iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5014

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Secure and Energy-Efficient Data Transmission System Based on Chaotic Compressive Sensing in Body-to-Body Networks

Ananda Krishnan[1], Richard Amalraj[2], Mohan Raj, Dr. B. Muthukumar[3]
[1, 2, 3]*Department of Computer Science and Engineering Kalasalingam Academy of Research and Education*

Abstract: ***The usage of wireless networks is increasing day by day. They are used for communication purposes. But as time has gone they are used a lot as wireless body area networks which have a different purpose such as in the military and health related areas. They are known as WBAN's, which we will be focusing on as there are ways to conserve and save energy while using the features of the WBAN. In order to do so we adapt the method of chaotic compressive sensing which will help saving energy and also assist us with data security issues. It is referred to as CCS, which is primarily used to save vast storage space and also the sensitivity of the CCS can improve the security aspects. There are a couple of mechanism that will help with the security in data transmission such as better encryption quality. Lots of results show that when space is saved the overall performance of the WBAN improved. We will be looking at this is detail in the sections below.***
Keywords: Body to body network, chaotic compression. Energy efficient and secure.

I. INTRODUCTION

In the case of Wireless body area networks there are several sensors involved. They are usually found in the body via implants. These are used mainly for medical purposes for monitoring heart rate or psychological changes in a person. Nowadays the concept of sensors in the body has drastically changed. They can be worn in the form of a watch in order to check the number of calories that are spent in a day. They can be used to check a lot of other features that can be tracked in our smartphones. Doctors can also use WBAN's to potentially discover any possible health complication even before they become major. Also, data can be collected over time which can be used for further research. There are terminals that are the mediums of communication such as phone and laptop computers. All of this can be stored in one common database and can be used even for basic treatment purposes. There are many projects based on WBAN's for health care. Not only can it be used for regular treatment it can be used for real time scenario's.

There is short coming with the sensors as only a few of them can be used on a human body. They have limited bandwidth and cannot be transmitted over long distance. The research

here mainly focusses on health care. The other issue here is the power consumption. This can also be handled with a few resources. Not only for medical treatment, BBN's can be used for entertainment purposes. It can collect any kind of information and store it and use or for further purposes.

The transmission distance in WBAN's is very limited so the only way to make them reliable is to make them rely on infrastructure networks

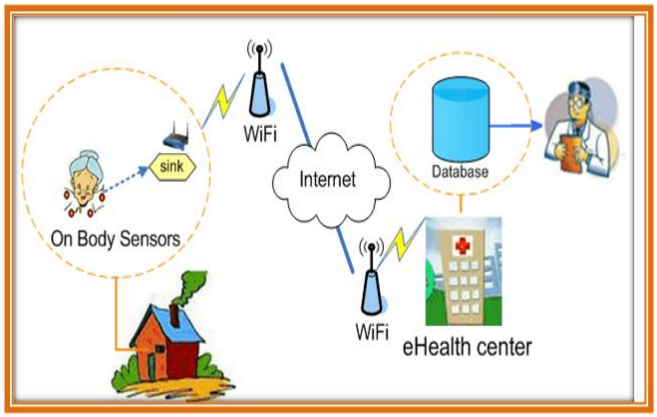


Fig 1. Architecture of WBAN

On a comparison with WBAN, the network scale of BBN is more, but the sensors here have to do twice the work. Due to that very reason we see what can be done with both the instances.

The energy consumption is very heavy and the placement of some sensors is very difficult. Energy harvesting methods has been proposed. In the case of BBN further energy is consumed. An energy efficient MAC protocol is the best way to approach it. It is used for medical emergency monitoring. Power optimization is very important considering we need them to work accurately and efficiently. There is an algorithm in place for this to be fixed.

Next part is the security of data in BBN. They are very important data and cannot be risked being stolen or lost. So, an efficient security standard must be in place for the data to be safe. The solution is to encrypt all the layer in the network. WBAN has several security solutions. There should always be authentication and integrity of data must be maintained. There are also other sources that can resist security threats from external sources.

In the case of BBN both the problems can be handled up to some extent. But then it cannot be perfect. BBN is more power efficient but not that safe in terms of security. But with the help of CS which is chaotic compression both encryption and the power efficiency can be handled. However, the number of nodes in the BBN is very large.

