A Comparative Study on Security Levels in WLAN

Avala Ramesh
Dept. of Computer Sc. & Systems Engg.
Andhra University College of Engineering,
Andhra University,
Visakhapatnam, India

S. Pallam Setty
Dept. of Computer Sc. & Systems Engg.
Andhra University College of Engineering,
Andhra University,
Visakhapatnam, India

ABSTRACT
Security of wireless network is vital research area for the researchers and scientists. This work demonstrates a deep study of security levels in Wireless Local Area Networks (WLAN). This study includes different security schemes of WLAN like Security Aware Packet Scheduling Algorithm (SPSS), Automated Security-Aware Packet Scheduling (ASPS), Bio-cryptic Security-Aware Packet Scheduling (BSPS), Enhanced Bio-cryptic Security-Aware Packet Scheduling (EBSPS), Enhanced Merged Bio-cryptic Security-Aware Packet Scheduling (EMBSPS) and Multi Merged Bio-cryptic Security-Aware Packet Scheduling (MMBSPS). To analyze the performance of the each algorithm some simulations were conducted by considering different parameters like Security Level (SL), size of Wireless Data Packet (WDP), Speedy Authentication (SA) and Load- on-network Switch (LOS). The simulations were performed using Matlab and Network Simulator-2. Finally our experiment result concludes that, each algorithm has got its own advantages and limitations.

General Terms
Wireless communications and Security.

Keywords
Bio-Cryptography, Quality-of-Security, ASPS, SPSS, Biometrics, Security Level, Enhanced Merged Bio-cryptic Security- Aware Packet Scheduling-Algorithm, Bio-cryptic Security-Aware Packet Scheduling-Algorithm, BSPS, EBSPS,MMBSPS.

1. INTRODUCTION
Network Security is a branch of science which deals with providing the security to the network using Cryptography or Stenography. When Cryptography is compared with the stenography, cryptography techniques are more efficient than stenography [1]. Cryptography comprises of the encryption and decryption of digital bits. The encryption and decryption will be based on cryptic-key. Key comprises of set of digital bits, where key size was fixed. In general, there are two type of keys available in literature, namely Public key and Private key [2]. There are many successful algorithms that were available in cryptography like, Advanced Encryption (AES), RSA algorithm, Digital Signatures etc., [3]. In addition to this there are many more authentication mechanisms that are available in cryptography; they are Authentication Tokens, Certificate-based Authentication, Biometric Authentication, Kerberos, Key distribution center, Single Sign On approaches and many more [4].

This work concentrates majorly on the user strengthening the user authentication process in WLAN. There are certain attacks that are existing in the literature of Network security. There are certain attacks like session hijacking, person-in-the-middle attacks, replay attacks etc,. are causing great damage to the network, for which the data is going to be misused [5]. To reduce these sorts of attacks many scholars, has came up with their solutions [6, 7, 8]. Even in literature there are many solution exists, still authentication mechanisms are weak.

To enhance the authentication mechanism in WLAN, we came up with the better solution using bio-cryptography process [9, 10]. To strengthen the security mechanisms, this work as adopted the security levels in WLAN [11]. This work summarizes the usage of security levels in WLAN using text and biometric based authentication schemes. In biometric based encryptions, we need to frisnt find the edges of the biometric image and later it should be encrypted with an cryptography algorithm. In our previous works, we experimented with deiferent edge detection techniques; finally we concluded Canny operator performs better than Laplacian and Zero cross edge technique for stronger encryption [12].

The significant contributions of this work comprises of: (1) study and analysis Security levels in the wireless LAN's; (2) Discussion on innovative security level approaches (3) a new results of data packet transmission and performance; (4) a simulator where the SPSS, ASPS, BSPS, EBSPS, EMBSPS, EMBSPS and MMBSPS algorithms is implemented and evaluated.

