ATMC: Anonymity and Trust Management Scheme Applied to Clustered Wireless Sensor Networks

Shaila K[1*], Sivasankari H[1], S H Manjula[1], Venugopal K R[1] and L M Patnaik [2]
[1*]Department of Computer Engineering, University Visvesvaraya College of Engineering,
Bangalore University, Bangalore, India
E-mail: shailak17@gmail.com
[2]Honorary Professor, Indian Institute of Science, Bangalore, India

***Abstract*—Wireless Sensor Networks consists of sensor nodes that are capable of sensing the information and maintaining security. In this paper, an Anonymity and Trust Management Scheme applied to Clustered Wireless Sensor Networks (ATMC) is proposed which enhances the security level. It also provides a stable path for communication. It is observed that the performance of the network is better than existing schemes through simulation**.

***Index Terms*— Anonymity, Cluster head, Trust value, subrange values, Wireless Sensor Networks**

I. Introduction

Wireless Sensor Network (WSNs) consists of a large number of tiny sensor nodes that are equipped with sensing, processing and communicating components. WSNs applications include target tracking in battle field and environmental monitoring etc.. Sensor networks face many security challenges because of their inherent limitations in their energy, computation and communication capabilities. The deployment nature of sensor networks makes them more vulnerable to various attacks. Sensor networks are deployed in unattended and physically insecure environment, presenting the added risk of physical attack. Thus, providing security to WSNs becomes very important.

Traditionally, cryptography and authentication approach are used to provide security. Conventional approach of providing security is not sufficient for autonomous network, so trust based approaches are used for providing security to the network. In order to evaluate the trustworthiness it is essential to establish the co-operation and trust between sensor nodes. Group-based Trust Management Scheme [1] uses Hybrid Trust Management and works on two topologies: *intra-group topology* and *inter-group topology*.

Motivation : During processing of data, each node forwards the trust of its neighbors to cluster head upon request. When sink sends request to cluster head, it transmits neighboring clusters trust value to the sink. So, there is a possibility of adversary performing traffic analysis during the communication between sensor nodes.

Hence, security level has to be enhanced by incorporating identity anonymity feature to the existing Group-based Trust Management Scheme.

Contribution : In this paper, we have proposed an Anonymity based Trust Management algorithm to establish and maintain trust values between communicating sensor nodes. In identity anonymity, identity of the sensor nodes is hidden from the compromised sensor nodes while calculating the trust values. The adversary cannot predict other subranges of the sensor node and hence enhances the security in WSNs.

II. Literature Survey

Riaz et al., [2] proposed Group-based Trust Management Scheme which calculates trust for group of sensor nodes in each cluster. It works on intra-group topology using distributed trust management approach and inter-group topology using centralized trust management approach.

Garth et al., [3] have proposed distributed trust-based framework and a mechanism to select the trustworthy cluster head from each cluster. Each node has a watchdog mechanism that allows it to monitor network events of other nodes. Using the information obtained through monitoring, enables the nodes to compute and store trust levels. It uses direct and indirect information coming from trusted nodes. Trust is calculated based on the parameters such as average packet drop rate, data packet and control packet. Each node holds the trust value of all its neighboring nodes and sends trust levels to cluster head upon request. Since trust calculation is not based on second hand information, it reduces effect of bad-mouthing. Further, reputation-based trust framework for WSNs is proposed in [4], which prevents the election of compromised or malicious nodes as cluster heads, through trust based decision making. It describes the secure cluster formation algorithm to establish trusted clusters through pre-distributed keys. It employs Beta distribution function in modeling reputation between two nodes. Reputation and trust is built over time and allow continuation of trusted cluster heads election.

Karthik et al., [5], compares various trust management Techniques for high trust values in WSNs. The trust values are maintained based on the various processes like trust establishment, trust propagation, trust metrics and Group Based Trust Management Schemes. Efthimia et al., [6] propose Certificate-based approach mechanism for deployment knowledge on the trust relationships within a network and Behavior-based trust model views trust as the level of positive cooperation between neighboring nodes in a network.

Krasniewski et al., proposed TIBFIT protocol in [7], which determines event and location in the presence of failure of sensor nodes, coupled with diagnosis and isolation of faulty or malicious nodes. All nodes in the network are grouped

DOI: 01.IJNS.3.4.1092

into clusters with rotating cluster heads. Each node is assigned a trust index at the cluster head, to indicate its track record in reporting past events correctly.

