pISSN 1976-913X
eISSN 2092-805X

J Inf Process Syst, Vol.9, No.3, September 2013 http://dx.doi.org/10.3745/JIPS.2013.9.3.477

Self-Localized Packet Forwarding in Wireless Sensor Networks

Tarun Dubey* and O. P. Sahu*

Abstract—Wireless Sensor Networks (WSNs) are comprised of sensor nodes that forward data in the shape of packets inside a network. Proficient packet forwarding is a prerequisite in sensor networks since many tasks in the network, together with redundancy evaluation and localization, depend upon the methods of packet forwarding. With the motivation to develop a fault tolerant packet forwarding scheme a Self-Localized Packet Forwarding Algorithm (SLPFA) to control redundancy in WSNs is proposed in this paper. The proposed algorithm infuses the aspects of the gossip protocol for forwarding packets and the end to end performance of the proposed algorithm is evaluated for different values of node densities in the same deployment area by means of simulations.

Keywords—Localization, Node Density, Packet Forwarding, Redundancy, WSNs

1. INTRODUCTION

Wireless Sensor Networks (WSNs) consist of spatially distributed, autonomous sensors that have been fabricated using thin film technology for monitoring physical or environmental conditions, such as moisture, temperature, sound, pressure, light, volatile organic compounds, and many other phenomenon of interest over large sequential scales [1, 2, 3]. Sensor nodes in the network are outfitted with memory, a radio frequency transceiver, and a power source. They float the information in the form of packets/messages wirelessly over a specified protocol [4]. Packet forwarding is a common means for sensor nodes to efficiently share their packets with each other. The packet sharing mechanism can be utilized to initialize the network arrangement for route discovery between a given pair of senor nodes and could serve as an efficient method to localize sensor nodes. The simplest way of packet forwarding is flooding [5], under which each sensor node resends when it receives a packet for the first time. It is attractive for its simplicity but causes high redundancy, packet collisions, and the wastage of bandwidth [6]. Therefore, an efficient packet-forwarding scheme is required to reduce the packet-forwarding redundancy in sensor networks [7]. As an amendment to flooding, various probabilistic broadcast protocols have been proposed. The proposed protocols [8, 9] avoid the above-cited problems and provide alternative solutions to flooding. In addition, sensor network applications also require broadcast protocols to support different degrees of reliability. Hence, probabilistic protocols are more suitable. One of the basic extensions to flooding is gossiping [10], where each sensor node forwards a packet in a probabilistic manner. The extensions for gossiping protocols

---

Manuscript received March 15, 2013; first revision May 13, 2013; accepted June 28, 2013.

Corresponding Author: Tarun Dubey

* Department of Electronics and Communication Engineering, National Institute of Technology, Kurukshetra, India. (tarundubey79@yahoo.co.in, ops_nitk@yahoo.co.in)

[11, 12] are predominantly static in nature and cannot adapt to the changing topology, as well as to the changing application requirements. Therefore, static protocols require the network designer to conservatively preconfigure the parameters on a case-by-case basis, in order to allow for changes in the network topology (node density and the number of duplicate forwarded packets). In this paper, we propose a Self-Localized Packet Forwarding Algorithm (SLPFA) to control redundancy in WSNs. The proposed algorithm infuses the technique of a gossip protocol for forwarding packets between the sensor nodes and routinely adapts to a changing network topology with increasing node density. The simulation results highlight that SLPFA is light weight in view of the limited assets available with sensor nodes and works in a self-localized manner. Self-localization allows sensor nodes to reconnoiter their surroundings, cooperate to form topologies, and adapt to environmental changes, all without human intervention. Sensor networks require nodes to discover relative positioning information (e.g., distance estimations or directional estimations) of neighboring nodes. The ability to attain these estimates is the basis of localization algorithms. If any local information is known, simple geometric relations can be used to calculate the local topology, which can then be subsequently disseminated throughout the network, and thereby providing a globally coordinated localization. Locations can also be estimated by forwarding the local constraints of all of the nodes in the network to a central server or sink, which can then find location estimates. Self-localization is a location aware phenomenon of sensor systems. It is where sensor nodes interact with each other to initiate localized packet forwarding decisions without a global network state update, to ensure Quality of Service (QoS). The location information can only be exchanged with immediate neighbors if each sensor node is aware of its immediate neighbors within its radio range and their locations. Using the neighbor locations, each sensor node can locally make a per packet forwarding and if each sensor node forwards the packet to a neighbor closer to the destination area, the packet can eventually be delivered to the destination without any topology information.

