SEEDI: Secure and Energy Efficient Approach for Detection of an Intruder in Homogeneous Wireless Sensor Networks

Article *in* International Journal of Computer Theory and Engineering · January 2010

DOI: 10.7763/IJCTE.2012.V4.597

CITATIONS
2

READS
40

6 authors, including:

K. Shaila
Vivekananda Institute of Technology, Bangalore
109 PUBLICATIONS **231** CITATIONS
SEE PROFILE

SH Manjula
UVCE, Bangalore University
94 PUBLICATIONS **201** CITATIONS
SEE PROFILE

Venugopal K R
University Visvesvaraya College of Engineering
925 PUBLICATIONS **3,707** CITATIONS
SEE PROFILE

Lalit M Patnaik
Indian Institute of Science
838 PUBLICATIONS **8,678** CITATIONS
SEE PROFILE

SEEDI: Secure and Energy Efficient Approach for Detection of an Intruder in Homogeneous Wireless Sensor Networks

K. Shaila, M. Sajitha, V. Tejaswi, S. H. Manjula, K. R. Venugopal, and L. M. Patnaik

***Abstract*—Wireless Sensor Networks consists of tiny devices which processes and routes the sensed data. The process of detecting any external and internal intruders entering to a Wireless Sensor Network area is referred to as intrusion detection. An intruder is a moving attacker entering a particular area. In this paper, we propose an algorithm Secure and Energy Efficient Approach for Detection of Intruder (SEEDI) in homogeneous Wireless Sensor Networks. Single sensing and Multi-sensing intruder detection are considered in our algorithm. Simulation results showed that the proposed algorithm resulted in better performance.**

***Index Terms*—Intrusion detection, node density, sensing range, transmission range, wireless sensor network.**

I. Introduction

Wireless Sensor Network (WSN) is a collection of large number of sensor nodes which are deployed in spatial environment. These nodes are capable of sensing any of the physical or environmental conditions. WSNs are widely used in military applications such as in borders for finding out the infiltrations, industrial process monitoring and control, healthcare applications etc.. Sensor nodes perform sensing, data processing and communication with limited resources like power, computational capabilities, memory size and low bandwidth. Therefore, utmost care has to be taken while constructing the networks under these constraints. Energy is vital for many applications in WSNs since it is impossible to recharge the deployed nodes. One approach is to put some sensor nodes in sleep mode and wake them up when required to save energy.

Sensors are deployed in a variety of domains and many applications should be secure from attacks. A lot of security protocols or mechanisms have been designed for sensor networks. For example, SPINS (Sensor Protocol for Information via Negotiation), a set of protocols, provides secure data confidentiality, two-party data authentication, data freshness and authenticated broadcast for sensor network [1]. Localized Encryption and Authentication Protocol (LEAP), is designed to support in-network processing based on different security requirements for different types of message exchange [2].

Manuscript received August 14, 2012; revised September 26, 2012.

K. Shaila, M. Sajitha, V. Tejaswi, S. H. Manjula, and K. R. Venugopal are with the Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore 560 001

L. M. Patnaik is with the Honorary Professor, Indian Institute of Science, Bangalore, India (e-mail: shailak17@gmail.com)

INSENS is an intrusion tolerant routing protocol for WSNs [3]. Security solutions in the network are divided into two categories: *prevention* and *detection*. Prevention techniques, such as encryption, authentication, etc., are used to prevent attacks from outside. These preventive measures reduce the chance of intrusion, but are not able to eliminate the intrusion completely. Intrusion detection is essential to achieve longer lifetime and defend the network security by the intruders.

In WSNs, if preventive measures fail, the network can identify and resist the attacks by means of intrusion detection techniques. Thus, Intrusion Detection Systems (IDSs) are important for the security of networks. IDSs are defined as a monitoring system for detecting any malicious intruder that invades the network domain [4]-[6]. Detecting a moving intruder is a crucial application in WSNs. Intrusion detection is defined as the first contact time when the intruder hits the sensing range of a sensor belonging to large sensor cluster.