II. SYSTEM STUDY

A. Feasibility

Every project is feasible provided given unlimited resources and infinite time. Unfortunately, the development of a computer-based system is more likely to be plagued by resource scarcity and stringent schedules. It is both necessary and prudent to evaluate the feasibility of a project at earliest possible time. Wastage of miniport and financial resources and untold professional embarrassment can be avoided if an ill-conceived system is recognized early in the development phase. So, a detailed study was carried out to check the workability of the proposed system.

Feasibility study is a test of system proposal regarding its workability, impact on the organization, ability to meet user needs and effective use of resources. Thus, when an application is proposed, it is normally going through a feasibility study before it is approved for development.

Feasibility and risk analysis is related in many ways. If project risk is great, the feasibility of producing quality is reduced. Thus, during feasibility analysis for this project, following three primary areas for interest was considered very carefully. There are several types of feasibility.

Three Key Consideration involved in the feasibility analysis are:

B. Economic Feasibility

The purpose of the economic feasibility assessment is to determine the positive economic benefits to the organization that the proposed system will provide. It includes quantification and identification. An evaluation of development cost lighted against the ultimate income or benefit derived from the proposed system. The proposed system will not cause any expenditure since all the requirements are available in the firm.

C. Technical Feasibility

A study of resource availability that may affect the ability to achieve an acceptable system. Technical feasibility is the most difficult area to ensure at initial stage. Since te objectives, functions, performance cannot be predicted to its fullest, everything seems possible, provided the right assumptions are made.

It is essential that the process of analysis and definition can be conducted in parallel with an assessment of technical feasibility. The consideration that is normally associated with technical feasibility includes resource availability at the organization where the project is to be developed and implemented. This assessment is based on an outline design of system requirements, to determine whether the company has the technical expertise to handle completion of the project. When writing a feasibility report, the following should be taken to consideration:

1) A brief description of the business to assess more possible factors which could affect the study
2) The part of the business being examined
3) The human and economic factor
4) The possible solutions to the problem

At this level, the concern is whether the proposal is both technically and legally feasible (assuming moderate cost). The technical feasibility assessment is focused on gaining an understanding of the present technical resources of the organization and their

applicability to the expected needs of the proposed system. It is an evaluation of the hardware and software and how it meets the need of the proposed system.

D. Social Feasibility

Social feasibility addresses the influences that a proposed project may have on the social system in the project environment. The ambient social structure may be such that certain categories of workers may be in short supply or nonexistent. The effect of the project on the social status of the project participants must be assessed to ensure compatibility. It should be recognized that workers in certain industries may have certain status symbols within the society.

III. MODULES

A frequency domain sparsity signal and an image Lena is used in the experiment. The frequency domain sparsity signal is generated by Matlab, the image Lena is widely used in previous works. Three chaotic maps, i.e. Chebyshev, Logistic, Tent, are used to generate measurement matrices, which are compared with the Gaussian random matrix. In the first subsection, the feasibility is verified, the security is analysed in the next subsection, the last subsection gives the results of the image encryption and analyses the performance.

A. Feasibility of CCS

Feasibility verification includes the recovery error, the incoherence of the measurement matrix and the sparsity matrix, and the compressive ratio. The experiment results of these aspects were analysed one by one. In this experiment, the signal length N is 256, the sparsity$K$ is 7, and the recovery algorithm isOMP. The size of all of the four measurement matrices are 64 × 256. The Gaussian matrix are generated randomly. The Chebyshev matrix is generated by the Chebyshev system. The initial value is 0.32, the chaotic parameter is 20. The sampling initial position is 1, the sampling distance is 4. The Logistic matrix is generated by Logistic system. The initial value is 0.32, the chaotic parameter is 4. The sampling parameters are the same as those of the Chebyshev matrix. The Tent matrix is generated by Tent system. The initial value is 0.32, the chaotic parameter is 0.3. The sampling parameters are the same as those of the Chebyshev matrix.

B. Security Analysis of CCS

The key space and the key sensitivity will be analysed in this part. Key sensitivity of CCS with the Chebyshev chaotic system. Five kinds of perturbation matrices are compared with the original matrix. The performances are measured by the relative error with different SNR. Curve (1) denotes the result of the original encrypted matrix. Curves (2)–(6) denote the results of the five kinds of perturbation matrices.

