International Journal of Engineering & Technology, 7 (4.12) (2018) 73-77

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Comparative Analysis of Trust Based Applications in Wireless Sensor Networks

Radhika Gupta[1]*, Dr. Sahil Verma[2], Dr. Kavita[3], Anup lal Yadav[4]

[1]*M.Tech Student in Lovely Professional University*
[2]*Assistant Professor in Lovely Professional University*
[3]*Assistant Professor in Lovely Professional University*
[4]*Assistant Professor in SRMIET*
Corresponding author:sahil.21915@lpu.co.in

Abstract

The wireless sensor network is a type of ad hoc network which is vulnerable to security attacks, specifically insider attacks. In spite of the fact that confidentiality, integrity and authentication helps in forestalling the particular sort of attacks, but they come at an expense. A traditional and evergreen concept of the trust evaluation and management, among the nodes of a network, for communication is a good and effective security measure. Overseeing trust in a distributed wireless sensor network is a challenging task when coordinated effort or participation is must in accomplishing mission and framework objectives. The paper represents a survey of various trust applications which are very helpful for carrying out a secure data transmission in a sensor network. The analysed trust applications malicious attack detection, secure data aggregation, secure node selection and secure routing.

Keywords: *Malicious attack detection, secure data aggregation, secure node selection, trust applications, wireless sensor networks.*

1. Introduction

A wireless sensor network is a major branch of mobile ad hoc networks (MANET). An ad hoc network is distributed infrastructure-less arrangement of nodes, with the capability of self-configuration [10]. Therefore, sensor network is a collection of sensor nodes which can be deployed on fly without any need of centralized and infra structured co-ordination. The pace of technology development in the field of wireless communication and micro-electro-mechanical system has facilitated the deployment of WSNs at a considerable level. WSNs are made out of a relatively large number of sensor nodes. As a rule, sensor nodes are reliable, exact, adaptable, modest, and simple to deploy. A few zones and businesses that are liable to natural requirements depend on WSNs [19] for information accumulation and observing. They are broadly utilized as a part of numerous applications, for example, crisis reaction, medicinal services observing, military, farming, environment checking, homeland security and smart power matrix.

1.1 Wireless Sensor Network (WSN)

Wireless sensor networks (WSN) are the uncommon class of the multi-hop specially appointed systems that are produced to control and screen a wide scope of occasions and marvels. Like WMNs, WSNs are effective in both scholarly communities what's more, industry. WSNs are conveyed for particular application situations (e.g., accuracy horticulture, auxiliary observing etc.). Consequently, the outline of these systems exceedingly relies upon the particular application situation and the necessities of the application regarding dependability, convenience. In a WSN, various remote hubs are deployed inside the monitoring region. These hubs can directly communicate with each other or follow relay hub strategy to transmit the collected information to sink node/base station. In a precise manner, sensor networks are defined as a pure traditional MANET which are application specific. This is shown below with the help of few examples like a sensor network for construction monitoring fig 1.1.

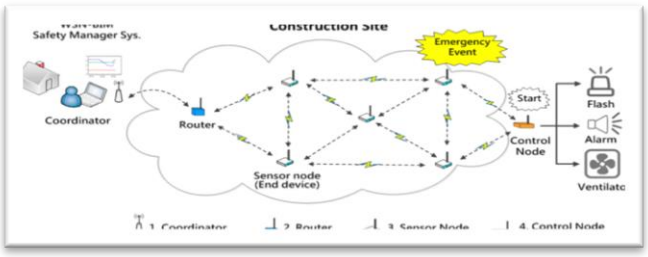

Fig 1: Construction Monitoring sensor network [10]

1.2 Characteristics of WSN

Wireless sensor networks are the sub set of ad hoc networks, but differ in some ways from their super set. Following are the characteristics [19] of sensor networks.

1. WSN's are the infrastructure less ad hoc networks without any central coordination.
2. The nodes in WSN are deployed in thousands and densely in the monitoring area.
3. The sensor nodes can be mobile or stationary, depending upon the requirement.
4. The sensor nodes have ability of self-configuring and provide robust operations with fault tolerance mechanisms.
5. Sensor network operates without a human interface or it can be said that they reduces the human workload specifically in the areas where human access is difficult.

6. In a sensor network, sensor nodes have direct interaction with the physical world. They gather the real time information and transmit it to the base station.
7. Sensor nodes are deployed for various purposes and different types of sensors are optimized for a specific application.
Apart from these, a good wireless sensor network provides [22] power efficiency, responsiveness, reliability and scalability.
Power Efficiency: It is the ability of nodes to manage themselves and consume as less power when there are changing data routes in the network. It is an important point to be considered as the case is of wireless sensor network, in which nodes are running on batteries and remotely located, with no power point access.
Responsiveness: It is defined as the capability of a network to quickly adapt the changes made in the network itself.
Reliability: The purpose of creating a sensor or any other network is met when it provides a reliable communication. A reliable communication is possible when network is free from insider and outsider security attacks, mischievous nodes and other attacks.
Scalability: Scalability is ability of network to grow in terms of quantity i.e. scaling the number of nodes with causing minimum overhead as possible. But this is not the case in real terms, as it causes overhead. Therefore, it should be the last resort to opt when no other option is available.

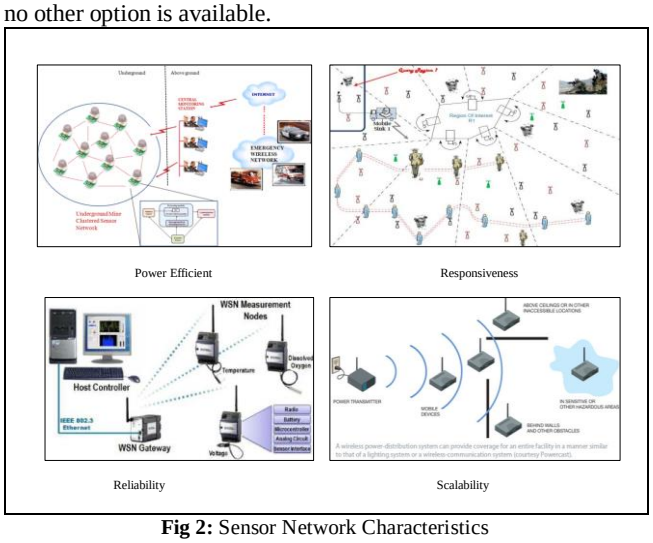

Fig 2: Sensor Network Characteristics

1.3 Applications of WSN

The use of sensor technology has gained a very fast growth in varieties of applications [19][21]. The sensors are the backbone for supporting internet of things these days. Few applications are categorized as follows
1. Medical Applications: Sensor nodes have envisioned a great significance in medical science. Treatment of cancer, heart, bone marrow and kidney transplants have become possible due to sensor and other powerful technology. Use of body sensors (physical contact with body) have eliminated the use of devices for measuring blood pressure, sugar levels etc. hence preventing patients from any last moment serious problems i.e. providing post-operative care.
2. Environmental Applications: Physical sensors are very effective in monitoring environmental factors such as temperature, moisture, humidity, heat, ph. value etc. Sensing these parameters can lead to brilliant growth in terms of agriculture, weather forecasts, reducing fire accidents etc. Along with these physical sensors are also capable of sensing gases, motion of any kind hence providing security and prevention measures against any disastrous situations. The gas and sound sensing sensors are aiding in minimizing the air pollution and sound pollution.
3. Industrial Applications: In the industrial field sensors have just made the infrastructure smart. The buildings, bridges etc. are becoming intelligent by deploying sensors in them. Also use of sensors monitors the wear and tear of the structure due to any natural disaster or according to time that is lapsed after fresh construction, hence provides the information like mechanical stress bearing of bridges and need for renovating them Smart traffic indicators, use of RFIDs are contributing in development of healthy economy.
4. Military Applications: Sensor network serves in several military applications such as tracking of enemy troop movements, detect the use of biological or chemical weapons, improved battlefield communications etc. Auto-deployment and self-configuring nature of sensors plays a vital role when it comes to military purpose.
5. Other Application Areas: The above mentioned areas are the major broad application domains which when applied collectively give rise to another solution for serving different fields. The research is going on the sensors hoping to come out with more powerful and world changing applications.
However, the wireless medium makes the communication and network error and security prone, by different insider and outsider attacks. The insider attacks can harm the network integrity and authenticity to a big extent. Usually the malicious or compromised nodes in the sensor networks are insider attackers which are very difficult to be figured out. Hence, for the guarantee of correct operation of the whole network, network security plays a vital role, which is important to be addressed. In spite of the fact that confidentiality, integrity and authentication [5] helps in forestalling the particular sort of attacks, but they come at an expense. Also as a rule, alone they are not efficient for securing the network, sufficient for outsider attacks.
The trust, a term of social sciences gives a degree of belief about the behaviour of a particular entity. Therefore, it relates in ad hoc sensor networks when the nodes do not having any prior knowledge of interaction, wish to create a communicative network with an acceptable level of trust among themselves. There are properties [3] defined for trust in terms of ordinary or mobile sensor network, can be summarized as follow:
The trust should be dynamic: paper says that rather than using the trust obtained initially throughout network life, it should be evaluated dynamic. This is due to mobile nature of nodes and scalability of network. Therefore, static trust is of no use after a time elapsed since network formation.
Subjective says that every time it is not necessary to get the same level of trust for a trusted node by the trustee. It is due to experience with other nodes or network topology.
Asymmetry, means vice versa is not true. If a node A have some trust level for node B, doesn't mean B will have same level of trust for node A.
Context Dependency implies it depends upon context of the task which determines which different types of trust will be required.
Incomplete transitivity Trust does not follow the mathematical rule of transitivity among nodes. If node A trusts node B and node B trusts node C, then it is not guaranteed that Node A and C will have good level of trust among them.
A detailed analysis of the various trust models [17] for the wireless sensor networks and their applications is done. The rest of the paper is organized as follows: proposed trust techniques and its application in the earlier research works are presented. This is followed by the inferences drawn from the survey done and the conclusion. A variety of trust techniques are studied for maintaining the integrity of the network, which are classified under two broad categories named node trust model and data trust model. The applications include malicious attack detection, secure data aggregation, secure routing and secure node selection.

2. Related Work

Trust evaluation techniques are broadly classified as node trust and data trust. Node trust involves use of either centralized or distributed system and data trust deals with the data transmission i.e. communication.
Zhengwang Ye et. al. 2017 has provided security measures to sensor network by introducing a Dynamic trust Evaluation Mechanism (DTEM). The main focus is to protect data being communicated in the network against any theft or loss, hence data based

trust technique is used.. Two trust metrics namely direct and indirect trust [1] authors have calculated for sensor nodes. Proposed solution adjusts the direct and indirect weight values dynamically and also introduces concept of dynamic sliding window for calculating varying trust values from time to time. The direct trust is based on factors like communication trust, energy trust, and data trust. This follows the punishment factor and regulating function. The indirect trust is evaluation is based on the conditions in order to enhance the accuracy of trust value on the trusted recommendations from a third party. The paper deals with detection of the insider or malicious node, however contribution in suspect nodes separation and routing is not covered.

Yun Liu et. al. 2016 presents a modified trust evaluation scheme for secure data aggregation [2] in wireless sensor networks. The strength of link i.e. relationship between two nodes contribute as the basis of trust formation. Every node in the cluster monitors each other, and uses beta reputation system. This system and strength of link between nodes is used to calculate the trust values for nodes. Therefore, the focus of paper is to achieve higher accuracy in evaluating a node's trustworthiness by introducing the concept of the strength of link into trust-based secure data aggregation.

Suat Ozdemir 2008 has proposed a novel functional reputation based data aggregation protocol, RDAT [6]. A reputation value is assigned to each sensor nodes which is evaluated by data aggregators with the help of functional reputation. Node's reputation and trust is based on sensing, aggregation and routing. The protocol combines the values obtained through these three steps to access trustworthiness of node. The focal point of proposed solution is to check for false data aggregation by malicious nodes and maintain the integrity of aggregated data.

Yanli Yu et. al. 2012 Authors have presented a survey of different trust mechanisms and countermeasures against possible attacks in sensor networks. Paper describes various security measures against attacks then focuses on notion of trust [16] in context of security in sensor networks. The trust schemes are classified as secure routing and secure routing. For secure routing, some trust models are talked about like EMPIRE, RFSN, TRANS etc. and for secure data TIBFIT and secure data sensing methods are mentioned. Along with these, other trust methods such as fuzzy trust model etc. are described. Development of more precise algorithms for less trust energy expenditure is suggested for the readers.

Fenye Bao, Ing-Ray Chen et al. 2012 Authors have proposed a hierarchical trust management protocol [15] for the cluster based wireless sensor networks. The paper represents solution for three major issues of WSNs namely scalability and re-configurability, to cope with malicious sensor nodes and detect intrusions in the network. Hierarchical trust management addresses three parameters as trust composition, trust aggregation and trust formation. Hierarchy of trust composition is formed as from cluster-head (CH) to sensor node (SN), SN to SN and CH to base station (sink node).

Hui Xia, Zhiping Jia et.al. 2014 A trust based multicast routing protocol (FAPTrust) is proposed whose trust metrics are calculated by using fuzzy logic. The crux of the paper is to preserve the security of the network and provide effective routing decision [14]. The node's trust in the network is calculated using fuzzy logic. Paper presents some information on basic trust models, trust evaluation methods and types of attacks ad-hoc network is prone to. Fuzzy logic rules prediction is used to predict updated trust value of node and entropy mechanism based fuzzy AHP theory to weight the decision factors. However environmental factors are not considered as trust calculation metric.

V. Ram Prabha et.al. 2017 A fuzzy based trust model is proposed for improving malicious node detection accuracy in wireless sensor networks [9]. Mamdani fuzzy member function is used which computes the final trust value as low (l), medium (m) or high (h). The initial multi- valued trust undergoes fuzzification. Two kind of trust models are considered, communication behaviour trust (CBT) and social behaviour trust (SBT). These two models computes trust on the basis of multi attribute trust metric which are message success rate (MSR), elapsed time at node (ET), correctness and fairness (CF) and fed to fuzzy base where these values undergoes fuzzy process and finally fuzzy output is combined to give final trust value to find whether the node is active node of network or not.

I. Maarouf et.al. 2009 A reputation based system implements a new monitoring mechanism called an efficient monitoring procedure in a reputation system (EMPIRE) [4], is proposed for the better trust aware routing. Reputation system works under 3 phases, monitoring rating and response. The sensor nodes are in either ON or OFF state. Therefore, only the ON state nodes undergo monitoring. Rating evaluates the amount of risk associated with the routing through the observed node. The risk obtained is proportional to the malicious behaviour of node in the past. Finally, the response is decision to choose next hop for routing, which is based on risk, energy and distance values.

Nathan Lewis et.al. 2008 authors enhanced the existing trust models for the mobile sensor network. The existing models [20] are based on neighbour's trust and node reputation, hence called Efficient Reputation based Routing Mechanism [13] (ERRM). The test case was performed to check how mobility affects the trust values and hence decision if choosing secure route. The network functionality is tested in the hostile node environment as well.

Riaz Ahmed Shaikh et.al. 2006 have proposed a novel group based trust protocol for distributed wireless sensor networks. Lightweight Group Trust Management Scheme [18] (GTMS) is given for the grouped or clustered networks, in which a single trust value is assigned or calculated for a group. The method provides protection against reputation and data attacks but is vulnerable to denial of service attack.

Hosam A. Rahhal et.al. 2011 provided a cross layer based trust model [12] for the security of static wireless sensor networks. Trust Cross Layer Model (TCLM), based on the acknowledgements from data link and network (TCP) layer aims to detect malicious attacking node and provide secure routing. The acknowledgements are used to check the trustworthiness of next hop to find a secure route to the sink node.

X. Anita et.al. 2014 Authors present a secure routing collaborative lightweight trust based protocol (CLT) [7] for wireless sensor networks. A centralized node trust model approach is used. A novel trust based counsellor is employed to monitor the network nodes and warn them if their trust value drops below the threshold value. Also protocol uses both direct and indirect trust values and sliding time window mechanism for evaluating historical trust. Though the protocol provides protection against insider and outsider attacks, it does not a distributed approach of calculating trust and also no provision of monitoring of anonymous node entry in network is made.

3. Qualitative analysis of trust applications in WSN

In WSN concept of trust plays a vital role as it provides security to network in different terms, which are malicious attack detection, secure data aggregation, secure routing and secure node selection. Table 1 provides the comparative analysis of these applications based on

1. Approach they follow
2. Application area
3. Advantages

Table 1 Comparative analysis of applications

Trust Applications	Approach and Sub Approach	Appliance Area	Advantages	Disadvantages
Malicious Attack Detection	Node Trust Approach Fuzzy logic Probability Theory Weighting and fuzzy logic Weighting and probability theory Reputation System	Hostile and militant work areas	1. Efficient data detection of malicious node. 2. Fuzzy deduction reduces uncertainty of data. 3. Preciseness of trust computation is assured.	1. Vulnerable to data forwarding attacks. 2. Chances of power loss of nodes in large networks.
Secure Data Aggregation	Data Trust Approach Weighting Beta Trust System	Medical field, Military or battlefields	1. Follows both centralized and distributed data aggregation way as per requirement. 2. Minimizes number of transmissions hence saves node's energy.	1. Vulnerable to data collision attacks. 2. Malicious attackers are not paid attention. 3. Trust value updating is done rarely.
Secure Node Selection	Node Trust Approach Fuzzy Logic Hierarchical and behavioural trust	Cluster based sensor networks.	Separation of malicious node make selection of secure and trusted cluster heads.	Process of selecting trusted head is power consuming.

Comparison of surveyed secure routing methods

Table 2: Comparison of routing schemes

Trust Protocol	Approach	Advantages	Disadvantages	Complexity
EMPIRE	Partial use of reputation system	Monitoring activities are reduced.	Forwarding attacks are not considered.	Managing ON and OFF status of sensors.
ERRM	Weighting	Effect of malicious nodes is prevented.	More power consumption in practice of finding best path.	Fewer complexes.
TCLM	Beta distribution and beta statistics	Can deal with larger number of hostile nodes.	Scalable only for denser WSN.	Data sensing and monitoring require additional hardware(watchdog)
GTMS	Trust evaluated on the basis of time based past interactions.	Complex computations are less.	Trust mechanism does not consider malicious attacks.	Minimal Complexity

4. Conclusion

Wireless sensor network is an infrastructure less network, which lacks a backbone support for communication. Due to this reason it is vulnerable to different types of network attacks. Trust evaluation techniques are a way of providing protection from insider as well as outsider attacks. Based on the techniques, trust plays its role in various form of applications. Those applications are malicious attack detection, secure data aggregation, secure routing and secure node selection. Each of the applications can be used on an individual level or in combination with other one. The analysis reveals that most of the trust applications are node trust based; less focus is given on data trust. Also trust evaluation process did not consider performance factors like delay and transmission power.

References

[1] Z. Ye, T. Wen, Z. Liu, X. Song, and C. Fu, "An Efficient Dynamic Trust Evaluation Model for Wireless Sensor Networks," J. Sensors, vol. 2017, pp. 1–16, Oct. 2017.

[2] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," IEEE Commun. Surv. Tutorials Tutorials, vol. 13, no. 4, pp. 562–583, 2011.

[3] Y. Liu and C. L. Q. Zeng, "Improved trust management based on the strength of ties for secure data aggregation in wireless sensor networks," Telecommun. Syst., 2015.

[4] I. M. U. B. A. R. Naseer, "Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks," vol. 3, no. May 2008, pp. 846–858, 2009.

[5] T. Zahariadis, P. Trakadas, H. C. Leligou, and S. Maniatis, "A Novel Trust-Aware Geographical Routing Scheme for Wireless Sensor Networks," pp. 805–826, 2013.

[6] S. Ozdemir, "Functional Reputation Based Data Aggregation for Wireless Sensor Networks," pp. 592–597, 2008.

[7] X. A. M. A. Bhagyaveni and J. M. Leo, "for Wireless Sensor Networks," pp. 117–140, 2015.

[8] A. Ahmed, K. A. B. U. Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "3.A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks," Front. Comput. Sci., vol. 9, no. 2, pp. 280–296, 2015.

[9] K. P. Rama Prabha and N. Jeyanthi, "A Trust and Fuzzy Cluster Based Dynamic Secure Routing Algorithm for Mobile Ad Hoc Networks," Wirel. Pers. Commun., vol. 98, no. 3, pp. 2959–2974, 2018.

[10] I. Chlamtac, M. Conti, and J. J. N. Liu, "Mobile ad hoc networking: Imperatives and challenges," Ad Hoc Networks, vol. 1, no. 1, pp. 13–64, 2003.

[11] M. Ma and Y. Yang, "SenCar: An Energy-Efficient Data Gathering Mechanism for Large-Scale Multihop Sensor Networks," IEEE Trans. Parallel Distrib. Syst., vol. 18, no. 10, pp. 1476–1488, Oct. 2007.

[12] H. A. Rahhal, I. A. Ali, and S. I. Shaheen, "A novel Trust-Based Cross-Layer Model for Wireless Sensor Networks," in 2011 28th National Radio Science Conference (NRSC), 2011, pp. 1–10.

[13] N. Lewis and N. Foukia, "An Efficient Reputation-Based Routing Mechanism for Wireless Sensor Networks: Testing the Impact of Mobility and Hostile Nodes," in 2008 Sixth Annual Conference on Privacy, Security and Trust, 2008, pp. 151–155.

[14] H. Xia, E. H.-M. Sha, and Z. Jia, "Research of trust model based on fuzzy theory in mobile ad hoc networks," IET Inf. Secur., vol. 8, no. 2, pp. 88–103, 2014.

[15] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," IEEE Trans. Netw. Serv. Manag., vol. 9, no. 2, pp. 169–183, Jun. 2012.

[16] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," J. Netw. Comput. Appl., vol. 35, no. 3, pp. 867–880, May 2012.

[17] G. Han, J. Jiang, L. Shu, J. Niu, and H. Chao, "Journal of Computer and System Sciences Management and applications of trust in Wireless Sensor Networks : A survey," J. Comput. Syst. Sci., vol. 80, no. 3, pp. 602–617, 2014.

[18] R. A. Shaikh, H. Jameel, Sungyoung Lee, S. Rajput, and Young Jae Song, "Trust Management Problem in Distributed Wireless Sensor Networks," in 12th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'06), 2006, pp. 411–414.

[19] M. R. Ahmed, X. Huang, D. Sharma, and H. Cui, "Wireless Sensor Network: Characteeristics and Architectures," vol. 6, no. 12, pp. 1398–1401, 2012.

[20] N. Lewis and N. Foukia, "An Efficient Reputation-Based Routing Mechanism for Wireless Sensor Networks: Testing the Impact of Mobility and Hostile Nodes," in 2008 Sixth Annual Conference on Privacy, Security and Trust, 2008, pp. 151–155.

[21] Murthy, C. Siva Ram, B.S. Manoj (2004): Ad Hoc Wireless networks Architecture and Protocols. South Africa: Pearson Education.

[22] https://wirelessmeshsensornetworks.wordpress.com/2014/02/18/characteristics-of-a-wireless-sensor-networks/

Radhika Gupta has received the degree of Bachelor of Engineering (B.E.) in Computer Engineering and currently is a student of Master of Technology (M.Tech) in Computer Science and Engineering in Lovely Professional University.

Dr. Kavita received the degree of Bachelor of Technology (B.Tech) in Computer Science and Engineering, Master of Technology(M. Tech) in Computer Science and ing ,and Ph.D in Computer Science and Engineering. She is working as an Assistant Professor in Lovely Professional University in the Department of Computer Science and Engineering. She has more than 40 publications in international journals and attended 4 international conferences. She is an editorial board member of 7 international journals.

Dr. S. Verma received the degree of Bachelor of Technology (B.Tech) in Computer Science and Engineering, Master of Technology(M. Tech) in Computer Science and Engineering and doctorate in Computer Science and Engineering .Currently, he is working as an Assistant Professor in Lovely Professional University in the Department of Computer Science and Engineering. He has more than 50 publications in international journals and attended 6 international conferences. He is an editorial board member of 11 international journals and has guided 12 students of M.Tech.