Yu et al., presents a Trustworthiness-Based QoS Routing protocol in [8] for Wireless Ad-hoc Networks. It addresses different issues like secure route discovery, secure route setup and trustworthiness-based Quality of Service routing metrics and presents message exchange mechanism to detect internal attacks. The message redundancy is enforced by sending various copies of same message if the route redundancy does not exist. But there are several other issues not addressed like, the procedure for each node to implement and maintain local certificate repository, building of trust among a node and its neighbors.

Yao et al., [9] propose a Parameterized and Localized Trust Management Scheme (PLUS) for sensor network. Since all the database parameters are to be maintained it requires storage devices. When the keys get compromised there is a possibility of detecting information by the adversary. This can be avoided by introducing anonymity scheme as in [10] [11] so that knowing the virtual information can be avoided. They propose Hashing band ID Randomization and Reverse Hashing ID Randomization and provide anonymity to the nodes.

The efficiency of the WSNs can be improved by filtering the unnecessary messages at every hop as in [12] for heavy networks. They have not specified what happens if a node becomes malicious. There is a possibility of an adversary determining the base station and disrupting it. To overcome this problem in [13] [14] [15] [16] state that the anonymity of the base station has to be maintained by considering multiple sinks. Since mobile sinks are considered, there is a possibility of the hotspots of some particular sink and if the mobile sink is not within the coverage area then the security is less.

III. System Model

Consider a static Wireless Sensor Network consisting of a large number of small devices called sensor nodes. The number of nodes in a sensor network can be of 144 sensors with 600 x 600 nodes, 225 sensors with 800 x 800 nodes and 324 sensors with 1000 x 1000 nodes. Each sensor node has its own ID. The network is divided into number of groups referred to as clusters as shown in Figure 1. Cluster Head (CH) is elected for each cluster, which has more power compared to other members of the cluster. Each sensor node can communicate with all its cluster members directly. Each cluster head communicates with neighboring cluster heads as well as with sink either through intermediate CH or directly.

IV. Problem Definition

Consider a given grid based WSNs, in which nodes are organized in the form of clusters. The trust values are computed and communicated from the nodes to sink through the cluster head. During this process, the adversary performs traffic analysis and alters the trust values. The objective of this work, is to avoid traffic analysis attack.

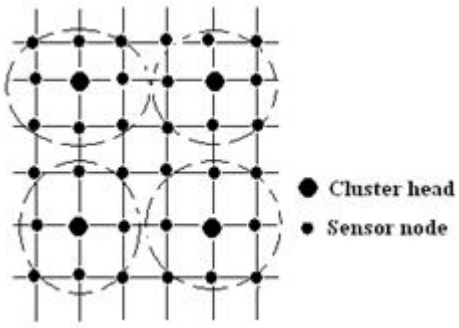

Figure 1. Deployment of Sensor Nodes in Grid Fashion

Assumptions :

(i) Initially all nodes will be in uncertain zone.

(ii) Each node has enough memory to store range of dynamic IDs.

(iii) Sensor nodes have to exchange their ID ranges within a short period, to avoid the nodes compromising with an adversary.

(iv) Adversary cannot attack sink.

V. Algorithm And Implementation

In order to overcome the traffic analysis attack, anonymity of the nodes and trust values are maintained during transmission. Initially, *N* nodes are generated using random function and are arranged in a grid fashion. These nodes are divided into smaller groups called as clusters and they elect their leader called as *Cluster Head* as proposed in Selection of Cluster Head algorithm in Table 1.

These cluster heads communicate with the other cluster heads and the sink. An adversary can track the information being transmitted if it is able to trace the IDs of the sensor nodes. To overcome this problem, identity anonymity is created by dividing the dynamic ID pool into number of subranges of equal size. Each sensor node is given randomly chosen subranges that are overlapping and non-contiguous from ID pool as explained in Assigning Anonymity IDs algorithm in Table 2. Map table is created at each sensor node to map true ID of sensor node with dynamic sender and receiver ID.