The rest of the paper is structured are as follows: Section 2 discusses previous works in the area of Security Levels in WLAN. Section 3 describes the network system prototype and architecture. In section 4, it is represented with the performance metrics of algorithms. Finally, it is concluded the paper with future work discussed in Section 5.

2. RELATED WORKS
This chapter discusses the background works that is related to the SL in WLAN. Totally we have considered the six SL designed algorithms in our study.

2.1 Overview of WLAN Security Level Algorithms

2.1.1 Security-Aware Packet Scheduling Algorithm (SPSS)
Xiao Qin etl., has introduced the concept of security level [13]. They assumed and designed a network model, comprise of Source WN's, Destination WN's and an Network Switch (NS). NS contains, Admission Controller (ADC), Security Level Controller (SLC), Accepted Queue, Rejected Queue and Earliest Deadline Fisrt Scheduler. The brief descriptions are as follows:

- Source Nodes: It will sends the WDP to the Destination Nodes

- Admission Controller: It admits the WDP and checks, whether the packets has reached before its deadline. If the packet reaches before deadline, it will be forwarded to SLC, else the packets are sent for the rejected Queue.
- Security Level Controller: Once WDP arrives from ADC, depending upon the bandwidth available from NS to DN's. If the bandwidth is high, the security level will be increased otherwise, the SL is decreased.
- EDFS: This scheduler is especially used in the Real Time Systems. It is used to desing the deadlines for the WDP's.
- Destination WN: Once the WDP's are filtered and improved security packets are delivered at he Destination Nodes.

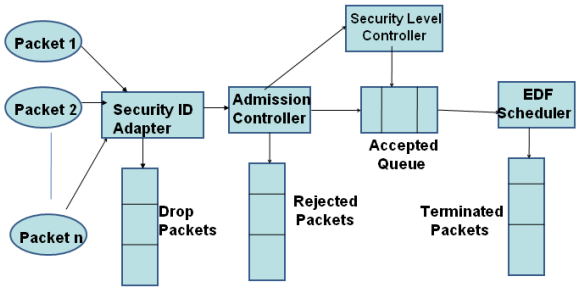

Figure 1: Architecture for SPSS algorithms [13].

2.1.2 *Advanced Security-Aware Packet Scheduling Algorithm (ASPS)*

Later Rajesh Duvvuru etl. has adopted the security levels from the 2.1.1 work [14]. In this work, they discussed the strengthening authentication mechanisms in WLAN. In SPSS, there is a problem that exists, in the form of, Security Level allocations to the specified to the each and every user. But these allocations was resolved by designed a novel Authentication server and named its as Advanced Radius authentication server (ARAS) and SL are assigned automatically. The ARAS is an extension to the CISCO's Radius Authentication Server. It will assign security level to the each and every WN depending up on Device Identification Number (DID). Due to proper allocation of the SL's reflects in the best utilization of the Load-on-Network Switch (LOS). If the allocation wasn't right, there will be chance of misuse of security level. A normal WN user, who don't require highest level of security. Suppose if he/her opted for the highest level of security, which may hamper network performance.

2.1.3 *Bio-cryptic Security-Aware Packet Scheduling Algorithm (BSPS)*

Once again Rajesh Duvvuru and team introduced the Bio-cryptography in Security Levels [11]. In addition to the text they considered the biometrics also for the authentication of users to access WLAN. They introduced the three level of security. The allocation of security levels will be made by ARAS system. The security levels are specified as follows:

- Security Level1: Only Encrypted Text with RSA Algorithm.
- Security Level 2: Combination of Text as well as Finger print. Encrypted using RSA Algorithm.
- Security Level 3: Here one more level of security was added to the SL-2 in the form of Iris. The same encryption procedure has followed.