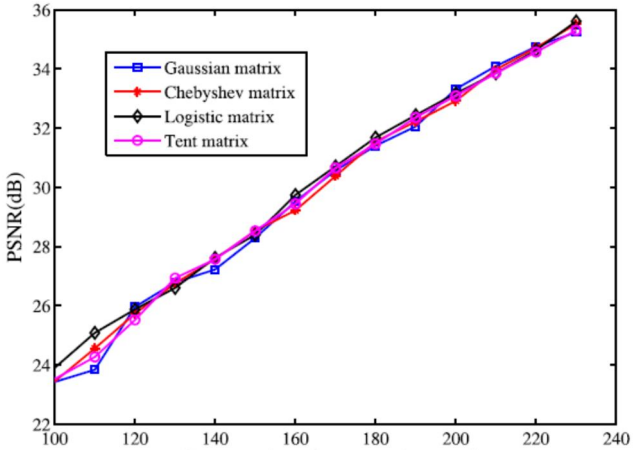


Fig 2. Encryption Analysis

C. Encryption Results and Analysis

In this part, the image encryption results are shown, and the security of the proposed method is analysed by image histograms, adjacent pixels correlation and image entropy. The plain image is an image of Lena by 256 × 256, and the gray value is from 0 to 255. The sizes of all of the encrypted matrices are 190 × 256. Fig. 21 shows the encrypted images. In Φ1 is a Chebyshev matrix, the initiation value is 0.32, the chaotic parameter is 20, the sampling initial position is 1, the sampling distance is 4, Φ2 is a Tent matrix, the initiation value is 0.32, the chaotic parameter is 0.4, the sampling initial position is 1, the sampling distance is 4.

Fig 3: Histogram Images

CCS involves extensive bandwidth usage. That can be represented in the form of his image entropy.

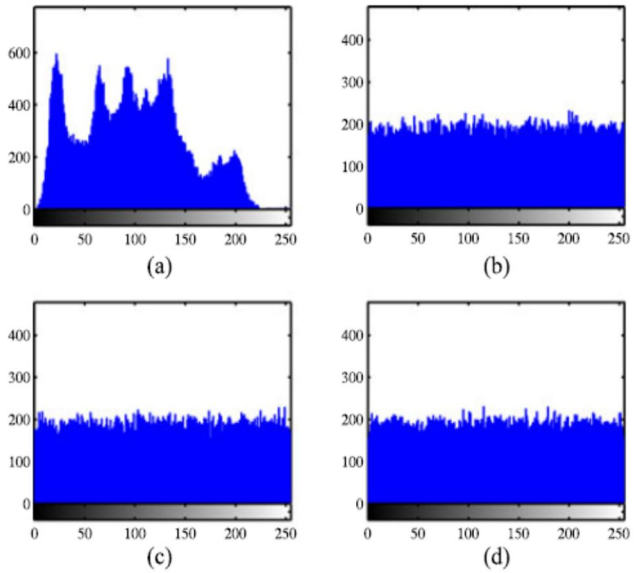


Fig: 4: Image Entropy

IV. FUTURE WORK

A. The future work for this thesis can be divided into the following areas:

1) We have simulated the benefit of CS theory to wireless ECG systems for five records of ECG signals. Our future work will involve developing the CS theory to other records of ECG signals, including abnormal records.

2) We have simulated the benefit of CS upon normal and abnormal ECG signals to provide a robust sampling approach. Our future work involves developing the CS theory to other types of biomedical signals such as EMG and EEG signals.

3) We have simulated the benefit of CS theory to WBANs for the on-body to on-body scenario. Our future work will involve developing the CS theory to other scenarios such as on-body to in-body, and in-body to on-body. We have also examined MFCs with CS for a particular ECG signal. It will be another part of our future work to employ MFCs with CS theory for other types of biomedical signals

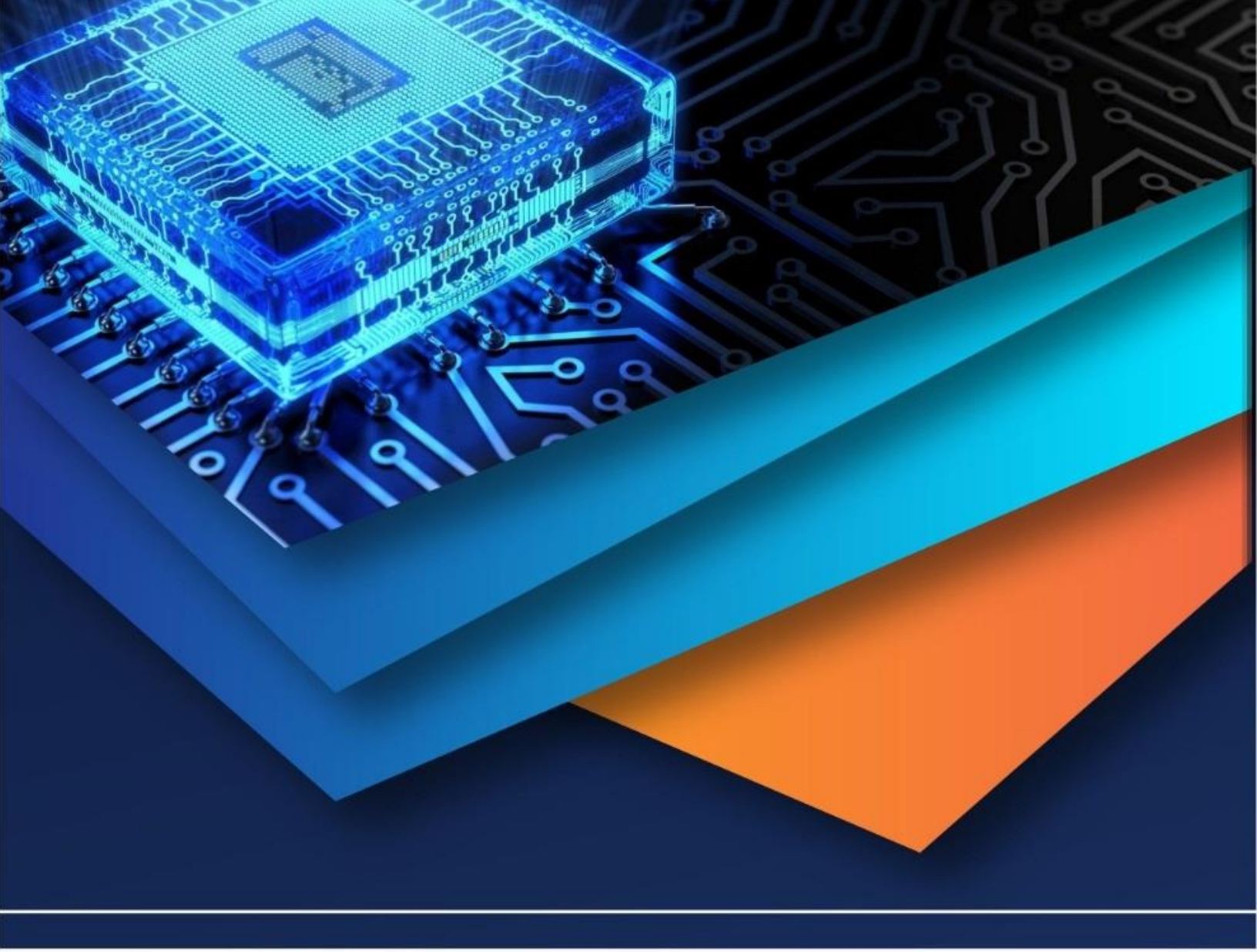
4) Our future work also involves fabricating biomedical wireless sensors based on the results of this work.

V. CONCLUSION

The main conclusion of this dissertation is that advanced WBANs based on CS will be able to deliver healthcare not only to patients in hospital and medical centers but also in their homes and workplaces; thus offer cost saving and improve the quality of life. As an important result of these networks, patients gain more mobility and comfort around medical equipment. Further applications of WBANs with CS theory introduce abundant possibilities to improve the quality of collected Data in order to make Data decisions for diagnostic and therapeutic Purposes. The simulation results show that the encryption performance is excellent. Future works could be carried out to develop CCS in mobile context, like sports games, in which the mobility of the body and the body gesture should be taken into account. Moreover, for saving energy further, the routing protocols are needed for BBN. Although future research is needed, this work indicates that CCS is available in BBN to fulfill the energy-efficiency and security and saving the storage space.