The rest of the paper is organized as follows: Section 2 provides the description of the gossip protocol and highlights a few of its essential preliminaries in reference to WSNs. Section 3 presents the proposed SLPFA. The simulation model and simulation results are described respectively in Section 4 and Section 5. Finally, the paper concludes with Section 6.

2. GOSSIP PROTOCOL

The location knowledge of sensor nodes in WSNs is important since collected data only has relevance if the location from where it has been sensed is well known. Data collection and forwarding is based on common phenomena, so there is a high probability that this data has some redundancy. Gossip is a probability-based protocol and its definition states that whenever a sensor node wishes to send a packet, it randomly selects a neighboring sensor node, and upon receiving the packet for the first time the neighboring sensor node repeats this process. If the same packet is received twice, it is discarded. In order to achieve this, each sensor node has to keep track of the packets it has already received [13]. Besides supporting packet forwarding, the gossip protocol also performs tasks to help inter process interactions for an information exchange in networks where sensor node failure is quite frequent. This section summarizes some vital preliminaries for the gossip protocol with reference to sensor networks [14].

2.1 Node Density

The number of sensor nodes, N determines the level of confidence for the gossip protocol. The gossip protocol relies on the aspect that each sensor node can make its communication based on negotiations with neighboring sensor nodes. For a dense area A, sensor nodes are likely to receive more packets. Hence, it might prove beneficial to hold the packets with very low probability. In some cases the area A might be very sparse. Hence, it might be beneficial to hold the packet with a probability, say $P = 1$. Therefore, the probability with which a sensor node holds the packets directly depends on the node density D of the sensor nodes deployed in the network. Sensor node density can be calculated using equation (1).

$$D = N\pi r^2 / A \tag{1}$$

In equation (1), R is the coverage radius of each sensor node.

2.2 Node Degree

The node degree $\acute{N}$ depends on the values of A, N, and r; and is calculated using equation (2).

$$\acute{N} = N - 1\left(\pi r^2 / A\right) \tag{2}$$

It is to be noted that $\acute{N}$ is a variable parameter, since A, N, and r cannot always be homogeneous in WSNs.

2.3 Frequency of Received Packets

Sensor nodes are understood to be adjacent if the distance between them is less than the defined transmission range. The sensor nodes, if set to a very low probability of listening, will transmit a packet only when there is a change. However, they may send a very few packets in some special cases. Furthermore, such a sensor node may or may not choose to listen depending upon the initial value of P. Thus, a sensor node will only gossip if it receives a new packet. Otherwise, it will continue to be in a passive state.

2.4 Fan Out (*n*)

This is defined as a configuration parameter to count the number of sensor nodes that have been selected as gossip targets. Upon receiving a message for the first time, the sensor node selects gossip targets to forward the message. The trade off associated with this parameter lies between the desired fault tolerance level and observed redundancy. A high value of n guarantees fault tolerance but it also leads to an increase in the network redundancy.

2.5 Relative Message Redundancy (*RMR*)

RMR measures the message overhead for a gossip protocol. It is calculated using equation (3).

$$RMR = m / \left(n - 1\right) - 1 \tag{3}$$

In equation (3) m denotes the number of packets forwarded during a procedure. This metric is applicable if at least two sensor nodes receive the packet. A zero value for RMR denotes that there is exactly one packet exchange per sensor node and is clearly the optimal value. A high value of RMR indicates a poor network usage and for gossip based packet forwarding the value of RMR should tends to $n - 1$.

2.6 Maximum Rounds

This is the maximum number of times a given gossip packet is retransmitted by the sensor nodes. Each packet is transmitted with a round value, initially with the value of zero, which is increased each time a sensor node retransmits the packet. Sensor nodes will only retransmit a packet if its round value is smaller than the maximum rounds parameter. The gossip protocol can operate in one of the two modes listed below.

2.7 Unlimited Mode

In this mode of operation the parameter of the maximum rounds is undefined, and there is no specific limit to the number of retransmissions executed to each gossip packet.

2.8 Limited Mode

In this mode of operation, the parameter of the maximum rounds is defined with a value above zero. This effectively limits the maximum number of hops executed by each packet in the overlay.

3. THE SELF-LOCALIZED PACKET FORWARDING ALGORITHM (SLPFA)

SLPFA is intended for packet forwarding in high density WSNs. It is to be noted that scalability is a critical issue in sensor networks, which are composed of hundreds and thousands of densely deployed sensor nodes. The localization of sensor nodes increases with the increase in sensor node density, as each sensor node makes the decision to forward the packet according to the local information obtained from its neighboring sensor nodes. We assume that SLPFA does not require any topology information. Thus, the overhead remains small and all of the sensor nodes have the same characteristics (same communication and sensing range). The position of each deployed sensor node is not known in any arbitrary coordinate system since we assume that the neighbors of a particular sensor node are determined based on the packet forwarding and the sensor nodes are static in nature. In this way, the sensor nodes decide locally whether or not to forward the packets (serving like an active node) or to ignore the previously received packets. Packet forwarding is said to be redundant if each sensor node in the network has already received the same packet at an earlier time. The major challenge associated with this type of packet exchange lies in the accurate estimation of redundant packet counts for a varying number of sensor nodes within the network, which are confined to the total number of forwarded packets. SLPFA is based on the assumption that the sensor nodes N are deployed within a specified area A and that they are allowed intuitively broadcast message m, for event E_N, due to the increase in the number of sensor nodes corresponding to a high density wireless sensor network. The steps of the proposed algorithm are shown in Table 1.

Table 1. Algorithm description

Self-Localized Packet Forwarding Algorithm (SLPFA)

```
1:  BEGIN
2:  define $A$, $N$ and $m$
3:  where m and $N \subset A$
4:  Initialize $N$ =50 and $m$ = 1,
5:  define $E_N$
6:  deploy $N$ such that $N \in A$
7:  Start
8:  packet forwarding
9:  forward initial packet, $m$
10: select the neighbor sensor node as gossip targets, $n$
11: If the neighbor sensor node receives packets for the first time, go to Step 9;
    Or else go to step 14
12: End
13: If the neighbor sensor node receives the packet twice,
14: Then discard packet forwarding;
    update, if $N$ abandons its attempt to re-forward a packet
15: repeat step 8 for $N$ ={100,150, 200, 250, 300, 350, 400, 450 and 500} with m = 1
16: check redundant packets individually for each round with  N = {50,100, 150, 200, 250, 300, 350, 400,
    450 and 500}
17: END
```

The algorithm described in Table 1 is useful in networks where short packets dominate the network traffic. Furthermore, it also employs the strategy of localized implementation for packet forwarding. SLPFA employs the concept of an active network with high computing capability and is useful in reducing the packet traffic in WSNs. This is because the collection point does not require large packets in context of location awareness.

It is obvious that SLPFA incorporates the benefits of gossip protocol in a self-localized manner to control redundant packet forwarding. The algorithm also guarantees the advantage that the sensor node has to be active only during packet forwarding and no node has to localize itself with respect to a global coordinate system. This ensures that sensor nodes with the smallest distance from their neighboring sensor nodes will also require minimum forwarding in order to forward the packet. SLPFA is a pure localized algorithm since any action invoked by a sensor node does not affect the network as a whole.

