iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** V **Month of publication:** May 2016

DOI:

www.ijraset.com

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

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Mechanism To Detect The Selfish Nodes

E.Divya kalyani[1], Dr. S. Kirubakaran[2], K. Maheswari[3]
[1]P.G Scholar, Info Institute of Engineering, Coimbatore, Tamil Nadu, India
[2]Associate Professor, Info Institute of Engineering, Coimbatore, Tamil Nadu, India
[3]Associate Professor, SNS institute of Technology, Coimbatore, Tamil Nadu, India

Abstract: ***In Manet (mobile adhoc network) the nodes cooperate to work. But the performance is being affected due to cost intensive activity in which nodes do not cooperate. This behavior among the nodes is being identified using watchdog mechanism. They combined the watchdogs to detect the selfish nodes based on first hand information whenever the contact occurs. But there are several issues in detecting these selfish nodes. This may fail because of false positive and negative detection among the neighbor nodes, which does not match the watchdog detection. In this paper, I propose an EDTM (Efficient Distributive Trust Model) for wireless sensor nodes based on the packets received by the nodes. By this we can calculate the direct and recommended trust. We also can calculate the data, energy and communication, trust more efficiently. Furthermore, the accuracy can be improved by reliability familiarity. The security and trustworthiness of sensor nodes can be evaluated more precisely.***

Keywords: SELFISH NODES ,MALICIOUS NODES, FALSE POSITIVE ,FALSE NEGATIVE, WATCHDOGS,WSN, ENERGY EFFICIENT, DISTRIBUTED TRUST MODEL.

I. INTRODUCTION

In an emerging technology WSN play a major role, such as traffic management, battlefield surveillance etc.providing the security among them is so important for safe application of WSNs. There are various security mechanism to avoid threats, but they suffer in DoS. To establish the secure communication between nodes we need to ensure that all nodes are trusted. Nowadays many developers have established various trust models between the nodes to build the relationship.

The two key factors are watchdogs and reputation system.Watchdogs are responsible for monitoring the communication nodes . They check the behavior and detect the selfish nodes. The reputation system are responsible for reputation value. In RFSN they have discussed about the direct trust and not about the recommended trust.in PLUS Parameterized and Localized trust management scheme recommendation is being used to built the trust among the nodes. Here in Fig 1 which has the network structure in which message from source node to the destination where they are sent with trust calculations based on direct indirect and recommended trust. Whenever that is the node judge node which perform trust evaluation receive the packet ,it check the integrity value if it fails the trust value will be decreased.

Another trust evaluation algorithm which is based on trust factors depending on the communication behavior between the nodes. At the communication point of view we cannot decide whether the sensor nodes can be trusted or not. In addition to this energy level should be taken into account to calculate the trustworthiness of sensor nodes.

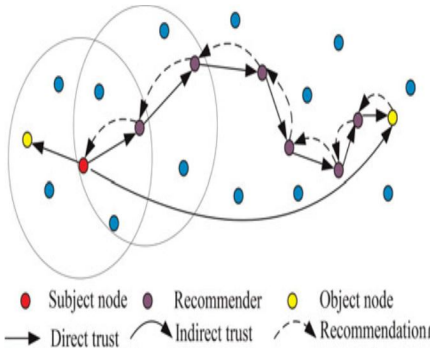


Fig 1 network structure

There are two ways to calculate the trust. They can be done based on direct trust and indirect trust and not all recommended trust are reliable. However, in real application a sensor node to obtain trust value of non neighbouring nodes. They need the information of two hop neighbor nodes to establish the routing and localize them. Since we have dynamic topology the trust relationship between sensor nodes constantly changes. Truest changes with time and environment conditions.the proposed system by which evaluation of

©IJRASET: All Rights are Reserved

relationship between sensor nodes more precisely and efficiently.

II. LITERATURE REVIEW

To reduce these type of issue in the network and increase the efficiency of the system ,the trust between the neighboring nodes is being calculated. H. S. Lim [1] address that sensor nodes are being increasingly deployed in decision making infrastructure. By this decision makers aware of trustworthiness of data which is being collected are crucial. Quantitative measures of trustworthiness that is valued in computing their trust scores as well as data provenance. Inter- dependency property which is reflected from cyclic frame work by which trust value is obtained. These trust scores which affect the true score of the network which are manipulated. The principle of value similarity comes from "if the same event has similar values,trust scores will be higher". Thus, they have used cyclic framework and also formal method to compute rust values of each nodes.

Wei Gao [2] developed a trust model by improving the subjective logic and analyzing them since they have problem in uncertainty of system,anonymity ,and opening ,the dynamics. Negative event and time effect they have introduced a new trust qualification formula. They have also defined the definition of risk. They can prevent the security dangers of cheat and slander and also the trust relationship between peers are more effective and precise. The problem arose in computing environment can also be resolved effectively.

V. C. Gungor [3] address that in today electric power systems have significant advantages over traditional communication technologies in wireless sensor networks. However the complex electric power system has great challenges in WSN communication. It presents an experimental study on statistical approaches.there are different environments like substation,control room . Field test has been performed. The empirical and experimental result provides valuable insight about sensor network platform and design decision.

G. Han [4] deals with security threats because of communication and computation of delay in wireless sensor network cannot be reduced with traditional security mechanism. They are being suggested with trust management models for effective mechanism.managing trust between the nodes and how they can be modelled are being researched. In this paper they have detailed survey on trust models in WSNs like malicious attack detection, secure routing, node selection, localization, etc. Based on analysis and comparison is done for essential for developing a robust trust model in WSNs.

S. Ganeriwal [5] discussed about the model the automatic data collection through the tiny device was increased in sensor network technology. These technology to measure the unprecedented densities. The challenge in data reliability ,there is significant benefits in every data driven technology. The vulnerable data integirity for both system failure and node. Faults are indicators in data collection system which do not provide any information. In a data fusion network the final outcome is easily affected by corrupted sensor measurement then the problem is reduced. In this paper they have a unified and generalized approach about data accuracy. The communication of trust is being developed between nodes. They can detect the past behavior and future behavior of each node using a framework. For trust evaluation , integration and reoputation methods, beta reputation system from Bayesian formula. This acts as a middleware service between two sensor network operating system.

R. Feng [6] presents WSNs with many factors battlefield applications and exposed node to the environment without protection will be affected and compromised. To address this a new method has been proposed called NBBTE (Node Behavior Strategies Banding Belief Theory of the Trust Evaluation Algorithm). This algorithm integrates the node behavior and evidence theory. The behavior of these nodes trust factors and network application are obtained. By calculating the average trust factor we can obtain the direct and indirect trust value. To give the input as vector of evidence, fuzzy set method is applied. The difference between the direct and indirect trust value which make the D-S combination with the trust value of node. The result which gives simulation of detection of malicious nodes and the trust value characteristics. The real contribution of nodes to evaluate the trust is being proposed.

K. Govindan [7] address in MANET trust plays a major role. The uncertainty and uncontrollability are coping up with the free will of others. The movement of nodes and complexity constraints, there are many challenges in MANETS for trust computation and management. The quality and reliability are being affected which cause the damage in the nodes. The transaction of the nodes has a positive influence among the trust level of the nodes. There are many detailed computing approach in MANETs are a been discussed. The trust propagation, prediction aggregation algorithms is analysed which influence the dynamics of trust and security level.

K. Nordheimer [8] presents the important issue between two unfamiliar users is determining the trust value. The network characteristic which has limitation by calculating these values. Monte Carlo Simulation method by which the local trust value is estimated and interpret the probability of trust are being proposed. The two unfamiliar users who have indirect statements are also

©IJRASET: All Rights are Reserved

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

being estimated. The basic trust properties are being satisfied by new approach in which the trust and distrust information are incorporated.

W. Gao [9] proposed the data dissemination have node mobility and end to end disconnection. By sending the information to single destination the social based approaches are used. In social network perspective the multicast in DTNs is used for the first time. The single and data item is studied in multi cast DTNS and also the difference between the unicast and multicast. The Knapsack problem of selecting the multicast for exploiting node centrality and social community. There is a similar delivery ratio and delay compared with epidemic routing and the reduction of cost may be made by reducing in the reduction of relay used in the network.

Jinfang Jiang [10] address that the trust between the nodes are being calculated by three method direct recommended trust and indirect trust by which they can reduce the sefish node. Wen the contact occurs while transferring the packets the routing table alerts the source node that the path message can be traveled in the particular path. Using EDTM they have simulation results are efficient and the packet loss is also reduced.