Motivation: In WSN clustering, energy utilization, routing, data aggregation, multimedia, collaborative processing, security etc., are related to each other. Whatever be the application, if WSN formed is not secure from external and internal attacks then the entire effort of data transmission is lost. There are two types of attacks: *external* and *internal*. External attacks may change the nodes to become malicious which results in abnormal behavior. So it is very important to identify the external attacks that occur in WSN.

Contribution: In his paper, we have developed SEEDI algorithm that handles internal intrusion detection and energy consumption for intrusion detection process. The internal intrusion detection includes the analysis of data sent by each node. The algorithm proposed is used for internal data analysis; it selects a set of nodes among the entire nodes and activates its IDS module. Related work is discussed in Section 2, System Model and Problem Definition in Section 3. The implementation and algorithm is discussed in Section 4, Mathematical analysis in Section 5, Simulation results are given in Section 6 and Conclusions in Section 7.

II. Related Work

Zhang et al., [7] studied the problem of intrusion detection in Wireless Ad-hoc Networks. They have proposed architecture for distributed and cooperative intrusion detection system for Ad-hoc Networks, which was based on statistical anomaly detection techniques which requires much time to detect intrusion in data and during traffic. Liu et al., [8] have explored the effects of sensor mobility on sensing, coverage and detection capability in a mobile WSN. Wang et

al., [4] have provided a unifying approach in relating the intrusion detection probability with respect to the intrusion distance and the network parameters (i.*e.*, node density, sensing range and transmission range) under single-sensing detection and multiple-sensing detection models, in both homogeneous and heterogeneous WSNs assuming a straight line or linear motion intrusion path for an intruder.

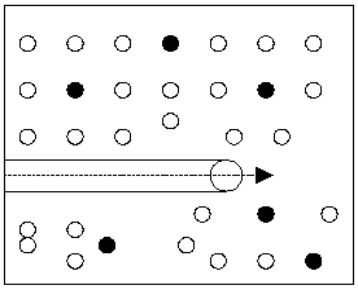

Fig. 1. Intruder moving in straight path.

Yun et al., [9] proposed a novel probabilistic sine-curve mobility model to explore the effects of different intrusion paths using single-sensing and *k*-sensing detections in a given WSN. For intrusion detection of an object, the detection probability is determined by the object size, the number of sensors, sensing radius, the number of subsets and the size of the monitored region.

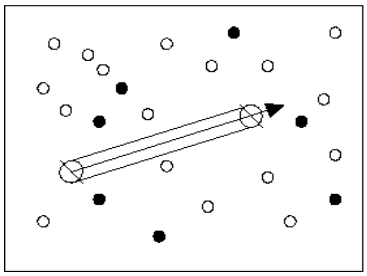

Fig. 2. Intruder dropped from air.

III. System Model And Problem Definition

A. Network Model

Consider a homogeneous WSN in a two-dimensional (2D) plane with N sensors, denoted by a set $N = (n_1, n_2, n_3 \ldots n_n)$, where, n_i is the i^{th} sensor. These sensors are uniformly and independently deployed in an area $A = L \times L$ which results in a 2D Poisson point distribution of sensors. The sensors deployed in WSN are static. In a homogeneous WSN, each sensor has the same sensing radius of r_s, the transmission range r_x and node density λ. A sensor can only sense the intruder within its sensing area *i.e.*, a disk with radius r_s centered at the sensor.

In a WSN, a point is said to be covered by a sensor if it is located in the sensing range of any sensor(s). The WSN is divided into two regions, the covered region, which is the union of all sensor coverage disk and the uncovered region, which is the complement of the covered region within the area of interest *A*. We have assumed that the sensing coverage area is not known to the intruder. Consider an intruder moving from the boundary as shown in Figure 1, the distance moved by the intruder is *D*. The intruder is detected only, when there is a sensor in the area moved by the intruder. The intruder can move through a straight line or through a curved path. It follows a straight path only when it knows the exact destination, otherwise it follows a curved path. In this paper, we are considering only straight path. The area moved by the intruder is,

$$S = 2 \times D \times r_s + \pi r_s^2 / 2 \quad (1)$$

If the intruder is entering the WSN area from a random point, *i.e.*, the intruder is dropped from the air, then the area moved by the intruder is shown in Figure 2 and is given by,