4. SIMULATION MODEL

We assume two-tier network architecture for optimizing the randomly placed sensor nodes. The algorithm is implemented for WSNs, and the test results are presented in the next section. This section explains that the notations followed by the visualization of sensor node densities. The simulation parameters are shown in Table 2.

Table 2. Simulation parameters

Parameter	Value
Network dimension	500 m x 500 m
Transmission range of sensor nodes	200 m
Event	1
Protocol	Gossip
Sensor node distribution	Normal

4.1 Notations

- A is the area of the wireless sensor network.
- D is the sensor node density of the network (i.e., the average number of sensor nodes per region).
- r is the coverage radius of each node.
- N are the total number of deployed sensor nodes.
- m are the number of forwarded packets.
- h are the number of sensor nodes that have rebroadcasted the packet after its reception.
- R_B is the rebroadcast ratio (i.e., the ratio of number of sensor nodes that have rebroadcasted the packet to the number of sensor nodes in the entire network).
- P is the probability by which a sensor node can receive a packet.
- n are the number of sensor nodes selected as gossip targets.
- E_N is the number of events scheduled for forwarding the packet.

Based on the above notations, equation (4) and equation (5) are obtained.

$$R_B = h/N \tag{4}$$

$$N = A\left(D/r^2\right) \tag{5}$$

The rebroadcast ratio R_B manifests the efficiency of the gossip protocol since R_B is inversely proportional to the broadcast efficiency. The high value of R_B results in a high redundant rebroadcast with a low broadcast efficiency. Therefore, based on equation (4) and equation (5), the efficiency of SLPFA is determined by the minimum value of R_B, and can be calculated using equation (6).

$$R_B = hr^2/AD \tag{6}$$

The values of A, D, and r are determinate. Hence, in order to obtain the minimum value of R_B, the value of h should be minimized, because if the node density D increases, then the value of R_B decreases. SLPFA is evaluated for different values of N. The sensor node densities are shown respectively in consecutive Fig. 1, Fig. 2, Fig. 3, Fig. 4, Fig. 5, Fig. 6, Fig. 7, Fig. 8, Fig. 9, and Fig.10.

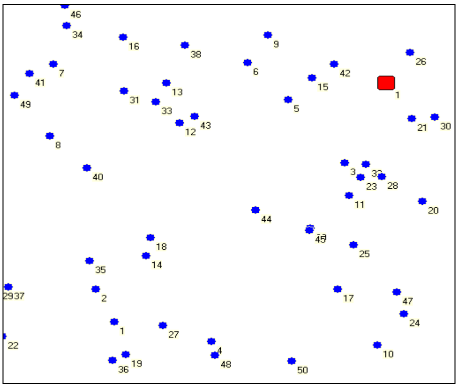

Fig.1. Sensor node density (*N* = 50)

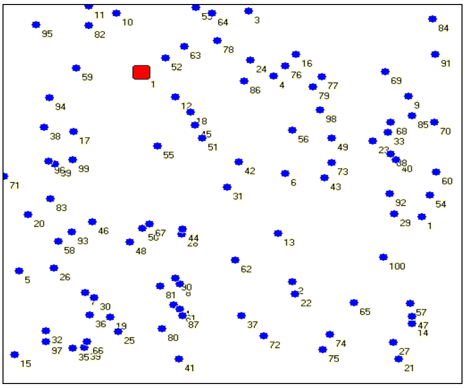

Fig. 2. Sensor node density (*N* = 100)

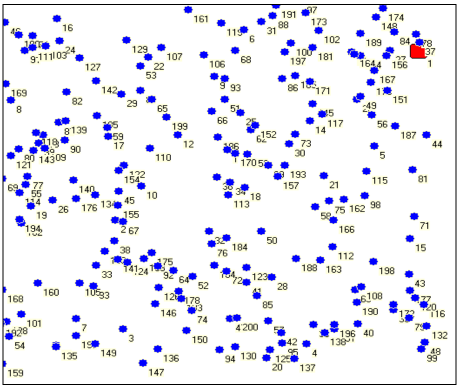

Fig.3. Sensor node density (*N* = 150)