2.1.4 *Enhanced Bio-cryptic Security-Aware Packet Scheduling Algorithm (EBSPS)*

This was an extension to the BSPS algorithm. Rajesh Duvvuru etl. has inherited the ASPS architecture and bio-cryptic security levels from the previous works [11, 14]. Here Totally five security levels were presented by the authors, in addition to existing work they added the two more level of security in the type of Palm, and Facial biometric authentication. The same procedure was adopted in this work for encrypting the Biometric images for WLAN authentication. In this architecture also ARAS plays a crucial role [15]. In addition the previous work security level, the rest security levels are as follows:

- Security Level-4 : It is combination of Text, Finger print, Iris and Palm print which was encrypted using RSA Algorithm
- Security Level-5: This is the last level of security that was designed, it contains simple Text, Finger print, Iris, Palm print and Face biometric images, these are also encrypted using RSA algorithm.

2.1.5 *Enhanced Merged Bio-cryptic Security-Aware Packet Scheduling Algorithm (EMBSPS)*

In the previous works, it is found that, there was great loss of bandwidth and authentication time [9]. To improve the performance of BSPS and EBSPS, we introduced the merged bio-encryption for the WLAN security. We have innate the same architecture of EBSPS, with slight modification. The updated information's to the architecture are as follows:

- Two biometric images are considered. For instance, those images are thumb print and Iris. These images segmented into two equal halves and later the left portion of thumb print is merged with the right portion of Iris image.
- Once the image was merged, later the resultant image was subjected for edge detections.
- Next the encryption procedure is applied on the edged detected biometric images using RSA algorithm. Finally we observed a new merged bio-cryptic image.

Moreover, the merged procedure has totally changed the scenario of Security levels. The newly designed security levels are as pursues:

- Security Level 1: A simple cryptic text password.
- Security Level 2: It is similar the SL-2 of BSPS and EBSPS. It comprises of cryptic text password and cryptic thumb print.
- Security Level 3: This is a novel SL. Here, the biometric images are merged. In this SL, it contains cryptic text password and merged biometric image of thumb and iris which was encrypted with RSA algorithm.
- Security Level 4: This is also a newly designed SL. In addition to the above SL-3, it was added with the bio-cryptic palm print. SL-4 includes text, merged

thumb-iris and palm print which were encrypted with the same encryption algorithm.

- Security level 5: This is the last level of security that is designed. It comprises of text password, merged biometric images of thumb-iris and merged biometric images of Palm-Face.

2.1.6 Multi Merged Bio-cryptic Security-Aware Packet Scheduling Algorithm (MMBSPS)

In the preceding work, we achieved, good amount of packet size reduction due we utilized the bandwidth. MMBSPS gave the better results in terms of WDP size reduction. MMBSPS has adapted the procedure of EMBSPS with a bit slight variation, especially in the segmentation process of Biometric images. In EMBSPS, we have segmented the biometric image in to two equal halves, whereas in MMBSPS- the biometric image was spitted into the three vertically equal segments. The middle portion of each image is merged with the middle portion of another biometric image. In MMBSPS, one-third of image size is going to be considered, which will reflect in the biometric overall image size reduction. Most importantly, we also reduced the encryption time of data packet by modifying the Security Levels.

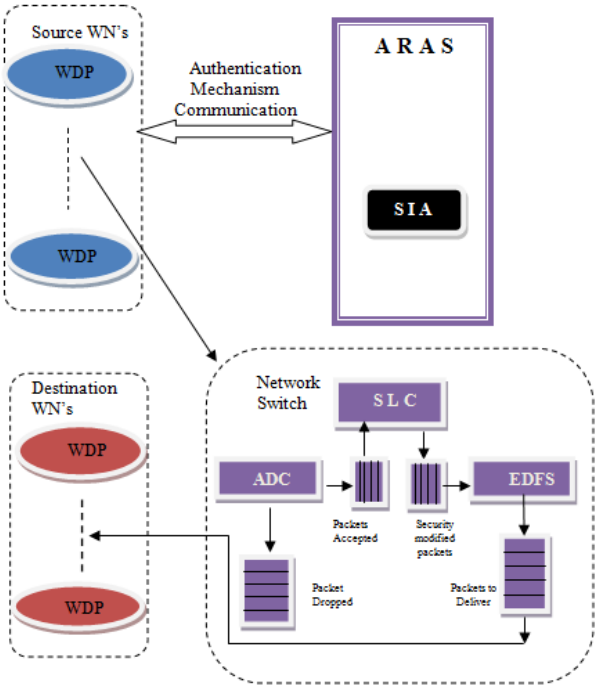

Figure 2: Generalized architecture for ASPS, BSPS, EBSPS, EMBSPS and MMBSPS algorithms.

The newly proposed SL as shown below:

- Security Level 1: Cryptic Text Password.
- Security Level 2: Cryptic Text and Thumb.
- Security Level 3: Cryptic Text and merged Thumb-Iris.
- Security Level 4: Cryptic Text and merged Thumb-Iris-Palm.
- Security Level 5: Cryptic Text and merged Thumb-Iris-Palm-Face.

All text passwords and merged images are encrypted using the RSA Algorithm [10].

3. SIMULATION SETUP

To simulate all the above experiments, we have used, the Java applets, Matlab 7 and NS-2. Initially we have done simulations using Matlab tool. Biometric images were taken for secure encryption. To encrypt the biometric images, we followed the procedure that was describes in the following works [Ref 9-15]. Where, the parameter speedy authentication was evaluated and tested. In NS-2 environment, we have we used the ten WN, NS node and ARAS node. Delay was introduced in each and every node. Delay was considered from encryption and decryption process of biometric images. We assumed packet drop in the network in the using Random probability distribution. Table 1 and 2 denotes the variables and their values for running simulations.

Table 1. NS-2 simulation parameters and values

Parameters	Values
Security Level Models	SPSS, ASPS, BSPS, EBSPS, EMBSPS and MMBSPS
Delay at WN	0.2 to 2 (sec)
Delay at ARAS	1.2 to 1.9 (sec)
Packet drop inside the network	Drop Tail
Packet Delivery Ratio	Poisson's Distribution
Traffic type	CBR
Maximum Speed	20 m/s
Minimum Speed	10 m/s
Transmission protocol	UDP
Transmission Range	600 m
Simulation time	1000sec.

Table 2. Matlab simulation parameters and values

Parameters	Values
Security Level Models	SPSS, ASPS, BSPS, EBSPS, EMBSPS and MMBSPS
Security Level	Ranges from 1 to 5
Speedy Authentication Time	Ranges from 1.8 to 3(sec)
Load-on-network Switch	Depends upon the Security Level.
Bio-cryptic Image Size	Depends on the edges detected pixel resolution
Size of the Authentication Packet	Varies from 255 KB to 294 KB
Encryption Time at WN	Ranges from 0.1 to 1.5 (sec)

4. PERFOMANCE METRICS

4.1 Packet Deadline

Packet deadline was one of the important consideration in the packet scheduling of the architecture. If the packet is not going to reach with in a particular time, those packet are not allowed to access the NS assuming that, some security attack was happen on that packets. These sort of packets are kept in

the rejected queue. Deadline differs from packet to packet. Deadline can be articulated as follows:

$$Di >= ITi – ETi \quad (1)$$

Where Di is the deadline of the packet I, ITi is the initial time and ETi is the ended time.

4.2 Impact of Security Level

Major portion of this work depends on the security levels in the WLAN. Security level operation cost can be derived as follows:

$$SLCi=TTi*(SLi/HS) \quad (2)$$

Where SLCi represents security operating cost of the ith packet, TTi is the transmission time of the packet i, SLi is the level of security of the packet i, and HS is the highest security level ranges from 1 to 5 according to the classes in the IP address.

4.3 Impact of Load-on-Network Switch

Load on network is also one of the important parameter for evaluating the performance of the system. Where, Security Level is directly proportional to the Load-on-Network Switch (LOS). Thus LOS can be derived as:

$$LOSi= (SLi/HS) \quad (3)$$

4.4 Impact of Authentication Packet Size

The impact of Authentication Packet Size (APS) will be more on throughput of the system. If the packet is more, obviously the packet delivery time is proportionately increases. Authenticate packet size can be articulated as follows:

$$APS= Sizeof (Encrypted \{Text,Biometric\text{-}1\ldots5\}) \quad (4)$$

4.5 Impact of Computation Time

Encryption time plays a vital job in the Encryption of biometric images through RSA algorithm. Encryption time of whole text and biometric credentials can be acquired through eq 5. Encryption time can also call as Computation time (CT).

$$TATi = CTWNi + CTARASi + AD \quad (5)$$

Where, AD is the authentication delay in the network, CTWNi and CTARASi represents computation time at Wirless Nodes and Advanced Radius Authentication Server . Here AD assumed using Radom probability distribution function.

4.6 Overall Performance

The overall performance of the each algorithm can be articulated in equation 6.

$$OPi = TATi + LNS + (SL * GR) \quad (6)$$

Where, OP represents Overall Performance of the network system and GR represents the guarantee ratio of the WDP.

5. RESULTS AND DISCUSSIONS

In this section the simulation results are summarized. The results are shown in the form of graphs and tables.

5.1 Analysis of Total Authentication Time of Security Levels

In this analysis, we have summarized computation times of MMBSPS, EMBSPS, EBSPS, BSPS, ASPS and SPSS. It is observed that, the computation of ASPS taking more time than SPSS due to ARAS and moreover computation times of these two algorithms are very less competitively to others. Here point to be noted that, both ASPS and SPSS are not Bio-cryptography algorithms. Even the computation time is very little, but weak in terms of security. Also, it is observed all the algorithms are performing similarly at SL1, due to text based encryption. Coming to the Bio-cryptic algorithms, MMBSPS computation time is very less comparatively EMBSPS, EBSPS and BSPS due to Triple merged algorithm. In addition to this it was observed that, the computation time of EMBSPS is less than EBSPS and BSPS due to the Equally Merged algorithm and EBSPS computation time is almost equal unto security level 3. EBSPS encryption time at SL-4 and SL-5 is more, when it is compared to BSPS. But, pointed to be noted is BSPS has only two biometric credentials. The detail chart, was shown in Table 3. Figure 3 shows the graphical representation of the TAT of Security Level Algorithms.

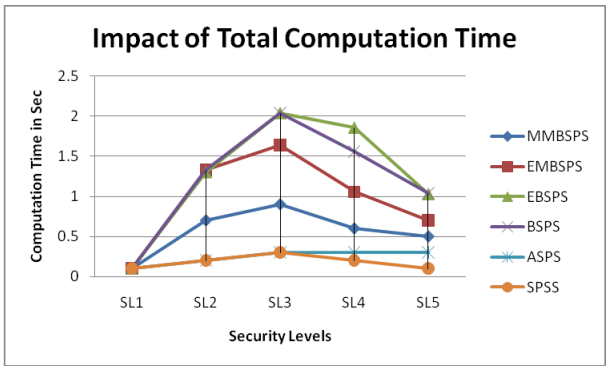

Figure 3: Impact of Total Authentication Time at different Security Levels.

5.2 Analysis on Load-on-Network Switch

The LNS is also one of the important parameter for the SL. Except SPSS, the rest of the algorithms authentication process is monitored by the Advanced radius authentication server. So, SPSS may have LNS high compared to the rest in some cases. LNS depend up on the encryption algorithm of the data packet.