$$S = 2 \times D \times r_s + \pi r_s^2 \quad (2)$$

Intrusion detection is defined as a mechanism for WSNs to detect the existence of inappropriate, incorrect or anomalous moving attackers. For example, while detecting an intruder in the battlefield. For this purpose, it is a fundamental issue to characterize node density and sensing range of WSN interms of a desirable detection probability [4]. Intrusion detection modules on sensor nodes try to detect the malicious action which occurs within its radio range. The monitoring technique (like watchdog, local monitoring) relies on the broadcast nature of sensor communication and takes advantage of high density sensors deployed in the sensing environment. The sensor nodes activate the intrusion detection modules called *monitor* nodes.

B. Problem Definition

The life span of WSN is directly dependent on the power. The power required to transfer data from a sensor is more compared to its internal processing. All sensors are performing the intrusion detection and passing this information to base station may cause unnecessary usage of power. It is better to activate only few sensors within a region of WSN at a time for intrusion detection. So, battery power of each sensor can be saved and this increases the WSN life span. There are limited external and internal intrusion detection techniques and no algorithm supports random detection of intruders.

C. Assumptions

Consider static sensors and intruder as a moving object. Each node has omni-antenna properties for sensing. The sink node knows each nodes location and its neighbor list. The algorithm is executed at the sink node and it sends a packet to the selected node to activate its IDS module.

IV. Intrusion Detection in Homogeneous WSNs

In this paper, an Intruder is defined as any moving object that enters into the WSN area. We have derived the detection probability for single-sensing and multi-sensing detection.

A. Implementation and Algorithm

Let *n* be the minimum number of sensors required to cover the network area. The minimum number of sensors participating in intrusion detection is equal to the minimum number of sensors required to cover the WSN area. Intrusion detection module performs two functions: (*i)* finding the intruder, (*ii*) passing the information to the base station. The SEEDI algorithm in Phase I determine the minimum number of sensors required to cover the area depending on both

sensing range and transmission range as shown in Table I. The SEEDI algorithm in Phase II determines the number of nodes required to perform intrusion detection is atleast *n* as shown in Phase II.

TABLE I: SECURE AND ENERGY EFFICIENT APPROACH FOR DETECTION OF AN INTRUDER (SEEDI) ALGORITHM

Phase I
MinNode(t_r,r_s)
{
if t_r >= r_s then
n $\prod r^2_s \equiv kmodL2$
where k = {0 to $\prod r^2_s$*-1}*
if t_r < r_s
$\equiv kmodL2$
$n\prod t_r2$
where k = {0 to $\prod t_r2$*-1}*
}
Phase II : At sink node
{
Assign U = {R} the set of nodes in the WSN area.
Let N(i) is the set of neighbors of node i. repeat
If N(i) ≠ Ø
Find min N(i)
Put i in Stack;
I={a / the distance between i and N(i) < (r_s/2)}
if N(i) > 1;
U = U - [i U I];
else
U = U - I;
Until U is Null
}

V. MATHEMATICAL ANALYSIS

A. Single Sensing Detection Model

An intruder is detected when it enters the sensing range of a sensor. When the intruder enters the area through the boundary and if the sensors are available, then the intruder is detected as soon as it enters the WSN area. Otherwise, it has to move a certain distance *D* before being detected by any of the sensors. The intruder is detected within the radius r_s of the circle around the sensor as shown in Fig. 3.

When the intruder starts from a point on the network boundary, as shown in Figure 1 and if intrusion distance $D > 0$, the corresponding intrusion detection area *A* is almost an oblong area. The area includes a rectangle of length *D* and a half circle of radius r_s and the area is,

$$A=2r_s D+ \pi r^2_s/2 \quad (3)$$

According to the definition of single-sensing detection, the intruder is detected if and only if there exist atleast one sensor within this area *A. i.e.*, the intruder is detected if it comes in the sensing range of any of the sensors, else the intruder is not detected. Similarly, when the intruder starts from a random point in the network domain, the corresponding intrusion detection area is given by equation (4). The sensing area includes two half circles and that of the rectangle. The radius of the circle is r_s and the length of the rectangle is *D*.

$$A=2\ r_s D+ \pi r^2_s \quad (4)$$

Initially, assume that the intruder starts from the boundary of the network.