REFERENCES

[1] A. H. Sodhro, Y. Li, and M. A. Shah, "Energy-efficient adaptive transmission power control for wireless body area networks," IET Commun., vol. 10, no. 1, pp. 81–90, 2016.
[2] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," Egyptian Informat. J., 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/ S1110866516300482
[3] X. Liu, Y. Zhu, Y. Ge, D. Wu, and B. Zou, "A secure medical information managementsystemforwirelessbodyareanetworks,"KSIITrans.Internet Inf. Syst., vol. 10, no. 1, pp. 221–237, 2016.
[4] S. A. Salehi, M. A. Razzaque, I. Tomeo-Reyes, N. Hussain, and V. Kaviani, "Efficient high-rate key management technique for wireless body area networks," in Proc. 22nd Asia-Pacific Conf. Commun., Aug. 2016, pp. 529–534.
[5] L. Wu, Y. Zhang, L. Li, and J. Shen, "Efficient and anonymous authentication scheme for wireless body area networks," J. Med. Syst., vol. 40, no. 6, pp. 1–12, 2016.
[6] H. Zhu, L. Gao, and H. Li, "Secure and privacy-preserving body sensor data collection and query scheme," Sensors, vol. 16, no. 2, 2016, Art. no. 179.
[7] A. M. R. Dixon, E. G. Allstot, D. Gangopadhyay, and D. J. Allstot, "Compressed sensing system considerations for ECG and EMG wireless biosensors,"IEEETrans.Biomed.CircuitsSyst.,vol.6,no.2,pp.156–166, Apr. 2012.
[8] R. Dautov and G. R. Tsouri, "Securing while sampling in wireless body area networks with application to electrocardiography," IEEE J. Biomed. Health Informat., vol. 20, no. 1, pp. 135–142, Jan. 2016.
[9] F. Pareschi, P. Albertini, G. Frattini, M. Mangia, R. Rovatti, and G. Setti, "Hardware-algorithms co-design and implementation of an analogtoinformation converter for biosignals based on compressed sensing," IEEE Trans. Biomed. Circuits Syst., vol. 10, no. 1, pp. 149–162, Feb. 2016.
[10] A. Wang, F. Lin, Z. Jin, and W. Xu, "Ultra-low power dynamic knob in adaptive compressed sensing towards biosignal dynamics," IEEE Trans. Biomed. Circuits Syst., vol. 10, no. 3, pp. 579–592, Jun. 2016.
[11] Y. C. Cheng, P. Y. Tsai, and M. H. Huang, "Matrix-inversion-free compressed sensing with variable orthogonal multi-matching pursuit based on prior information for ECG signals," IEEE Trans. Biomed. Circuits Syst., vol. 10, no. 4, pp. 864–873, Aug. 2016.
[12] M. Shoaran, M. H. Kamal, C. Pollo, P. Vandergheynst, and A. Schmid, "Compact low-power cortical recording architecture for compressive multichannel data acquisition," IEEE Trans. Biomed. Circuits Syst., vol. 8, no. 6, pp. 857–870, Dec. 2014.
[13] E. J. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," IEEE Trans. Inf. Theory, vol. 52, no. 2, pp. 489–509, Feb. 2006.
[14] D. L. Donoho, "Compressed sensing," IEEE Trans. Inf. Theory, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.
[15] Y. Tsaig and D. L. Donoho, "Extensions of compressed sensing," Signal Process., vol. 86, no. 3, pp. 549–571, 2006.
[16] J. A. Tropp and A. C. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," IEEE Trans. Inf. Theory, vol. 53, no. 12, pp. 4655–4666, Dec. 2007.
[17] H. Yuan, H. Song, X. Sun, K. Guo, and Z. Ju, "Compressive sensing measurement matrix construction based on improved size compatible array LDPC code," IET Image Process., vol. 9, no. 11, pp. 993–1001, 2015.
[18] W. Yan, Q. Wang, and Y. Shen, "Shrinkage-based alternating projection algorithm for efficient measurement matrix construction in compressive sensing," IEEE Trans. Instrum. Meas., vol. 63, no. 5, pp. 1073–1084, May 2014.
[19] G. Li, Z. Zhu, D. Yang, L. Chang, and H. Bai, "On projection matrix optimization for compressive sensing systems," IEEE Trans. Signal Process., vol. 61, no. 11, pp. 2887–2898, Jun. 2013.
[20] D. Xie, H. Peng, L. Li, and Y. Yang, "Semi-tensor compressed sensing," Digital Signal Process., vol. 58, pp. 85–92, 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY