iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4317

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 7 Issue IV, Apr 2019- Available at www.ijraset.com

A Survey on Efficient Routing Protocol in Wireless Sensor Network

Anamika Walter[1], Manoj Singh[2]
[1, 2]*Shri Shankaracharya Technical Campus, Shri Shankaracharya Engineering College, Bhilai (C.G.)*

Abstract: Wireless sensor network (WSN) is a lot of at least two terminals with remote associations; every node can be moved in a separate sensor network area. In the group based WSN, we choose a head node which is totally in charge of information transmission and going about as a head node among all nodes. Different nodes can fit to gather information however don't transmit information without the consent of the header node. We are additionally utilizing a portable sink which decreases the vitality loss of sensor nodes, Due to the movable property in the system area; we called it likewise Dynamic wireless sensor system. Wireless sensor network spread utilizing the portable sink, we lessen the system combination just as improve network life cycle.
Keywords: Wireless Sensor Networks (WSN), Mobile sink, Network Lifetime.

I. INTRODUCTION

Wireless communications have empowered the development of minimal effort, low-control, multifunctional sensor nodes that are little in size and convey in short separations. These little sensor nodes, which comprise of detecting, information preparing, and imparting parts, impact the plan of sensor systems dependent on joint exertion of an enormous number of nodes.
A sensor network is gathered of an enormous number of sensor nodes, which are compactly deployed either inside the event or exceptionally near it. The area of sensor nodes need not be built or prearranged. This permits easygoing sending in blocked off territories. This additionally implies sensor network protocols and calculations must hold self-sorting out abilities. An extra exclusive characteristic for sensor systems is the together effort of sensor nodes. Sensor nodes are worked in with an on-board processor as opposed to exchanging the raw information to the nodes trustworthy for the combination; sensor nodes utilize their preparing capacities to close-by complete basic calculations and transmit just the obligatory and partially processed information.

II. APPLICATION OF WSN

1) *Spot Monitoring:* Spot screens a standout amongst the most critical utilization of the DWSN in which we know the learning about what is happing in a specific spot. Like we need to comprehend the wonder of the foe in the certain or think about the action of non-military personnel in a specific range then we can utilize the DWSN.
2) *Ecological Monitoring:* When we will discuss the natural checking than amid the term of the environmental observing we see the wireless sensor network in the numerous fields like the Wireless Sensor network use about earth science.
3) *Air Quality Monitoring:* By the assistance of the DWSN we can quantify how much our air has been dirtied it is possible that it is appropriate for our wellbeing or not. By the assistance of the DWSN, we can spare our condition.
4) *Monitoring Quality Of Water:* According to the properties of the water with the assistance of Wireless sensor network, we can realize how much water has been contaminated of streams, lakes, and sea, just as the underground water repository.
5) *Earthquake Detection:* By the assistance of the DWSN we can distinguish the sliding of the land or development of the dirt in the earth.
6) *Usual Disaster Avoidance:* By the assistance of the Dynamic remote sensor network, we can maintain a strategic distance from the standard calamity like flooding in the sea and stream. With the assistance of the Wireless sensor organizes, we can screen the water level in the sea and make the advantageous move against debacle.
7) *Machine Health Monitoring:* By the assistance of the Dynamic wireless sensor network, we can help in the support of ventures Instrument. We can think about the machine, as indicated by the specific parameter holding up in the remote sensor system and make the product move against the generation of the merchandise.
8) *Agriculture Field:* In the field of horticulture, we can utilize the dynamic wireless sensor network. By the idea of the gravity feed water framework, we can screen the water tank level and we can control the siphon utilizing the remote I/O gadgets and spare the water by sending the information to the control place for charging .

9) *Military Applications:* sensor systems depend on the strong activity of dispensable and minimal effort sensor hubs, the harm of certain hubs by hostile activities does not influence a military task as much as the demolition of a conventional sensor, which makes the sensor, systems thought an improved methodology for combat zones.
10) *Fitness Applications:* Some of the Fitness applications for sensor systems are given that interfaces for the incapacitated; included patient checking; diagnostics; tranquilize the executives in emergency clinics, and so on.
11) *Residence Automation:* As innovation progresses, keen sensor nodes and actuators can be shrouded in apparatuses, for example, vacuum cleaners, microwaves, iceboxes. These sensor nodes inside the home apparatuses can participate with one another and with the outside system by means of the Internet or Satellite.