Theorem 1: The probability *P(D)* indicates that an intruder can be immediately detected once it enters a homogeneous WSN with node density λ and identical sensing range *r*. *P(D)* is given by,

$$P(D=0) = 1\text{-}e^{-n}$$

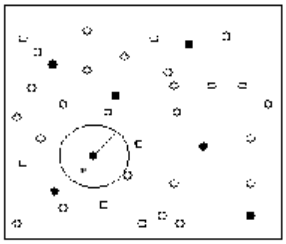

Fig. 3. Intrusion detection by single sensor.

Proof: According to Poisson distribution.

$$z\ P(m,A) = (A\lambda)me^{-A\lambda}/m! \quad (5)$$

where, *m* is the number of sensors, *A* is the area, λ is the probability of sensors responsible for intrusion detection. In this paper, only n_1 sensors are performing intrusion detection at a time. So $\lambda = n_1/A$. If there are no sensors in the area *A*, then the probability is equal to $P(0, A) = e\text{-}A\ \lambda$.

Based on complement of the probability, the probability that there is atleast one sensor in the area *A* and the intruder is detected by any of these sensors is,

$$1\text{-}P(0, A) = 1\text{-}e^{-n}{}_1 \quad (6)$$

Hence the theorem is proved.

Theorem 2: Suppose η is the maximal intrusion distance allowable for a given application, then the probability *P(D)* that the intruder can be detected within η in the given homogeneous WSN can be derived as,

$$P(D\leq\ \eta)=1\text{-}e^{-n}{}_2 \quad (7)$$

where, n_2 is the number of sensors participating in intrusion detection.

Proof : The volume moved by the intruder is,

$$A=2\pi r_s + \pi r^2_s/2 \quad (8)$$

So, if there is no sensor in that area, then the probability of detection is $P(0, A)$, then complement of $P(0, A)$ will give the probability of detecting intruder within the distance η.

B. Multi-Sensing Detection Model

Some applications require more than one sensor information about the intruder, *i.e.*, the case of finding intruder position. In this case we need the intruder to be detected only when it is within a sensing range of *K* sensors as shown in Fig. 4.

Theorem 3: Let $P_m(D = 0)$ be the probability that an intruder is detected immediately once it enters a WSN with node density λ and sensing range r_s in multi-sensing detection model. Then $P_m(D = 0)$ is given by,

$$P_m\left(D=0\right)=\sum_{i=0}^{m-1} e^{-n_i}$$

Theorem 3: Let $P_m(D = 0)$ be the probability that an intruder is detected immediately once it enters a WSN with node density λ and sensing range r_s in multi-sensing detection model. Then $P_m(D = 0)$ is given by,

$$P_m\left(D=0\right)=\sum_{i=1}^{m-1}e^{-n_1}$$

where n_1 is the number of selected sensors within the area

$$A=\pi r_s^2/2.$$

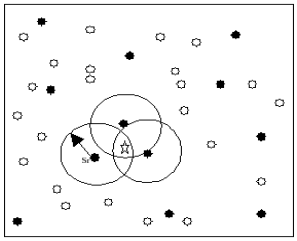

Fig. 4. Intrusion detection by multiple sensors.

where n_1 is the number of selected sensors within the area

$$A=\pi r_s^2/2.$$

Proof: This theorem can be proved based on Poisson distribution. The area is only one half circles with radius r_s. $P(i, A)$ gives the probability of detecting the intruder with i sensors. $\sum_{i=0}^{m-1}P(i,A)$ give the sum of the probabilities of detecting the intruder with less than m sensors. So, the complement will be the multi- sensing probability. The analysis for intruder detection less than maximum allowable distance can also be determined as in Theorem 2.

