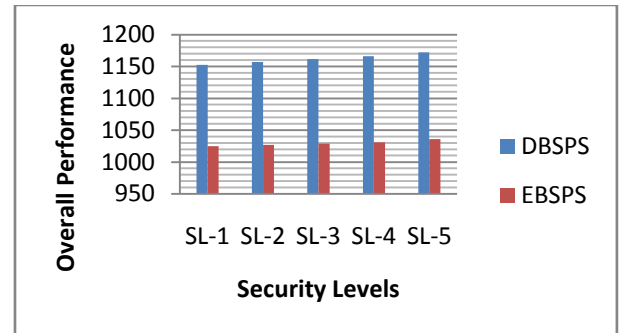


Figure 5: Overall Performance of DBSPS and EBSPS

Figure 5 illustrates a domination of DBSPS over EBSPS in terms of the overall performance. The simulation results prove that the overall performance of the proposed DBSPS is impressive. Figure 6 shows the simulation outcomes of DBSPS of each individual biometric template. In Figure the simulation packet of RDA5 Packet.

Table 1 Illustration of SL-5 using DBSPS algorithm


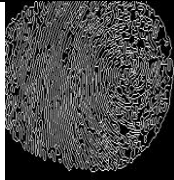
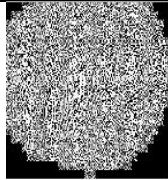
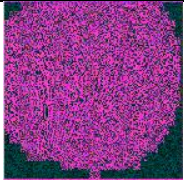
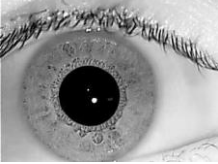
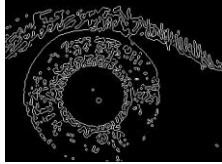
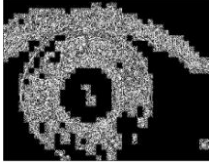
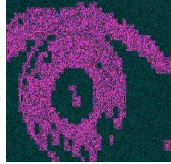
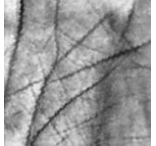


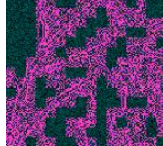



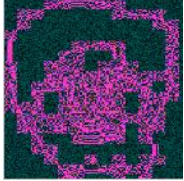

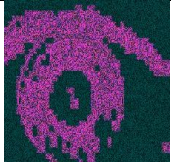

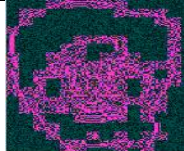
Name of the Sample	Biometric Sample/Text	Edge detection through Canny Operator	RSA Encryption	Selective Encryption
Thumb print				
Iris				
Palm print				
Face				

Table 2: Sample RDA5 Packet with simulation experiments

RDA5 Packet				
352 292 1 1 268 273 292 229 202				

## 6. CONCLUSIONS AND FUTURE SCOPE

Wireless networks play a vital role in the development of Information technology. In the proposed approach, it boosts the security in DBSPS by introducing the double bio-encrypted approaches, i.e. This work focused mainly on enrichment of security levels in Wireless LAN. In DBSPS authentication, every Biometric sample was re-encrypted with RSA and Selective encryption algorithms in order to strengthen the authentication process. Simulations were performed on different Biometric samples like thumb, Iris, palm and facial images using the MATLAB. The results of DBSPS were compared with the existing EBSPS. It is observed that, the SL levels are improved very strongly. But the limitation with the DBSPS consumes more time and it increases the burden on the Network Switch in terms of encryption and decryption of Biometric images. With this experiment, it is observed that, security is directly proportional to the total authentication time and the OP of the DBSPS is approximately 40 % improved compared to the EBSPS mechanism.

In future, the security may be enhanced by encryption using chaotic bio-encryption approaches.

## 7. ACKNOWLEDGMENTS

Our thanks to IJCA reviewers who have reviewed and suggested improvement of work. I also thank to our college SCET and SES for helping in the development of our project.

## 8. REFERENCES

- [1] Welch, Donald J., and Scott Lathrop. "A survey of 802.11 wireless security threats and security mechanisms." United States Military Academy West Point (2003).
- [2] <http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf>
- [3] Xi, Kai, and Jiankun Hu. "Bio-cryptography." Handbook of Information and Communication Security. Springer Berlin Heidelberg, 2010. 129-157.
- [4] Plateaux, Aude, et al. "One-Time Biometrics for Online Banking and Electronic Payment Authentication." Availability, Reliability, and Security in Information Systems. Springer International Publishing, 2014. 179-193.
- [5] <https://eaadhaar.uidai.gov.in/> (Accessed on 06/05/2014)
- [6] Ramesh, Avala, and S. Pallam Setty. "Analysis on biometric encryption using RSA algorithm." International Journal Multidisciplinary Educational and Research 1.3 (2013): 302-307.
- [7] Bhariya, Sulakshana. "Guide Jagveer," "A Bio-Cryptography Approach for Improving the Security of Image Encryption and Decryption," International Journal of Technology 2.1 (2012): 01-04.
- [8] Duvvuru, Rajesh, et al. "Performance Analysis of Multi-class Steganographic Methods Based on Multi-Level Re-steganography." ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol II. Springer International Publishing, 2014.
- [9] Xiao Qin, et, "Improving Security of Real-Time Wireless Networks Through Packet Scheduling," IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 7, NO. 9, pp.3273-3279, September 2008.
- [10] Rajesh Duvvuru, Sunil Kumar Singh, G. Narasimha Rao, Ashok Kote, B.Bala Krishna and M. Vijaya Raju, "Scheme for Assigning Security Automatically for Real-Time Wireless Nodes via ARSA," In Proc. Of QSHINE 2013, LNICST 115, Springer, pp. 185-196, January, 2013.
- [11] Rajesh Duvvuru, P. Jagadeeswara Rao and Sunil Kumar Singh, "Improving Security levels in WLAN via Novel BPS", In Proc. Of IEEE International conference on Emerging Trends in Communication, Control, Signal Processing & Computer Applications 2013(C2SPCA-2013), pp. 71, October 10-11, 2013
- [12] Duvvuru, Rajesh, et al. "Enhanced Security levels of BPS in WLAN." International Journal of Computer Applications 84.2 (2013): 33-39.
- [13] Ramesh, Avala, and S. Pallam Setty. "Enhanced Merged Security Levels of BPS in WLAN." International Journal of Computer Applications 88.7 (2014): 26-34.
- [14] Ramesh, Avala Ramesh and S. Pallam Setty. "Enhanced Authentication Mechanism in WLAN via MMBSPS", In Proc. of IEEE's International Conferences For Convergence Of Technology, Pune, India, pp, April, 2014.
- [15] Kumar, Sanjay. "Enhancing the Security Levels in WLAN via Novel IBSPS." Advanced Computing, Networking and Informatics-Volume 2. Springer International Publishing, 2014. 351-359.
- [16] Ramesh, Avala, and S. Pallam Setty. "A Comparative Study on Security Levels in WLAN." International Journal of Computer Applications 93 (2014).
- [17] Ajay Kumar, "Incorporating Cohort Information for Reliable Palmprint Authentication," Proc. ICVGIP, Bhubneshwar, India, pp. 583-590, Dec. 2008
- [18] Ajay Kumar, Sumit Shekhar, "Personal Identification using Rank-level Fusion," IEEE Trans. Systems, Man, and Cybernetics: Part C, pp. 743-752, vol. 41, no. 5, Sep. 2011.
- [19] D. Yadav, N. Kohli, R. Singh, and M. Vatsa, Revisiting Iris Recognition with Color Cosmetic Contact Lenses, 6th IAPR International Conference on Biometrics, June, 2013.
- [20] A. Sankaran, M. Vatsa, and R. Singh, Hierarchical Fusion for Matching Simultaneous Latent Fingerprint, In Proceedings of International Conference on Biometrics: Theory, Applications and Systems, 2012.