III. PROPOSED SYSTEM

The proposed system design a framework shows how the selfish nodes are being detected as in Figure 1 in which the message path is recognized and they are sent to the destination.

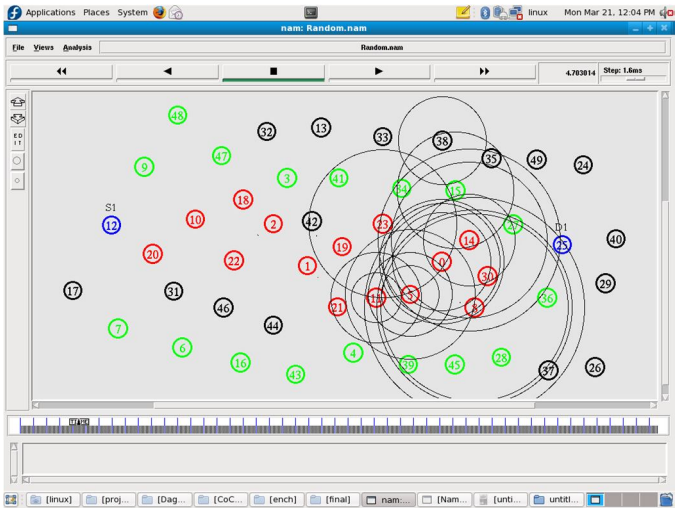


Fig 2 forwarding the packets

A. *Direct Trust:* Direct trust is a kind of trust calculated based on the direct communication behaviors. It reflects the trust relationship between two neighbor nodes. Direct trust by considering communication trust, energy trust and data trust. The sensor nodes in WSNs usually collaborate and communicate with neighbor nodes to perform their tasks. Therefore, the communication behaviors are always checked to evaluate whether the sensor node is normal or not. However, due to the nature of wireless communication, there are many reasons resulting in the packets loss and the communications between sensor nodes are unstable**.**

B. *Recommendation Trust:* The recommendations from third parties are not always reliable, need an efficient mechanism to filter the recommendation information. The filtered reliable recommendations are calculated as the recommendation trust. No direct communication behaviors between subject and object nodes, the recommendations from recommender are always taken into account for trust calculation. However, in most existing related works, the true and false recommendations are not distinguished. How to detect and get rid of false recommendations is important since it has great impact on the trust calculation

C. *Indirect Trust:* When a subject node cannot directly observe an object nodes' communication behaviors, indirect trust can be established. The indirect trust value is gained based on the recommendations from other nodes. The calculation of indirect trust includes two steps:

1) The first step is to find multi-hop recommenders between subject and object nodes,
2) The second step is the trust propagation which aims at computing the direct trust. The path from the subject node to the object node established by the recommenders is named as Trust Chain

©IJRASET: All Rights are Reserved

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

3) *Update Of Trust Value:* Due to the dynamic behavior of WSNs such as leaving or joining the network, the trust values of sensor nodes should be updated periodically. First, the trust value should not be updated too often. Because frequently updating the trust value will waste a lot of energy, and the trust evaluation will be easily affected by the network traffic conditions (e.g., congestion and delay). In addition, the update cycle time cannot be too long. A node's historical trust values should be taken into account to measure its current trustworthiness. If the cycle time is too long, it cannot efficiently reflect the current behaviors of the object node. To solve these issues, we use a sliding time window concept to update the trust value

IV. CONCLUSIONS

To identify the malicious nodes trust model, play a vital role in WSNs. In much application like secure routing, secure data aggregation and trusted key exchange it assist. Neighbour nodes can monitor each other with distributed trust model without any central node in wireless sensor nodes. To handle the information in a secure and reliable way an efficient trust model is needed. An efficient distributed trust model is proposed in this paper. In this model we can calculate the direct trust, recommended trust, indirect trust are being discussed.in this model with the simulation result we have a clear idea about efficient and attack resistant trust model. Fig 3 which deals with EDTM the delay is reduced. The message will be delivered in faster rate when compared with existing methods. Fig 4which deals with the overhead of the trust model is being reduced. The overall simulation result is shows that the trust between the neighboring nodes is calculated.