VI. Simulation and Verification

Our analytical results are verified through simulation using MATLAB for single-sensing and multi- sensing detection models in WSN. The simulation was carried out using 500 sensors which were uniformly distributed in a square network domain. The sensors are uniformly distributed in a two dimensional space of 1000×1000 meters. The node density is set as λ = 0. 0005 per square meter. The sensing range is varied from 0 to 50 meters and maximal allowable intrusion distance is 50 meters. The simulation results are obtained by changing node parameters such as density, transmission range and sensing range. The intruder is allowed to move through the WSN area starting from any point. Monte-Carlo simulation is performed and each data point shown in Figure is the average of the simulation results. The analytical results are calculated by using the Theorems 1, 2 and 3. For successive simulation runs, the sensors are uniformly redistributed in the network domain.

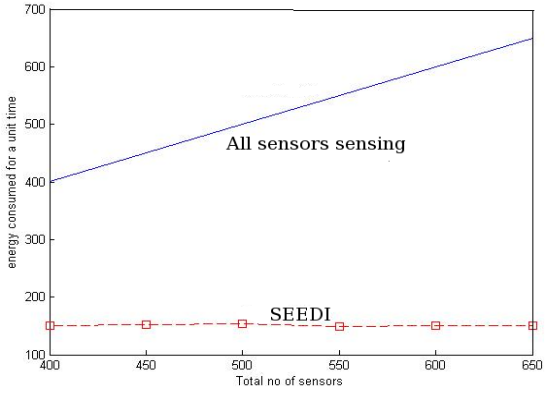

Fig. 5. Sensing range and probability of detection.

The simulation results show the detection probability. It is found that the detection probability remains same as in the case of analytical results, thus proving the correctness of the analytical model. Single-Sensing Detection probability and Multi-Sensing Detection probability is shown in Fig. 5. It shows that Single Sensing Detection probability is higher than that of Multi-Sensing Detection probability. This is because Multi-Sensing Detection impose a stricter requirement on detecting the intruder (*i.e.*, atleast 3 sensors are required).

The graph is obtained by changing the sensing range from 0 to 40. Each point in the graph is a result of 100 simulations. *i.e.*, to get each point we need to execute our simulation and find out the probability from the result of 100 executions. Here we can see that single sensing is possible at lower ranges also. But multi-sensing takes time to get the results, since it requires more than one sensor (in this simulation three sensor information were considered) information to detect the intruder.

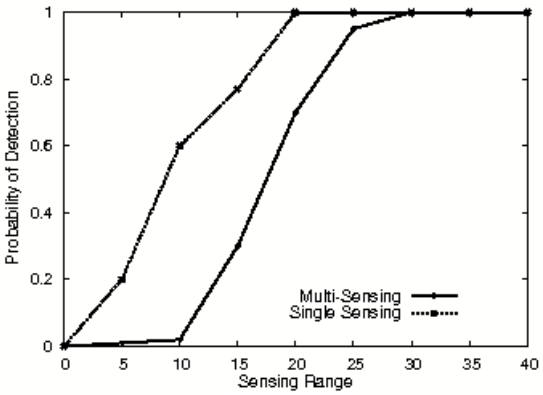

Fig. 6. Number of nodes activated by the ids module.

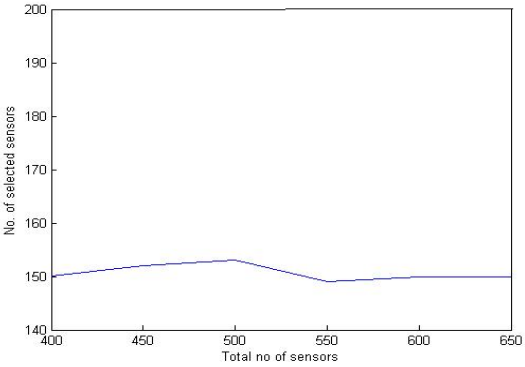

Fig. 7. Energy consumption vs. total number of sensors.

Fig. 6 demonstrates the average number of nodes selected by using SEEDI algorithm. The density of nodes is varied to check how many nodes are activating its IDS module. From the graph it is evident that even if the density of nodes in the area increases the number of nodes selected for intrusion detection remains within a small range. In order to plot the graph the sensing range and transmission range is fixed to 45 and the density is varied. The energy consumption by the network using SEEDI algorithm is analyzed in the Fig. 7. The assumption made is that the energy used by one node for a unit time is one unit. The results show that the energy consumption is less compared to the previous work.