The trust of any node indicates its ability to provide the required service. Based on the trust value, the nodes can be categorized as trusted, uncertain or untrusted nodes. If the node is malicious it is categorized as untrusted or uncertain node. Trust value is calculated first at Node level, then at Cluster head level and finally at sink level based on number of successful and unsuccessful interaction between the nodes using sliding window [2] for every *r* iterations. Similarly, the trust values are computed at cluster heads.

The trust values of the cluster members and cluster head is communicated to the sink. Finally, the sink allocates trust values to all the nodes in the network (Table 3). The nodes with values greater than 50 are trusted, while nodes with values less than 50 are untrusted and those with value exactly 50 are termed as uncertain. Next, verify if any past interaction had taken place between the communicating nodes. If there is no past interaction experience then node will go for

DOI: 01.IJNS.3.4.1092

TABLE I. ALGORITHM : SELECTION OF CLUSTER HEADS (SCH).

```
Begin: Algorithm SCH
Generate: N nodes using rnd function.
 for i=0:Ti:N do
  for j=0:Ti:N do
   Assign the nodes in grid pattern.
     if(n(i).neigh(1, 1))then
       Form Clusters of p nodes each.
     endif;
   endfor;
 endfor;

 for i=Ti:p:N do
  for j=Ti:p:N do
   for k=1:nd
    if(n(k).x==i)&&(n(k).y==j) then
        Elect the Cluster Head
    endif;
   endfor;
  endfor;
 endfor;
end;
```

TABLE II. ALGORITHM : ASSIGNING ANONYMITY IDS (AAI)

```
Begin: Algorithm AAI
 for i=1:nd x number of nodes in cluster.
     Calculate the anonymity IDs.
 endfor;
  for k=1: nd;
    for i=1:length(n(k).neigh)
      Create map table-determine subrange IDs
      of sender and receiver.
    endfor;
   endfor;
 for i=Ti:p:N do
  for j=Ti:p:N do
   for k=1: nd
     if(n(k).x==i)&&(n(k).y==j) then
       Randomly assign subrange IDs from
       map table to sender and receiver.
     endif;
    endfor;
   endfor;
 endfor;
end;
```

peer recommendation evaluation. Here, the node takes recommendation from trusted and uncertain nodes. So, malicious nodes cannot send false recommendation to trusted nodes. The sender and receiver in different cluster head receive the trust value through the sink. Cluster heads and its trust values are changed after every *r* iterations (Table 4, ATMC Algorithm).

VI. SIMULATION AND PERFORMANCE EVALUATION

The simulation is performed using MATLAB. Static sensor nodes organized in grid fashion are deployed in 1000m x 1000m area and the distance between the node is 50m. Cluster size in each network is equal, which consists of σ nodes. Each network comprises of one sink located at the middle of the terrain. Maximum trust value of the node is 100. Initially, all sensor nodes are in uncertain state, i.e., the trust value is 50. Let the average size of the cluster be σ and the number of nodes in the network be *N*. So the total size of the dynamic ID pool should be *N**σ. Each sensor has got equal number of

TABLE III. ALGORITHM : CALCULATION OF TRUST VALUES (CTV)

```
Begin: Algorithm CTV
 k=find(n(i).sw(:, 14)==2);
   if ~ isempty(k)
     for l=1:length(k);
       Calculate average trust values using
           n(i).h=(SM/2)*length(k));
     endfor;
   else
     k=find(n(i).sw(:, 14)==0);
      if ~ is empty(k)
        for l=1:length(k);
          Calculate average of 1/2nd of all untrustful
          node using (n(i).g=[1-n(i).h]/2_length(k));
        endfor;
      endif;
   endif;
  for j=1:length(n(i).sw(:, 1))
    if (100-h d" trust value d" 100) then
      node is trusted; so assign trust state.
    else
      node is uncertain or untrustful.
        Check if any past interaction occurred
       between node i and j, then node i takes
        peer recommendation about node j.
    endif;
  endfor;
end;
```

TABLE IV. ALGORITHM : ANONYMITY TRUST MANAGEMENT SCHEME FOR CLUSTERED WSNS (ATMC)

```
Begin: Algorithm ATMC
input: global nd, N, M, i1=k2, j1, k1,a, r, u, h, hi, p,  SM=0,
d=0, w=0;
initialize : trust value of each sensor node.

Set Ti=50, k=1, initial=0;
begin
  for (a = 1 to r)
     Phase 1: Call Algorithm SCH;
     Phase 2: Call Algorithm AAI;
   for j=1:length(n(i) : sw(:, 1))
     if j=~rd(i) then
        move the window using
            (100*S2)/(S + U)*(S+1);
     endif;
    endfor;

    Aggregate the trust values from all its neighbors
    and store in matrix form.
      Phase 3: Call Algorithm CTV;
        hi=find(n(i).neigh(:, 2)==1);
      if (j=~hi cluster head row) then
          assign trust value to the nodes.
      else
          assign trust value to cluster head.
      endif;
  endfor;
end;
```


DOI: 01.IJNS.3.4.1092

neighboring nodes of size σ-1. Each sensor node randomly selects σ-1 subranges from the ID pool and cluster head selects σ subranges to communicate with its cluster members and as well as neighboring cluster heads. When node receives any packet, its sender ID is compared with receiver ID in the Map table. Compute dynamic subrange IDs and consider only the integer values. The random assignment of IDs to the nodes is clearly illustrated in Table 5.

TABLE V. MAP TABLE: DYNAMIC ID RANGE FOR NODE 1

Neighbor ID	Sender ID range	Receiver ID range
2	26000-26025	26026-26050
3	15500-15525	15526-15550
13	**1190-11925**	**11926-11950**
14	**27000-27025**	**27026-27050**
15	58450-58475	58476-58500
25	31800-31825	31826-31850
26	21850-21875	21876-21950
27	23900-23925	23926-23950

For example: Let us consider the neighbor nodes 13 and 14 in Table 5. The sender ID range is between 1190-11925 and the receiver ID range is 11926-11950 for node 13. But node 14 sender ID range is 27000-27025 and receiver ID range is 27026-27050. This shows that though the nodes have consecutive node numbers, still the subrange IDs are different. When a cluster head wants to communicate with its neighboring cluster, then it uses different ID compared to the ID it uses for communicating with its neighbors.

The trust value is generated for each of the node separately. The trust value obtained for each cluster during simulation is tabulated in Table 6. For accuracy purpose the fractional value upto six points is considered. The trust value zero is assigned directly if the nodes have not been communicated for more than two sliding time window period instead of taking peer recommendations.

TABLE VI. TRUST VALUE FOR EACH CLUSTER

CN	Trust Value
1	4480.846941
2	4465.164315
3	4424.981300
4	4372.324430
5	4067.457464
6	4353.610797
7	4105.167300
8	4219.229978
9	4077.384847
10	4427.832076

The probability of detection of node IDs by an adversary is based on the degree of anonymity as shown in Figure 2. It shows that the probability of detection of the node IDs by the adversary reduces substantially by increasing the degree of anonymity and is minimized completely after 0.94.

If the nodes are not assigned with the anonymity IDs then there is a possibility of the adversary capturing the

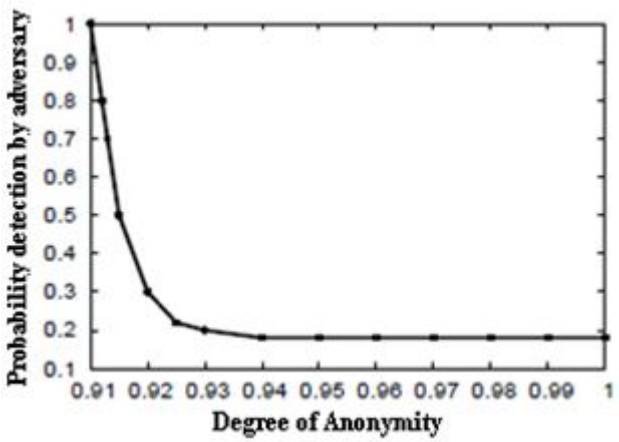

Figure 2. Degree of Anonymity

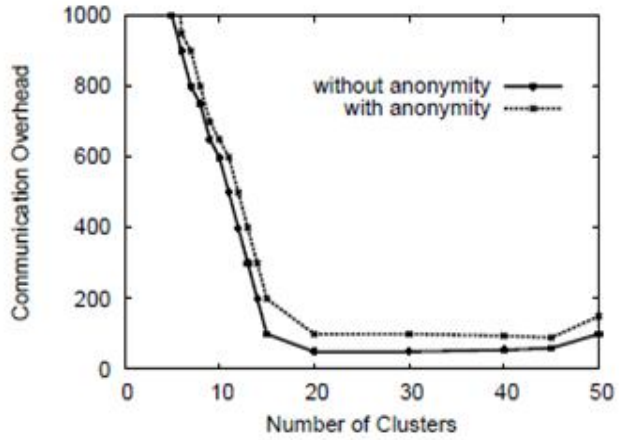

Figure 3. Communication Overhead Vs. Number of Clusters

node IDs and attacking or misinterpreting or dropping the packets. The introduction of both anonymity and assignment of trust value to the nodes increase the trustworthiness of the nodes and avoid misinterpreting, dropping the packets or traffic analysis.

The communication overhead for varying number of clusters consisting of the same number of nodes within a cluster is shown in Figure 3. It shows that communication overhead gradually reduces with increase in the number of clusters in WSNs. It is observed that the curve flattens with the formation of more than 20 clusters in a given network.

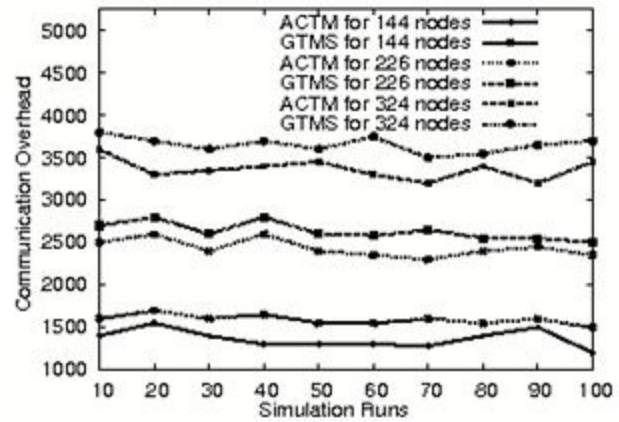

Figure 4. Comparison of ACTM (ATMC) with GTMS for Communication Overhead

DOI: 01.IJNS.3.4.1092

The communication overhead is plotted for 100 simulation runs for 144, 225 and 324 nodes as shown in Figure 4. The graph shows that the communication overhead is less compared to GTMS. The communication overhead varies depending on size and number of nodes in the network. If the number of iterations is increased, communication overhead reduces because transfer of nodes changes the position of nodes. Still each node possesses past recommendation values in the trust table even if their positions are changed and does not calculate the trust values from beginning. This reduces the communication overhead exponentially. The anonymity IDs are calculated initially and are just assigned to the nodes for every *r* iterations. With low communication overhead it is still able to provide enhanced security as it is using anonymity of IDs.

Conclusions

Security is an important issue in Wireless Sensor Networks. We propose an Anonymity and Trust Management Scheme (ATMC) algorithm to maintain security and avoid traffic analysis attack for WSNs. The proposed approach includes inclusion of anonymous IDs and assignment of trust values to each node. The concept of anonymity is introduced to hide the identity of the sensor nodes from the compromised nodes whereas anonymity of node IDs is not maintained in GTMS. The cluster head and its members are regularly reorganized randomly within the network and hence, the chance of early node failure is reduced. Thus, enhanced security, longer lifetime and reduced communication overhead are achieved in our algorithm.

References

[1] Saurabh Ganeriwal, Laura K. Balzano and Mani B. Srivastava, "Reputation-based Framework for High Integrity Sensor Network", *in ACM Transaction on Sensor Networks*. vol. 4, no. 3, 15:1-37, 2008.

[2] Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d'Auriol, Heejo Lee, Sungyoung Lee and Young-Jae Song, "Group-based Trust Management Scheme for Clustered Wireless Sensor Network", *in IEEE Transactions on Parallel and Distributed Systems*. vol. 20, no. 11, pp. 1698-1712, 2009.

[3] G. V. Crosby, N. Pissinou and James Gadze, "A Frame-work of Trust based Cluster Head Election in Wireless Sensor Networks", *in Proceedings of the 2nd IEEE Workshop on Dependibility and Security in Sensor Networks and Systems, Columbia*, 2006, pp. 10-22.

[4] Niki Pissinou and Garth V Crosby, "Cluster-based Reputation and Trust for Wireless Sensor Networks", *in Proceedings of the Fourth IEEE Conference on Consumer Communications and Networking (CCNC '07), Las Vegas, Nivada*, 2007, pp. 604-608.

[5] S. Karthik, K. Vanitha and G Radhamani, "Trust Management Techniques in Wireless Sensor Networks: An Evaluation", *in Proceedings of IEEE Conference on Communications and Signal Processing (ICCSP*), pp. 328-330, 2011.

[6] Efthimia Aivaloglou, Stefanos Gritzalis and Charalabos Skianis.: "Trust Establishment in Sensor Networks: Behaviour-Based, Certificate-Based and a Combinational Approach", *in International Journal on Systems Engineering*, vol. 1, no. 1/2, pp. 128-148, 2008.

[7] M. Krasniewski, P. Varadharajan, B. Rabeler and S. Bagchi, "TIBFIT: Trust Index Based Fault Tolerance for Arbitrary Data Faults in Sensor Networks", *in Proceedings of The 2005 International Conference on Dependable Systems and Networks, Yokohama, Japan*, 2005, pp. 672-681.

[8] Ming Yu and Kin K Lueng, "A Trustworthiness-Based QoS Routing Protocol for Wireless Ad-Hoc Networks", *in IEEE Transactions on Wireless Communication*, vol. 8, no. 4, pp. 1888-1898, 2009.

[9] Zhiying Yao, Daeyoung Kim and Yoonmee Doh, "PLUS: Parameterized and Localized Trust Management Scheme for Sensor Networks Security", *in Proceedings of IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*, 2006, pp. 437-446.

[10] Yi Ouyang, Zhengyi Le, Yurong Xu and Nikos Triandopoulos, "Providing Anonymity in Wireless Sensor Networks", *in Proceedings of IEEE International Conference on Pervasive Services*, 2007, pp. 145-148.

[11] A Wadaa, S Olariu, L Wilson, M Eltoweissy and K Jones, "On Providing Anonymity in Wireless Sensor Networks", *in Proceedings of the Tenth International Conference on Parallel and Distributed Systems (ICPADS'04)*, 2004, pp. 411-418.

[12] Yihua Zhang, Matthew Price, Lukasz Opyrchal and Keith Frikken, "All Proxy Scheme for Event Source Anonymity in Wireless Sensor Networks", *in Proceedings of Sixth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, 2010, pp. 263-268.

[13] Zhong Ren and Mohamed Younis, "Effect of Mobility and Count of Base Stations on the Anonymity of Wireless Sensor Networks", *in Proceedings of IEEE*, 2011, pp. 436-441.

[14] Qijun Gu, Xiao Chen, Zhen Jiang and Jie Wu, "Sink-Anonymity Mobility Control in Wireless Sensor Networks", *in Proceedings of IEEE International Conference on Wireless Computing, Networking and Communications*, 2009, pp. 36-41.

[15] Yousef Ebrahimi and Mohamed Younis, "Increasing Transmission Power for Higher Base-Station Anonymity in Wireless Sensor Networks", *in Proceedings of IEEE International Conference on Communications (ICC), Kyoto*, 2011, pp. 1-5.

[16] Y. Ebrahimi and Mohamed Younis, "Using Deceptive Packets to Increase Base-Station Anonymity in Wireless Sensor Networks", *in Proceedings of Seventh International Conference on Wireless Communications and Mobile Computing (IWCMC)*, 2011, pp. 842-847.

Biography

Shaila K 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.

DOI: 01.IJNS.3.4.1092

Sivasankari H is an Associate Professor in the Department of Information Science and Engineering at AMC Engineering College, Bangalore, India. She obtained her B.E in Electronics and Instrumentation Engineering from Bharathiar University and M.E degree in Computer Science and Engineering from Anna University. She is presently pursuing her Ph.D programme in the area of Wireless Sensor Networks in Jawaharlal Nehru Technological University. Her research interest is in the area of Wireless Sensor Networks and Information Security.

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 En gineering, Bangalore University, Bangalore. Her research interest includes Wireless Sensor Networks.

Venugopal K R 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 35 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.

DOI: 01.IJNS.3.4.1092