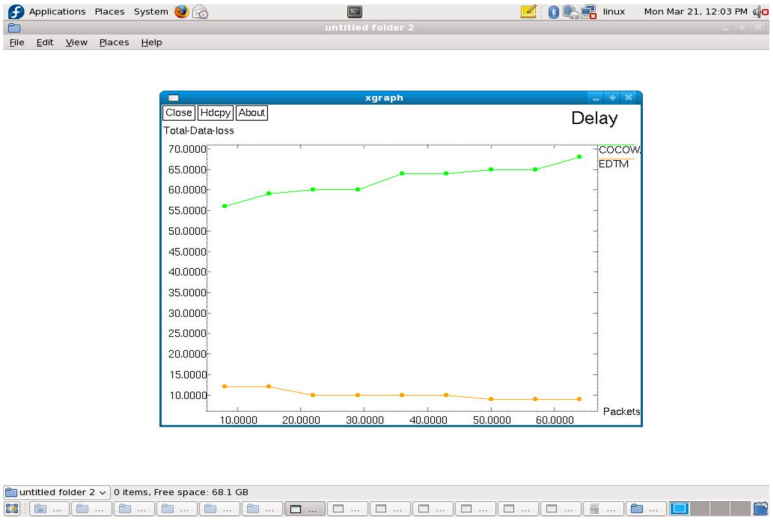


Fig3: x graph on delay

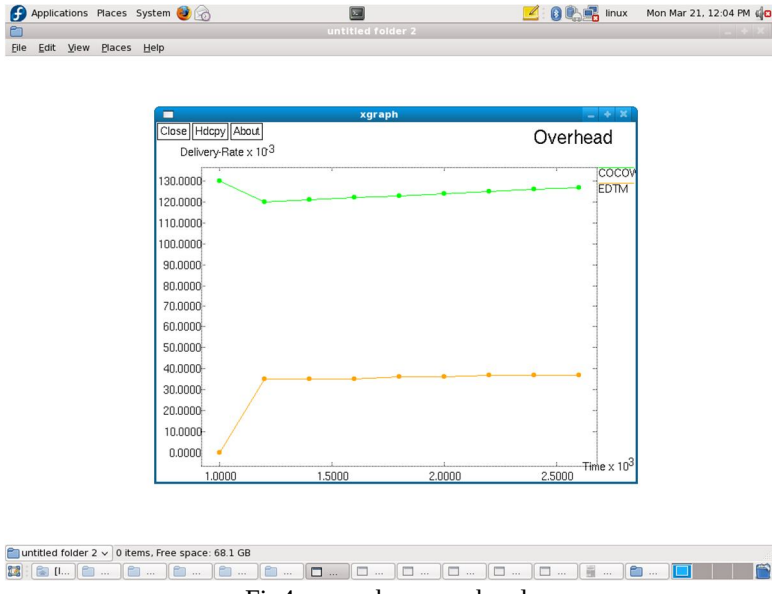


Fig4: x graph on overhead

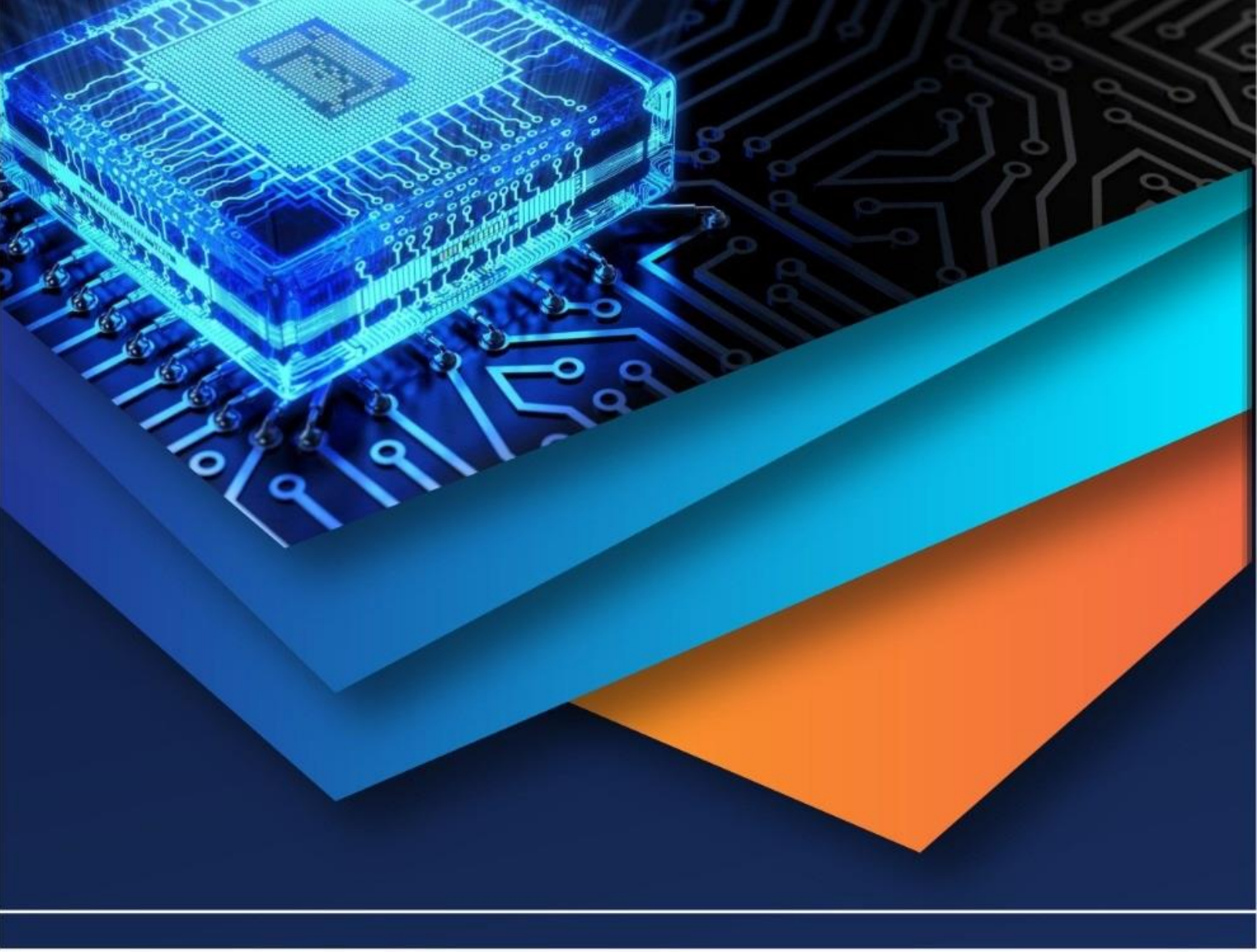
©IJRASET: All Rights are Reserved

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

REFERENCES

[1] H. S. Lim, Y. S. Moon, and E. Bertino, "Provenance based trust worthiness assessment in sensor networks," in Proc. 7th Int. Workshop Data Manage. Sens. Netw., 2010, pp. 2–7.
[2] W. Gao, G. Zhang, W. Chen, and Y. Li, "A trust model based on subjective logic," in Proc. 4th Int. Conf. Internet Comput. Sci. Eng., 2009, pp. 272–276.
[3] V. C. Gungor, L. Bin, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557–3564, Oct. 2010.
[4] G. Han, J. Jiang, L. Shu, J. Niu, and H. C. Chao, "Managements and applications of trust in wireless sensor networks: A Survey," J. Comput. Syst. Sci., vol. 80, no. 3, pp. 602–617, 2014.
[5] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation based framework for high integrity sensor networks," in Proc. 2nd ACM Workshop Security Ad Hoc Sensor Netw., 2004, pp. 66–77.
[6] R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and d-s evidence theory," Sensors, vol. 11, pp. 1345–1360, 2011.\
[7] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile ad hoc networks: A survey," IEEE Commun. Surveys Tuts., vol. 14, no. 2, pp. 279–298, 2nd Quarter 2012.
[8] K. Nordheimer, T. Schulze, and D. Veit, "Trustworthiness in networks: A simulation approach for approximating local trust and distrust values," IEEE Commun. Surveys Tuts., vol. 321, pp. 157– 171, 2010.
[9] W. Gao, Q. Li, B. Zhao, and G. Cao, "Multicasting in delay tolerant networks: A social network perspective," in Proc. 10th ACM Int. Symp. Mobile Ad Hoc Netw. Comput., 2009, pp. 299–308.
[10] Jinfang Jiang, Feng Wang, "An Efficient Distributed Trust Model for Wireless Sensor Networks",IEEE Transaction on parallel and distributed system, vol 26,no5 May 2015.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)