VII. Conclusions

In this paper, the external intrusion detection is minimized in an energy efficient way and probability of space. This probability gives an insight into the required number of sensors in a given deployment, their sensing and transmission range to securely detect an intruder in a WSN. We have developed an analytical model for intrusion detection and applied the same into single-sensing detection scenarios for homogeneous WSNs. The correctness of the analytical model is proved by simulation.

References

[1] A. Perrig, S. Robert, W. Victor, C. David, and J. D. Tygar, "SPINS: Security protocols for sensor networks," in *Wireless Networks*, vol. 8, no. 5, pp. 521- 534, 2002.

[2] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03)*, 2003, pp. 62-72.

[3] J. Deng, R. Han, and S. Mishra, "A performance evaluation of intrusion tolerant routing in wireless sensor networks," in *Proceedings of The Second International IEEE Workshop on Information Processing in Sensor Networks (IPSN'03)*, 2003.

[4] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks," in *Proceedings of IEEE Transactions on Mobile Computing*, vol. 7, no. 6, pp. 698-711, 2008.

[5] H. Kung and D. Vlah, "Efficient location tracking using sensor networks," in *Proceedings of IEEE Wireless Communications and Networking Conference*, 2003, vol. 3, no. 3, pp. 1954– 1961.

[6] C. Y. Lin, W. C. Peng, and Y. C. Tseng, "Efficient in-network moving object tracking in wireless sensor networks," in *Proceedings of IEEE Transactions on Mobile Computing*, 2006, vol. 5, no. 8, pp. 1044–1056.

[7] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proceedings of ACM MobiCom*, 2000, pp. 275-283.

[8] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility improves coverage of sensor networks," in *Proceedings of The Sixth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2005.

[9] Y. Wang, Y. K. Leow, and J. Yin, "Is straight-line path always the best for intrusion detection in wireless sensor networks," in *Proceedings of Fifteenth International Conference on Parallel and Distributed Systems*, 2009, pp. 564-571.

K. Shaila is an Associate Professor and Head in the Department of Electronics and Communication Engineering at Vivekananda Institute of Technology, Bangalore, India. She obtained her B.E and M.E degrees in Electronics and Communication Engineering from Bangalore University, Bangalore. She is presently pursuing her Ph.D programme in the area of Wireless Sensor Networks in Bangalore University. Her research interest is in the area of Sensor Networks, Adhoc Networks and Image Processing.

M. Sajitha received Master of Engineering in Computer Science from University Visvesvaraya College of Engineering, Bangalore University. Her research interest is in the area of Wireless Sensor Networks.

V. Tejaswi is a student of Computer Science and Engineering from Rastriya Vidayala College of Engineering, Bangalore. Her research interest is in the area of Wireless Sensor Networks.

S. H. Manjula received Bachelor of Engineering in Computer Science and Master of Engineering in Computer Science from University Visvesvaraya College of Engineering, Bangalore University, Bangalore and Ph.D from Dr. M G R University, Chennai. She is working as Associate Professor in the Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. Her research interest includes Wireless Sensor Networks.

K. R. Venugopal is currently the Principal, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science Bangalore. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored 31 books on Computer Science and Economics, which includes Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ and Digital Circuits and Systems etc. During his three decades of service at UVCE he has over 250 research papers to his credit. His research interests include Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining.

L. M. Patnaik is an Honorary Professor, Indian Institute of Science, Bangalore. He was Vice Chancellor in Defense Institute of Advanced Technology, Pune, India. He was a Professor since 1986 with the Department of Computer Science and Automation, Indian Institute of Science, Bangalore. During the past 35 years of his service at the Institute he has over 700 research publications in refereed International Journals and refereed International Conference Proceedings. He is a Fellow of all the four leading Science and Engineering Academies in India; Fellow of the IEEE and the Academy of Science for the Developing World. He has received twenty national and international awards; notable among them is the IEEE Technical Achievement Award for his significant contributions to High Performance Computing and Soft Computing. His areas of research interest have been Parallel and Distributed Computing, Mobile Computing, CAD for VLSI Circuits, Soft Computing and Computational Neuroscience.