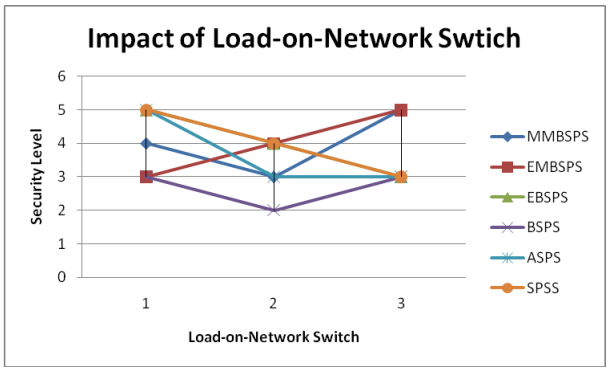

Figure 4: Impact of Load-on-Network Switch of Security Levels when data size = 512 bytes, Bandwidth = 3 MBPS, and deadline = 0.5 No/Sec.

Figure No. 4 shows impact of LNS on SL and Table 3 shows the ARAS based algorithms.

Table 3. ARAS dependent independent algorithms

Non-ARAS	ARAS
SPSS	ASPS, MMBSPS, EMBSPS, EBSPS and BSPS

5.3 Analysis on Size of Authentication Packet

Authentication Packet Size (APS) makes difference in terms of speedy authentication. Size of the authentication packet is partially dependent on the security level. In SPSS, ASPS, BSPS and EMBSPS algorithms authentication packet size is directly proportional to the SL. Whereas EMBSPS and MMBSPS it is not dependent on the SL and in addition they rely upon the image merging and edge detection. Figure No. 4 shows the Authentication packet size and its impact at different levels. Figure 5 shows clearly authentication analysis on SL if different SL algorithms.

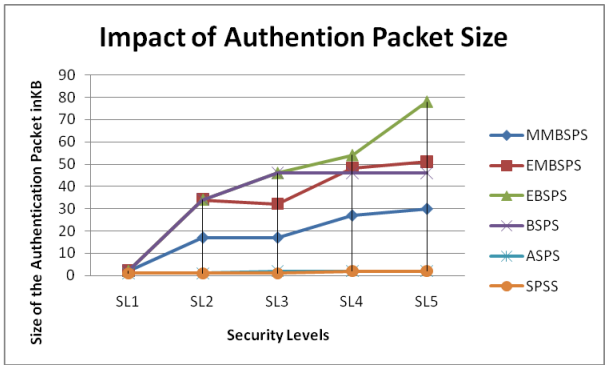

Figure 5: Impact of Authentication Packet Size at different Security Levels

5.4 Analysis on Overall Performance

As it was discussed in the earlier section, OP is important parameter and it is combination of SL, LNS, TAT and GR. In our simulation GR was assumed using Possions distribution. We have shown, three graphical performances based up on the similarities based on Bio-cryptography and ARAS among algorithms. Figure 6 shows the throughput comparison between MMBSPS, EMBSPS and EBSPS. The overall performance of the MMBSPS algorithm is better than EMBSPS and EBSPS algorithms at Security Level-5. On an average EMBSPS performance is 9% better than EMBSPS and 20 % better than EBSPS. In Figure 7 displays the performance of the MMBSPS, EMBSPS, EBSPS and BSPS algorithm when Security Level is three. At this stage also EMBSPS, EMBSPS, EBSPS achieve 40% better than BSPS in terms of security levels and approximate 20 % to 25% the overall performance is lesser than rest of the algorithms. Lastly, in figure no. 8 states the overall performance of all six algorithms at SL-1. In this level, only text was encrypted and the performance of SPSS is good due to less delay in the authentication mechanism. In general security level assignment is not done in SPSS by ARAS. Whenever the security level assignment was done by ARAS, in general there will be additional delay in authentication. In every graph through were calculated in terms of seconds. Throughput is inversely proportional to delay of the network.

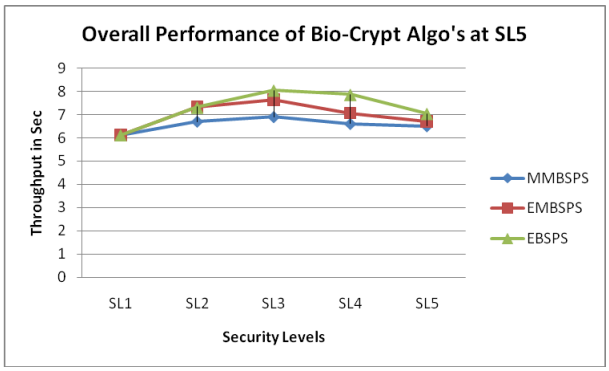

Figure 6: Impact of Overall Performance of Bio-cryptic algorithms at Security Level-5 when data size = 512 bytes, Bandwidth = 3 MBPS, and deadline = 0.5 No/Sec.

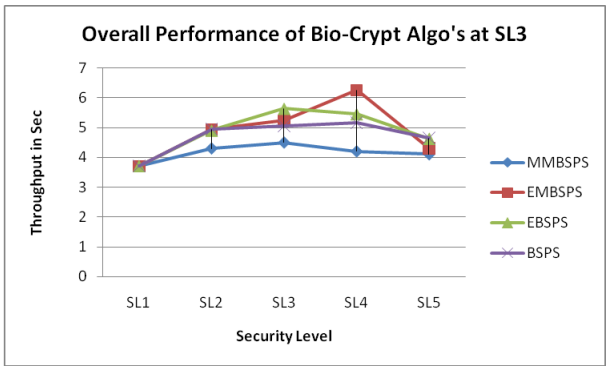

Figure 7: Impact of Overall Performance of Bio-cryptic algorithms at Security Level-3 when data size = 512 bytes, Bandwidth = 3 MBPS, and deadline = 0.5 No/Sec.

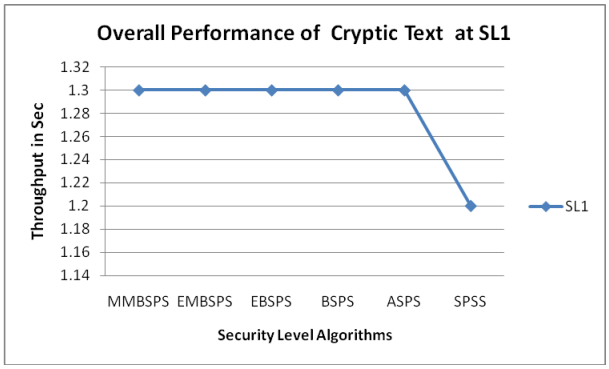

Figure 8: Impact of Overall Performance of SL algorithms at Security Level-1 when data size = 512 bytes, Bandwidth = 3 MBPS, and deadline = 0.5 No/Sec.

6. CONCLUSIONS

WLAN Security is major factor that are need to be considered for secure data exchange. Especially, the authentication mechanism plays an important role in access network scientific and research laborites. In this work, a analysis were made on the secure access to the WLAN's particularly, authentication scheme using different algorithms like SPSS, ASPS, BSPS, EBSPS, EMBSPS and MMBSPS. The algorithms are compared each other by considering diverse parameters like Authentication Time, Load-on-Network Switch and APS. It is observed that, SPSS, ASPS Authentication Time is less than BSPS, EBSPS, EMBSPS and MMBSPS. The details were clearly shown in figure 3. Next, LNS was discussed, if the LNS is high, the through will be low. LNS may be more for some cases in SPSS, the rest of

algorithmic performance is approximately similar to each other due to ARAS. The size of the Authentication packet plays a crucial role for speedy authentication. The size of the authentication packet hampers the overall network performance. If the size of the packet is more, the data transmission time is obviously increases. The APS of SPSS, ASPS is same, but those algorithms are week authentication mechanisms. Whereas Comparatively BSPS Authentication Packet Size is good, but maximum security level is three only. Overall the Authentication packet size and security aspect of MMBSPS is performing better rest of the algorithms.