III. SECURITY ISSUES IN WIRELESS SENSOR NETWORKS

Security in the Dynamic wireless sensor network is a standout amongst the most difficulties issue. To see a wide range of conceivable assault are dependably a decent answer for the security arrangement:

1) *Privacy:* Is a standout amongst the most vital for a dynamic wireless sensor network. It guarantees that the message of the sender is gotten by the genuine receiver. For the protection in the dynamic wireless sensor arrange, it utilizes the numerous procedures for the security toward the sink some system utilize productive single direction hash chains in sensor must affirm the wellspring of the reference point message before they can send the information to the sink node.
2) *Data Dependability:* Privacy in the information in the dynamic wireless sensor guarantee that the information has not been stolen by the interloper but rather it doesn't imply that till now information is secure. There might be chances that information can be hacked by the intruder. To give greater unwavering quality for example blunder free transmission of the information, the information dependability instrument gives security that the information has come to its present goal without adjustment of information.
3) *Data Novelty:* In the information, it ought to be guaranteed that we are not utilizing the old information we are utilizing the present information. Information novelty recommends that we are utilizing the present information. This is required when we utilize the common key. This guaranteeing should be possible by including a period subordinate counter with the bundle.
4) *Network test Systems:* Many powerful wireless sensor systems simulative investigations dependent on the reenactment apparatuses. Which gives the advantages to the engineer since devices give predefined models to most correspondence conventions?
5) *Authentication:* Besides adjusting bundles, a challenger can likewise conceivably alter the surge of the parcels through the expansion of phony parcels to the system. In this way, the challenger can make accepting node think about that the information originates from a veritable source. In addition, confirmation is required for a few managerial assignments (i.e., dynamic system Reprogramming, controlling node obligation cycle). In this manner, we can build up that message affirmation is Important for some, sensor network applications.

IV. EVOLUTION

In 2001, I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci studied about wireless sensor networks in which they describe the concept of sensor networks which has been made viable by the convergence of micro electro- mechanical systems technology, wireless communications and digital electronics. First, the sensing tasks and the potential sensor network applications are explored, and a review of factors influencing the design of sensor networks is provided.

In 2002, Jason Lester Hill design System Architecture for Wireless Sensor Networks they present an operating system and three generations of a hardware platform designed to address the needs of wireless sensor networks. Their operating system, called Tiny OS uses an event based execution model to provide support for fine grained concurrency and incorporates a highly efficient component model.

In 2004, Raquel A.F. Mini, Antonio A.F. Loureiro, Badri Nath develops The distinctive design characteristic of a wireless sensor network: the energy map in which the key challenge in the design of a wireless sensor network is maximizing its lifetime. This is a fundamental problem and new protocol engineering principles needing to be established in order to achieve this goal. The information about the amount of available energy in each part of the network is called the energy map and can be useful to increase the lifetime of the network. They propose using the energy map as a protocol engineering principle for this kind of network.

In 2005, Daniele Puccinelli and Martin Haenggi studied about Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing, in which Sensor networks offer a powerful combination of distributed sensing, computing and communication. They lend themselves to countless applications and, at the same time, offer numerous challenges due to their peculiarities, primary the stringent

energy constraints to which sensing nodes are typically subjected. The distinguishing traits of sensor networks have a direct impact on the hardware design of the nodes at least four levels: power source, processor, communication hardware, and sensors.

In 2006, Adam Dunkels, Niclas Finne, Joakim Eriksson, Thiemo Voigt suggest that while in general the overhead of a virtual machine is high, a combination of native code and virtual machine code provide good energy efficiency. Dynamic run-time linking can be used to update the native code, even in heterogeneous networks.

In 2006 Dirk WESTHOFF, Joao GIRAO, Amardeo SARMA describes security solutions for collecting and processing data in Wireless Sensor Networks (WSNs). Adequate security capabilities for medium and large scale WSNs are a hard but necessary goal to achieve to prepare these networks for the market. They include an overview of security and reliability challenges for WSNs and introduce a toolbox concept to support such a framework.