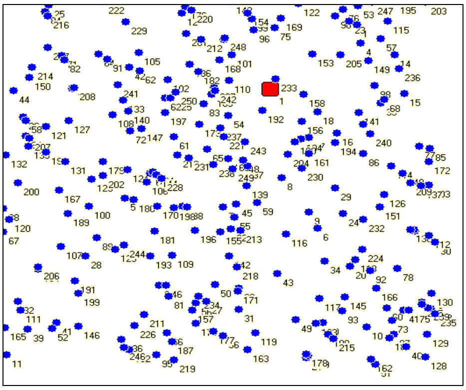

Fig. 4. Sensor node density (*N* = 200)

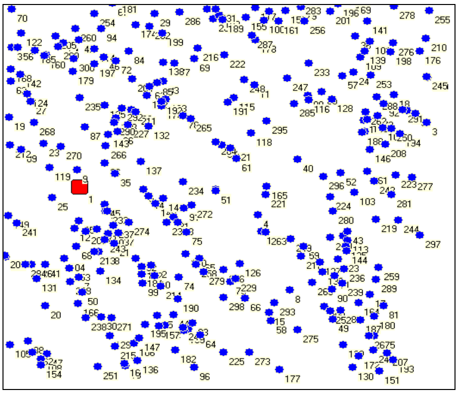

Fig.5. Sensor node density (*N* = 250)

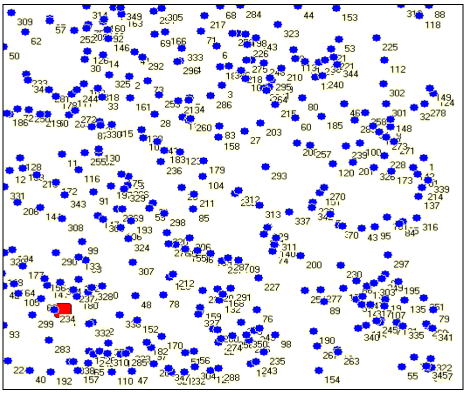

Fig.6.Sensor node density (*N* = 300)

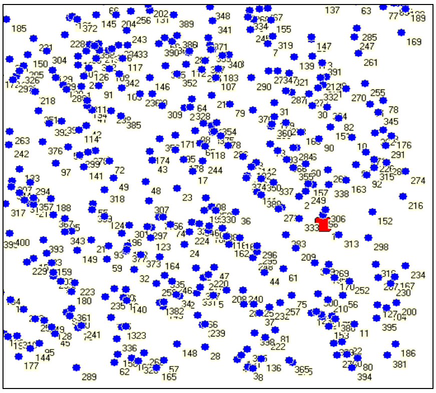

Fig.7. Sensor node density (*N* = 350)

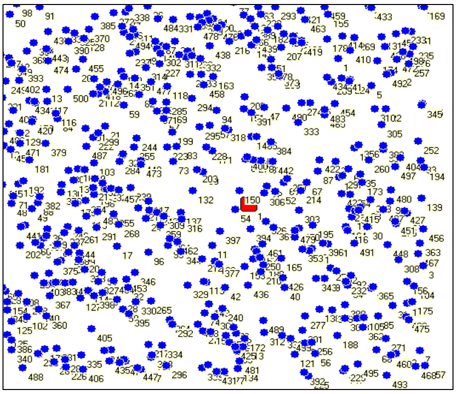

Fig. 8. Sensor node density (*N* = 400)

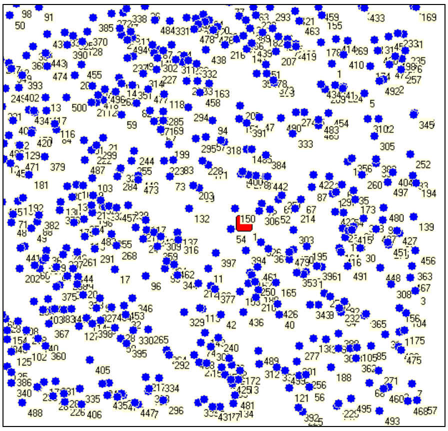

Fig.9. Sensor node density (*N* = 450)

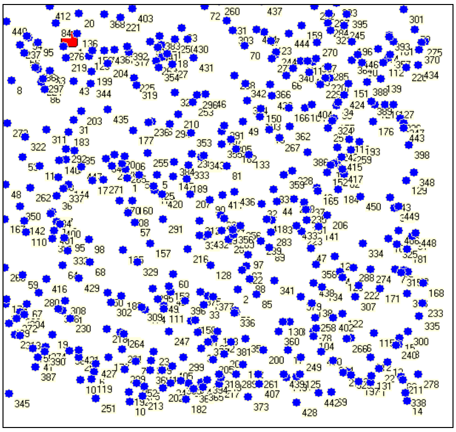

Fig. 10. Sensor node density (*N* = 500)

5. SIMULATION RESULTS

For analyzing the effect of SLPFA on WSNs, we simulated a wireless sensor network composed of a different number of sensor nodes. The simulations were performed on SNetSim [15], which is new simulation software, mainly for event driven conditions event-driven simulation software running on Windows based operating systems. It is simple and easy to use and the user can create his/her own protocols. It also has a complete stack for the gossip protocol. SNetSim provides a central management with functionality to set the deployment area and other parameters before creating the network topology. However, the simulator has a tendency to be specific to hardware and is not platform portable. Furthermore, it lacks information on the flow of events. The randomly placed sensor nodes were simulated in an area of 500 m × 500 m, such that each sensor node can communicate with a neighboring sensor node. It was observed that SLPFA promoted efficient packet forwarding within the entire network, besides maintaining a controlled level of redundancy with the increase in number of sensor nodes. The stability of the proposed algorithm in high-density sensor networks is guaranteed, as the network was simulated individually for different values of N ranging from 50 to 500. The received packet counts, the received redundant packet counts, and the packet delivery ratio against different values of N are shown in Table 3. The simulation results support controlled redundancy within the network with the increase in the number of sensor nodes over the same deployment area. Fig. 11 shows the graphical data between the number of sensor nodes and the percentage of observed redundancy. The evaluation of controlled redundancy is promising for networks with a large number of sensor nodes, as in cases of sensor node failures the network can effectively retain its packet forwarding in a fault tolerant manner. The controlled redundancy will also aid in improving sensor node localization in networks where the density of sensor nodes is a dominant factor. The throughput of the proposed algorithm is also evaluated in terms of the packet delivery ratio and is shown in Fig.12.

Table 3. Packet counts

Sensor nodes	Forwarded packets	Received packets	Redundant packets	Packet delivery ratio
50	100	30	70	0.55
100	200	79	121	0.56
150	300	121	179	0.58
200	400	166	234	0.66
250	500	208	292	0.69
300	600	248	352	0.69
350	700	292	408	0.73
400	800	335	465	0.79
450	900	376	524	0.88
500	1000	424	576	0.89

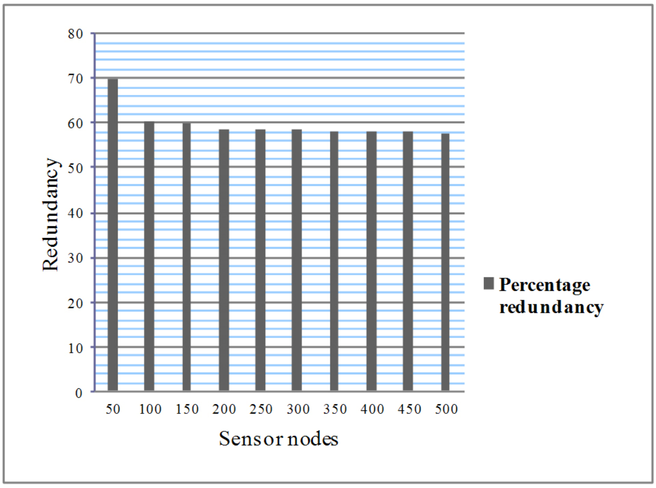

Fig.11. Redundancy vs. the number of sensor nodes

[4] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “A Survey on Sensor Networks,” IEEE Communications Magazine, Vol. 40(8), pp. 102-114, 2004.

[5] J. N. Al-Karaki and A. E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey,” IEEE Journal of Wireless Communications, Vol. 11(6), pp. 6-28, 2004.

[6] K. Sohraby, D. Minoli and T. Znati, “Wireless sensor networks: technology, protocols, and applications,” John Wiley and Sons, ISBN 9780471743002, pp. 203-209, 2007.

[7] B. Carbunar, A. Grama and J. Vitek, “Redundancy and Coverage Detection in Sensor Networks,” ACM Transactions on Sensor Networks, Vol. 2(1), pp. 94-128, 2006.

[8] L. Junhai, X. Liu and Y. Danxia, “Research on Multicast Routing Protocols for Mobile Ad hoc Networks,” Computer Networks, Vol.52, pp. 988-997, 2008.

[9] W.R. Heinzelman, J. Kulik, and H. Balakrishnan, “Adaptive Protocols for Information Dissemination in Wireless Sensor Networks,” Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 174-185, 1999.

[10] Z. J. Haas, J. Y. Halpern, and L. E. Li, “Gossip-Based Ad Hoc Routing,” IEEE/ACM Transactions on Networking, Vol. 14(3), pp. 479-491, 2006.

[11] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, “Negotiation Base Protocols for Disseminating Information in Wireless Sensor Networks,” Wireless Networks, Vol. 8, pp.169-185, 2002.

[12] R. Chandra, V. Ramasubramanian and K. P. Birman, “Anonymous Gossip: Improving Multicast Reliability in Mobile Ad Hoc Networks,” IEEE ICDCS, pp. 275-283, 2001.

[13] A.M. Kermarrec and M.V. Steen, “Gossiping in Distributed Systems,” Operating Systems Review, Vol. 41 (5), pp. 2-7, 2007.

[14] C.L. Barrett, S.J. Eidenbenz, L. Kroc, M. Marathe and J.P. Smith, “Parametric Probabilistic Sensor Network Routing,” Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications, pp. 122-131, 2003.

[15] http://www.dho.edu.tr/enstitunet/snetsim/index.htm

[16] R. Zhao, X. Shen, Z. Jiang, and H. Wang, “Broadcasting with Least Redundancy in Wireless Sensor Networks,” International Journal of Distributed Sensor Networks, Vol. 2012, Article ID 957606, pp.1-23,2012.

[17] S. Halder, A. Ghosal and S. DasBit, “A Pre-determined Node Deployment Strategy to Prolong Network Lifetime in Wireless Sensor Network,” Computer Communications, Vol. 34 (11), pp. 1294 - 1306, 2011.

Tarun Dubey

He received his B.Tech and M.Tech degrees in year 2001 and 2004 respectively. He is pursuing his Ph.D. from Department of Electronics and Communication Engineering, National Institute of Technology, Kurukshetra, India. His research interests include wireless sensor networks, digital communication, computer architecture and electronic warfare systems.

O. P. Sahu

He is Professor at Department of Electronics and Communication Engineering, National Institute of Technology, Kurukshetra, India. He has more than 75 papers in his credit in various national and international conferences and journals. His research interests and specialization areas include signals and systems, digital signal processing, communication systems and fuzzy systems.