In future, more algorithms and more parameters are needed to be considered for better study on authentication mechanism. Also stronger encryption mechanism has to be used for stronger security like ECC and Chos-Based [16,17].

7. REFERENCES

[1] Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt. "Digital image steganography: Survey and analysis of current methods." *Signal Processing* 90, no. 3 (2010): 727-752.

[2] Rivest, Ronald L., Adi Shamir, and Len Adleman. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM* 21.2 (1978): 120-126.

[3] William, Stallings, and William Stallings. *Cryptography and Network Security, 4/E*. Pearson Education India, 2006.

[4] Hardt, Dick C. "Distributed hierarchical identity management system authentication mechanisms." U.S. Patent No. 7,454,623. 18 Nov. 2008.

[5] Wu, Bing, et al. "A survey of attacks and countermeasures in mobile ad hoc networks." *Wireless Network Security*. Springer US, 2007. 103-135.

[6] Krawczyk, Hugo, Ran Canetti, and Mihir Bellare. "HMAC: Keyed-hashing for message authentication." (1997).

[7] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Packet leashes: a defense against wormhole attacks in wireless networks." *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*. Vol. 3. IEEE, 2003.

[8] Bellardo, John, and Stefan Savage. "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions." *Proceedings of the USENIX Security Symposium*. 2003.

[9] Avala Ramesh and S. Pallam Setty. "Enhanced Merged Security Levels of BSPS in WLAN." *International Journal of Computer Applications* 88 (2014).

[10] Avala Ramesh and S. Pallam Setty. "Enhanced Authntication Mechanism in WLAN via MMBSPS", In Proc. of IEEE's International Conferences For Convergence Of Technology, Pune,India, pp., April, 2014.

[11] Rajesh Duvvuru, P. Jagadeeswara Rao and Sunil Kumar Singh, "Improvizing Security levels in WLAN via Novel BSPS", 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] Avala Ramesh and S. Pallem Setty, "Analyis on biometric encryption using RSA algorithm," Published In the International Journal Multidiciplnery Educational and Research, Volume 1 – Issue Number 3, pp. 33-39, October 2013.

[13] 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.

[14] 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.

[15] Rajesh Duvvuru, P. Jagadeeswara Rao, Sunil Kumar Singh and Ankita Sinha, "Enhanced Security levels of BSPS in WLAN", Published In the International Journal of Computer Applications, Volume 84 - Number 2, pp. 33-39, December 2013.

[16] Zhongjian Zhao and Xiaoqiang Zhang. "ECC-Based Image Encryption Using Code Computing.." Proceedings of the 2012 International Conference on Communication, Electronics and Automation Engineering Advances in Intelligent Systems and Computing, Volume 181, Springer, pp 859-865, 2013

[17] Yaobin Mao and Guanrong Chen. "Chaos-Based Image Encryption." Applications in Pattern Recognition, Computer Vision, Neuralcomputing, and Robotics, Springer, pp 231-265, 2005.

Table 3. Security Level Comparisons

	SL1	SL2	SL3	SL4	SL5
SPSS	Text	Text	Text	Text	Text
ASPS	Text	Text	Text	Text	Text
BSPS	Text	Text +Thumb	Text + Thumb + Iris	Text + Thumb + Iris	Text + Thumb + Iris
EBSPS	Text	Text +Thumb	Text + Thumb + Iris	Text + Thumb + Iris +Palm print	Text + Thumb + Iris +Palm print + Face
EMBSPS	Text	Text +Thumb	Text + Merge (Thumb,Iris)	Text + Merge (Thumb,Iris) + Palm print	Text + Merge (Thumb,Iris) + Merge (Palm print ,Face)
MMBSPS	Text	Text +Thumb	Text + Merge (Thumb,Iris)	Text + Merge (Thumb,Iris Palm print)	Text + Merge (Thumb, Iris, Palm print ,Face)