In 2006 John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary decribes As wireless sensor networks continue to grow, so does the need for effective security mechanisms. Because sensor networks may interact with sensitive data and/or operate in hostile unattended environments, it is imperative that these security concerns be addressed from the beginning of the system design. However, due to inherent resource and computing constraints, security in sensor networks poses different challenges than traditional network/ computer security.

In 2006 Yong WangGarhan AtteburyByrav Ramamurthy presents a survey on security issues in WSNs First they outline the constraints, security requirements, and attacks with their corresponding countermeasures in WSNs. Then they present a holistic view of security issues. These issues are classified into five categories: cryptography, key management, secure routing, secure data aggregation, and intrusion detection.

In 2006 Al-Sakib Khan Pathan Hyung-Woo Lee Choong Seon Hong investigate , Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in the future. The inclusion of wireless communication technology also incurs various types of security threats. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks.

In 2007 Prabhudutta Mohanty, Sangram Panigrahi Nityananda Sarma, Siddhartha Sankar Satapathy they explored general security threats in wireless sensor network and made an extensive study to categorize available data gathering protocols and analyze possible security threats on them.

In 2008 Luis E. Palafox , J. Antonio Garcia-Macias they present the growing challenges related to security in wireless sensor networks. They show possible attack scenarios and evidence the easiness of perpetrating several types of attacks due to the extreme resource limitations that wireless sensor networks are subjected to. Nevertheless, they show that security is a feasible goal in this resource-limited environment; to prove that security is possible they Survey several proposed sensor network security protocols targeted to different layers in the protocol stack. The work surveyed in their chapter enables several protection mechanisms vs. well documented network attacks.

In 2008 Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz deals with some security issues over wireless sensor networks (WSNs). A survey of recent trends in general security requirements, typical security threats, intrusion detection system, key distribution schemes and target localization is presented. In 2009 Chiara Buratti Andrea Conti Davide Dardari and Roberto Verdone their survey paper aims at reporting an overview of WSNs technologies, main applications and standards, features in WSNs design, and evaluations. In 2010 Amar Adnan Rasheed M.S., Northeastern Dr. Rabi N. Mahapatra In their dissertation, they consider a number of security schemes for WSN (wireless sensor network) with MS. The schemes offer high network's resiliency and low communication overhead against nodes capture, MS replication and wormhole attacks. They propose two schemes based on the polynomial pool scheme for tolerating nodes capture: the probabilistic generation key pre-distribution scheme combined with a polynomial pool scheme, and the Q-composite generation key scheme combined with a polynomial pool scheme. The schemes ensure low communication overhead and high resiliency. In 2011 Dr. Manoj Kumar Jain in their paper they attempt to present a survey on the major topics in wireless sensor network security, and also present the obstacles and the requirements in the sensor security, classify many of the current attacks, and finally list their corresponding defensive measures. In 2012 Xiaojiang Ren Weifa Liang In their paper they consider data collection in an energy harvesting sensor network with a mobile sink, where a mobile sink travels along a trajectory for data collection subject to a specified tolerant delay constraint T. The problem is to find an optimal close trajectory for the mobile sink that consists of sojourn locations and the sojourn time at each location such that the network throughput is maximized, assuming that the mobile sink can only collect data from one-hop sensors, for which they first show that the problem is NP-hard. Then they devise novel heuristic algorithms. They finally conduct extensive experiments to evaluate the performance of the proposed algorithms. In 2013, Mian Ahmad Jan and Muhammad Khan, A Survey of Cluster-based Hierarchical Routing Protocols in which Wireless Sensor

Networks consists of small miniaturized Sensor nodes which collect data from their environment and route to a central Base Station. Due to their resource constraint nature, various routing protocols have been design to reduce the consumption of energy of the nodes. In this paper they have presented a brief survey of Cluster-based Hierarchical routing protocols. These protocols organize the nodes into small groups known as Clusters. One node per Cluster is elected as Cluster Head (CH) in each round to transmit the data to the Base Station. CHs are either selected by the desire node itself or by the Base Station. They presented a comparison among these clustering protocols in Section based on various features which highlights their transmission mode and selection algorithms for CHs. In 2014, Naveen Sharma and Anand Nayyar Review of Cluster Based Energy Efficient Routing Protocols for Wireless Sensor Networks. In recent times wireless sensor networks have grown enormously and become progressively attractive in wide variety of applications because of their low cost, small in size, self-organizing behavior in harsh environments. Routing is a vital technology in WSN. There are many routing protocols like: location based, multipath, data centric, mobility based, hierarchical routing, hybrid routing etc. Clustering is used to prolong the lifetime of the wireless sensor networks. Clustering is the process where sensing area is divided in groups to balance the energy level of sensor nodes known as clusters. An Optimal Clustering technique can reduce the energy consumption in WSN and increase the lifetime of the network. Energy is the main consideration when they analyze routing protocols for WSN. In this paper they present the study of different clustering based energy efficient routing protocols of wireless sensor networks and compared them on various parameters.

V. CONCLUSION AND FURTHER DEVELOPMENT

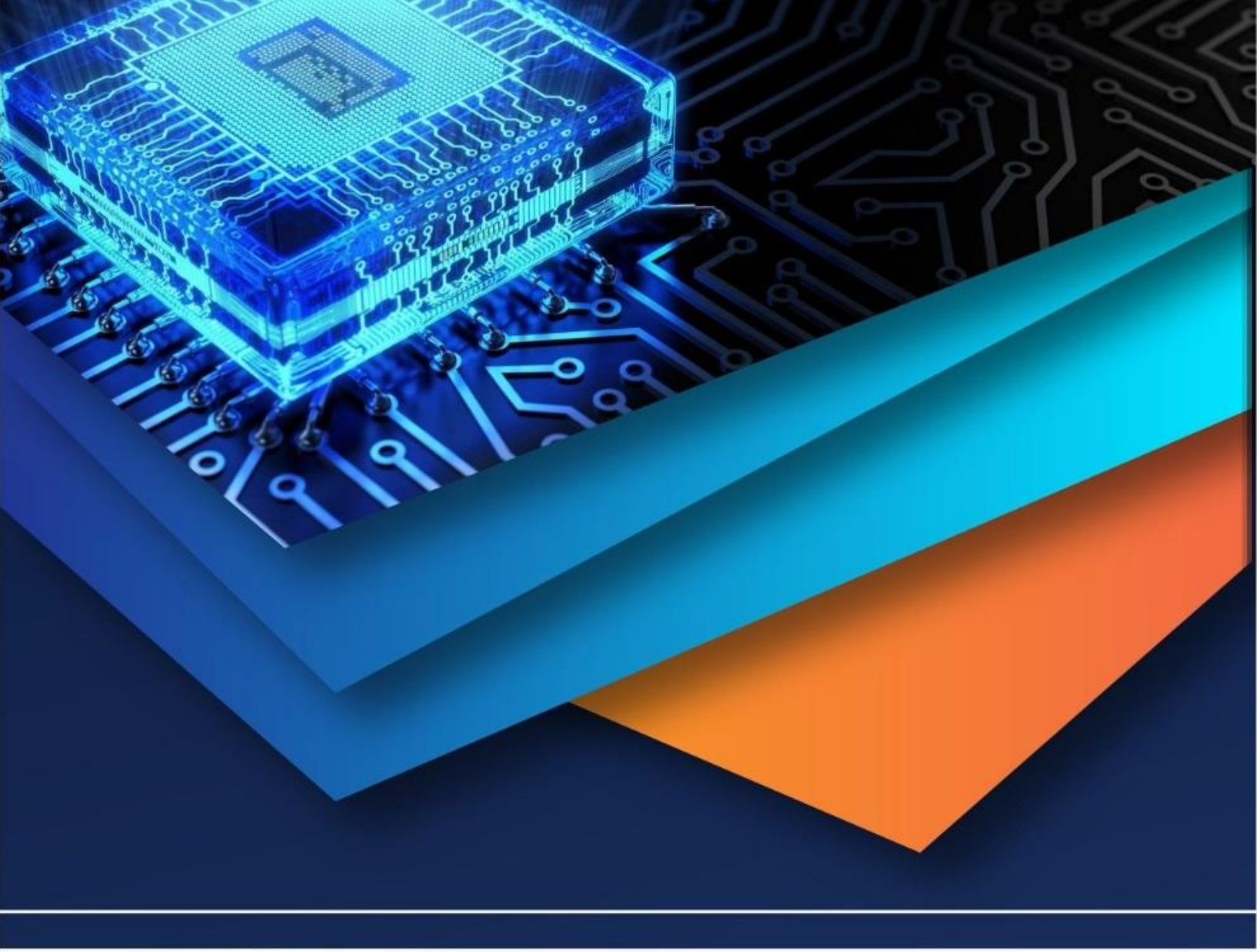
In the present situation, wireless innovation will use in everywhere throughout the world for quick correspondence of the end client. The significance of the wireless sensor network in our day by day life & security issues and survey of wsn has been examined in these papers, we have talked about the different kinds of the wireless sensor system and we have additionally talked about the different grouping based WSN and the benefits of these advances over the wired innovation. We have likewise considered different papers identified with the above subject.

REFERENCES

[1] F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci “A survey on sensor networks”, IEEE Communications Magazine, 40(8), pp. 102–114, 2002.
[2] Rahul C. Shah, Sumit Roy, Sushant Jain, Waylon Brunette,“Data MULEs: Modeling and analysis of a threetier architecture for sparse sensor networks”, In Proceeding of the IEEE Workshop on Sensor Network Protocols and Applications, pp. 30-41, 2003.
[3] Wang W. Srinivasan V, Chua KC,“Using mobile relays to prolong the lifetime of wireless sensor networks”, In Proceeding of the 11th Annual Int’l Conf. on Mobile Computing and Networking, pp. 270-283, 2005.
[4] S. ˇCapkun and J.-P. Hubaux. Secure positioning in wireless networks. IEEE Journal on Selected Areas in Communications, 24(2):221–232, 2006.
[5] In 2006 In 2006 Ossama Younis, Marwan Krunz, and Srinivasan Ramasubramanian, University of Arizona, “Node Clustering in Wireless Sensor Networks: Recent Developments and Deployment Challenges”, IEEE Network • May/June 2006, Pp:20-25.
[6] In 2009, Dilip Kumar, Trilok C. Aseri and R.B. Patel, **“**EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks”, Computer Communications 32 (2009), Pp: 662–667.
[7] L. Lamport, “Password authentication with insecure communication,” Communications of the ACM, vol. 24, no. 11, pp. 770-772, November 1981
[8] Debnath, Ashmita; Singaravelu, Pradheepkumar; Verma, Shekhar (19 December 2012). "Efficient spatial privacy preserving scheme for sensor network". Central European Journal of Engineering 3 (1): 1–10.
[9] Surie, D., Laguionie, O., Pederson, T.: "Wireless Sensor Networking of Everyday Objects in a Smart Home Environment". In Proceedings of the 4th International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Sydney, Australia, pp. 189-194, (2008).
[10] In 2010 Bager Zarei, , Mohammad Zeynali and Vahid Majid Nezhad proposed “a novel Cluster Based Routing Protocol in wireless sensor network”, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010, , Pp: 32 – 36.
[11] In 2012, Dervis Karaboga, Selcuk Okdem and Celal Ozturk, “Cluster based wireless sensor network routing using artificial bee colony algorithm”, Wireless Netw (2012) 18: Pp: 847–860.
[12] F. Viani, P. Rocca, M. Benedetti, G. Oliveri, A. Massa , "Electromagnetic passive localization and tracking of moving targets in a WSN-infrastructure environment " in Inverse Problems, vol. 26, (2010), p. 1-15.
[13] In 2013, Mian Ahmad Jan and Muhammad Khan**,** “A Survey of Cluster-based Hierarchical Routing Protocols” International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501Vol.3, No2, April 2013, Pp: 138 – 143.
[14] In 2014, Naveen Sharma and Anand Nayyar “Review of Cluster Based Energy Efficient Routing Protocols for Wireless Sensor Networks”, IJAIEM Volume 3, Issue 1, January 2014, Pp: 441 - 453.

Anamika Walter, B.E., M.Tech. Scholar in E-Security from Shri Shankaracharya Engineering College, Bhilai, India. Research areas are Wireless Sensor Network, mobile ad hoc network & its enhancement.

Manoj Singh, Asst. Professor, Dept. of Computer Science & Engineering at Shri Shankaracharya Engineering College, Bhilai, India, Having wide experience in the field of teaching. Research areas are Wireless Sensor Network, its Enhancements, and His research work has been published in many national and international journals.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY