International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Modified Belief Propagation-Based Defense against Routing Toward Primary User Attack in Cognitive Radio Networks

Dhanashree Yogesh Jangam[1], Aruna K. Gupta[2]

[1, 2]Computer Engineering Department, Jayawantrao Sawant College of Engineering,
Handewadi Road, Hadapsar, Pune-28, Maharashtra, India

Abstract: ***Current wireless networks are characterized by a static spectrum allocation policy, where governmental agencies assign wireless spectrum to license holders on a long term basis for large geographical regions ISM band has enabled the explosion of new technologies that is Wi-Fi due to this its license is free from characteristic. The widespreadadoption of Wi-Fi technology, combined with the rapid penetration of smart phonesrunning popular user services has overcrowded substantially the ISM band. Cognitive radio (CR) networks have involved many attentions newly; whilethe security issues are not yet studied fully. In this approach, propose a new and powerfulnetwork layer attack called routing-toward-primary-user (RPU) attack in Cognitive Radio networks. In this attack malicious nodes intentionally route a large amount of packets In this approach, suggest a new and powerful network layer attack called routing toward-primary-user (RPU) attack in Cognitive Radio networks. In this attack malicious nodes intentionally route a large amount of packets toward the primary users (PUs), purpose of malicious node is to cause interference to the PUs and to increase delay in thedata transmission among the secondary users.The main objective of the proposed work is to minimize the time for sendingthe data, and send the data by the path which is the longest distance from the primaryuser network. For that the pre belief value is calculated, belief propagation used to develop a defense strategy. Here a initial rout establish from source to destination, then according to it the each node keeps a feedback of other node on the route, compute belief, exchanges of feedback in a table record. On the basis of final belief values, the source node detects the malicious path.***

Keywords: Belief propagation, Cognitive, Modified BP, Radio Network, Routing toward primary user attack, security

1. Introduction

As Current wireless networks are characterized by a static spectrum allocation policy, where governmental agencies assign wireless spectrum to license holders on a longterm basis for large geographical regions ISM band has enabled the explosion of new technologies that is Wi-Fi due to this its license is free from characteristic. The widespreadadoption of Wi-Fi technology, combined with the rapid penetration of smart phonesrunning popular user services has overcrowded substantially the ISM band.Cognitive radio (CR) networks have involved many attentions newly, while the security issues are not yet studied fully. In this approach, propose a new and powerfulnetwork layer attack called routing-toward-primary-user (RPU) attack in Cognitive Radionetworks. In this attack malicious nodes intentionally route a large amount of packetstoward the primary users (PUs), purpose of malicious node is to cause interference tothe PUs and to increase delay in the data transmission among the secondary users. It isdifficult to detect the malicious nodes in the RPU attack because the malicious nodes mayclaim that those nodes, to which they forward the packets, behave dishonestly and causeproblems in the data transmission. To protect against this attack, a defense strategyusing pre belief propagation. At very _rst pre belief value is calculated. The suitable path is found forsending the data. By using the pre belief values the node can detect the maliciousnodes. This value gives the suitable path for sending the data within a time. Usingthis approach data securely send to destination node. In this approach proposed defensestrategy against the RPU attack is effective and efficient in terms of major reduction inthe delay and interference caused by the RPU attack.

A spectral resources demand is continuously growing and widely used. Radio spectrum utilization is moderately low [1], [2], [3], [4], [5]. This is publicized by the spectrum measurement. The reason behind this nothing but a traditional approach towards the portion of restricted allocation spectrum of explicit wireless systems and services. In a large regions and time spans, such spectrum has a licensed. The unlicensed cannot access wireless system even if the spectrum utilized the licensed system. By considering a latest concept with a more capable way of using spectral resources one can find a solution for supplying spectral demand. Spectrum holes left by idle primary users (PUs) are used by secondary wireless users with the help of Cognitive radio (CR) which is a revolutionary technique. A CR wireless network which is looked as a multichannel multi-access network, wireless routers works like SUs for communications purpose that can opportunistically utilized by different spectral holes without causing any hindrance to the PUs. In some current work [6], [7], [8], [9], [10], [11], [12], [13], [14] network automatically establishing nodes, maintaining connectivity, dynamically self-organized and self-configured for the distributed CR networks are shown.

The CR network has many advantages, but it also has disadvantages regarding security. The collaborative sensing and multihop routing like distributed entities are inherited rely between networks. Due to this security challenges are occurred. Reporting false selection frame (FSF) attack [15], The primary user emulation (PUE) attack [16], reporting false sensing data (RFSD) [17], common false evaluation attack [18], control channel denial of service [19], and are the discovered attacks based on the CR-based network.

We are studying a latest and great routing-toward-primary-user (RPU) attack in CR networks which is proposed in this paper. Here, in the routing toward primary user attack, the malicious node purposely sends a large amount of packets on the way to the primary users (PU), purpose to cause interference to the primary users and raise the delay in transmission of data among the secondary users. This interference is not only for a single device to the PUs, but also affects the many CR devices which are transmitted at the same time around the PUs and hence the large amount of PUs performance is damaged. The malicious nodes cannot generate interference directly to the PUs. Instead of honest nodes generate this interference by receiving the packets through the malicious nodes. Due to this reason detecting the malicious nodes is very difficult.

Against the RPU attack we developed a defense strategy based on belief propagation (BP) for increasing RPU attack awareness and representing its damage. The initiate route originated from source to destination without any information of the malicious nodes. On the basis of feedback information of the other nodes on the router, the each node on the rout keeps a table record. The every node computes the belief by exchanging the feedback with its neighbor's node. Based on the final belief values the malicious node detected by the source nodes and BP converges. By avoiding malicious nodes the data packets routs by source node to the destination node. For reducing the complexity of defense mechanism we are applying belief propagation (BP). These propose scheme is effective and efficient for detecting the RPU attackers. This is shown by the simulation result.

In this paper we learn the attacks and defense in CR network in section II, in section III we see the system overview and last conclusion and future scope of RPU in CR network.

2. The Literature Survey

New proportions of vulnerabilities are transports by spectrums which is access in CR systems. The different CR networks attacks are,

1. Attacks In Network Layer

In Wormhole attack, which is redirection attack, the attackers plot a high speed link among them. Due to this other nodes believe wrongly that other paths are longer than the path among the plotting attackers. A large amount of data traffic, which grounds traffic analysis, congestion or manipulation of facilitates datais attracted by plotting attackers [22]. Sybil attack, is the another network layer attack. Where by claiming false identities, aspiring to achieve a disproportionately large persuadein the network, or by imitating are the behaviors of a malicious node in a larger number of nodes [23]. The attacker can abuse, drop or eavesdrop messages as it sees fit by stimulating the source node to select a rout through the attacker [24]. Without considering about the CR system model and PUs existence, there are several attackers present in a network layer. They are wireless ad hoc or mesh or sensor. RPU attack which is projected in this paper also a redirection attack. These attacks cause the failure in data transmission as well as humiliate the PUs' performance. In this attack the malicious node accidently makes an honest node to harm the network, instead of causing the problem to the network, which is difficult to detect by the attackers. Due to this reason RPU attack is different from the above attacks.

2. Attacks in MAC Layer

The PU's signal characteristics features and available spectrum transmission is imitated by malicious nodes. This is nothing but a PUE attack [16], [20], [21]. SUs believe that PU is present there and they avoid it with the help of spectrum holes which is actually available. Against the collaborating spectrum sensing protocol, the RFSD physical layer attack is discovered [17]. This protocol used to recognizea proficient method to deal with the problem of unpredictability in single-user spectrum sensing, and false sensing data due to the miss detection in the decision or false alarm made by the fusion center is reported by the malicious SUs.

3. RPU Attack Model

Malicious nodes claim that they have best rout with low cost by sending fake routing information in the RPU attack. Due to this other honest nodes send packets through those malicious nodes.This model shows that the cost between the SU, which is near to the PU anditself is very low. And due to this reason honest node forwarded data packets this malicious node andall traffic will be routed through the attacker. In the RPU attack, malicious node can be any location; it does not require close to the PU. And it cause directly interference to the PUs or in the long delay data transmission. And it claims to those nodes to which it forwarded the packets because the source node cannot identify the bad node. It affects the data transmission failure as well as degrades the PU's performance. It also hurt the honest node instead of causing problems to the network. Due to this reason it us very difficult to convert or detect.

We consider the system performance in terms of probability, in this approach. In this case received power SU from PU falls below a certain threshold.According to application scenario and transmitter/receiver structure, the power threshold is determined.

For routing among SUs in CR wireless network is done by using shortest path routing algorithm [25], which is effective and efficient. The delay which is inversely proportional to the capacity is used to determine the cost of direct link.

3. System Overview

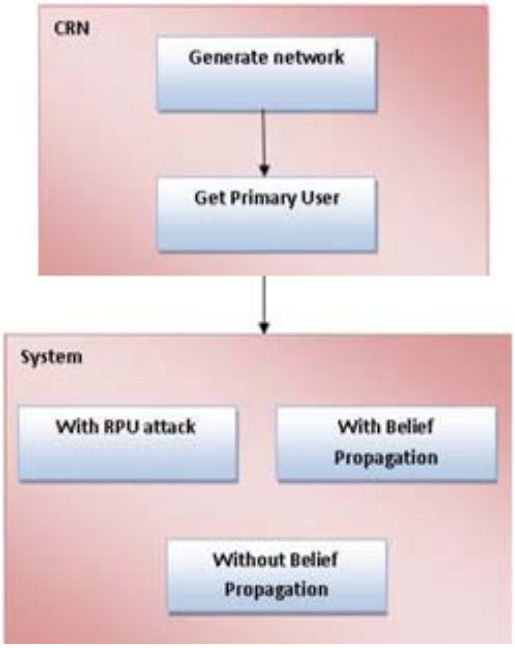
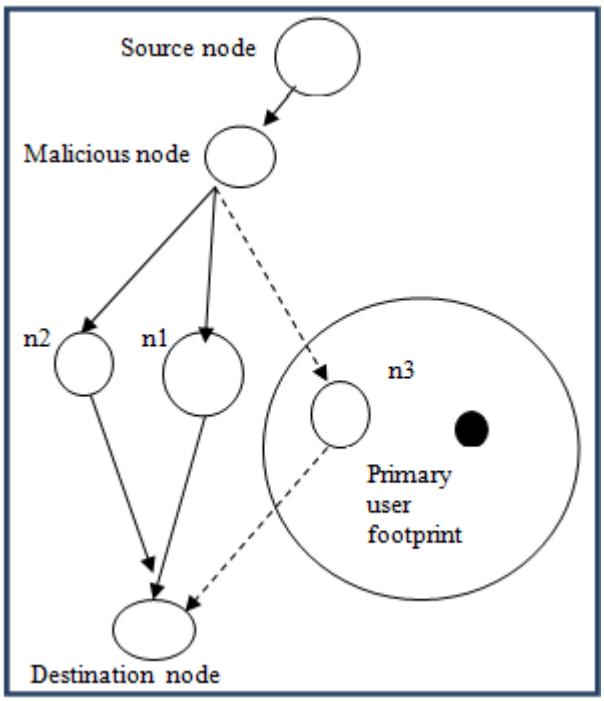


Figure 1: System Overview



Here,

Is a primary user

Is a secondary user

Is a connection link

Is a connectionless link

This fig shows the RPU attack. In this figure SUs are n1, n2, n3, source node and destination node. The footprint of PU is the shaded region. Here secondary node n3 is inside the region it is forced to the turn off for a specific time slot. At different time slot it can change in different shapes. Due to this reason the secondary nodes should be out of the PU's footprint. If the distance to the PU's is shorter then there are higher chances of turn off. In this fig. source node wants to transmit destination node but malicious node claimed that it have a shorter path to the destination node and source node forward the entire packet to the malicious node. This is nearer to the PU as compare to n2, even that malicious knows that n2 can also able to forward these packets.There are two chances first is malicious mode→ n1→ destination node and second is malicious node→n2→ destination node. But in second n2 near to the footprint there are chances of delay in data transmission and may be turning off frequently.

In this approach it consists of the concept of cognitive radio networks. In which here describes how routing toward primary user attack affect to data transmission delay and the defense strategy for this attack. Belief- Propagationbased defensestrategy is used for RPU attack.Only local observations are used in a single-user decision. For detecting the malicious node there is requirement of communication between all neighbor nodes and feedback exchange. For this we can use a simple flooding strategy but this give the significant like complexity of computation and overhead signaling. This problem can be overcome with the help of BP [26], [27], [28], which is calculated marginal distribution efficiently and circumvent the others node involvement which is not present in the initial rout. Can be detected which is described as follows:
Topology and network types are not considered here.

In network we are considering the source, destination and primary user node as well as attacker node

A. Mathematical Model

For the implementation of the proposed work, some mathematical formulas are required. The mathematical model of the proposed application is as follows:

Let n = no of nodes in the network.
R = Range of PuArea.
S and D are the source and destination node respectively;
R = calculate Range (100+Random (100));
IfAll(Position of a node in path(position >range))
Preferred Path;
Else(Position of a node in path(position <range))
Malicious Path;

Consider A is the threshold value for calculating the belief, l be the length of the nodes,

Then the threshold value is calculated as,

$$A = l * 2 * 100$$

From this equation the threshold value is calculated.

Let X be the time required for sending respond and receiving response again.

Now we will see the belief value calculation condition for all normal mode, post belief propagation and pre belief propagation.

In the cognitive radio network Y be the range of primary user. This range is fluctuated. If the nodes from the

secondary user enter in the primary user area then the node is temporarily off for some time.

In RPU attack Mode:
No Belief value is evaluated. User selects the source and destination node, and evaluate path. Malicious node referred the preferred path from this path data is send. Malicious node always referred the path which is near to the primary user range.

In Post Belief Calculation
In this user select the source and destination node, before sending the data, preferred path and belief value is evaluated. The conditions for that are as follows:

The time is calculated for each path between the source and destination node.

A > T then the path is **preferred path** for sending the data.
If **A < T** then the path is **malicious path** for sending the data.

From this condition belief value is calculated and data is send to the destination node and malicious path is detected

In Pre Belief Calculation
In this type, before selecting the send and destination node, the belief value is calculated. If in the network 10 nodes are present, then the belief value of node with each node is calculated. This was calculated for each node. All the condition of calculating the belief value is same as post belief calculation. In the pre belief method the belief value is refreshed or calculated in the given time spam. Reason behind that is because the range of primary user area is fluctuated.

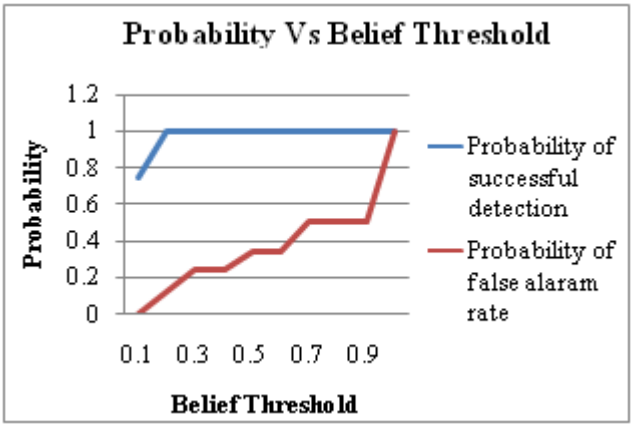
B. Algorithm

Proposed work is based on the pre belief calculation for secondary user in cognitive radio network.

```
If(NetworkCreated)
{    N= PU area Node;
   Calculate range R =  100;
    If(S= Source Node and D= Destination Node)
{  CalculateAllpath(S,D);
ShortestPath = DijkstraShortestPath(Based on min hope count);
   While(shortestPath != null)
   {   Calculate position of node in path = pos;
       If(pos Present in R)
       {   Node is sleepMode;
       }Else
{Active Mode;
}
       If(all active){
             Preffered Path;
       }
       Else{
          Malitious Path
       }
   }
     If( R is Varies R= 100+random(100)
         {
Calculate position of node in path = pos;
       If(pos Present in R)    {
             Node is sleepMode;
          }Else{
Active Mode;
}
If(all active){
      Preffered Path;
      }Else
      {
         Malitious Path
      }
} }
```

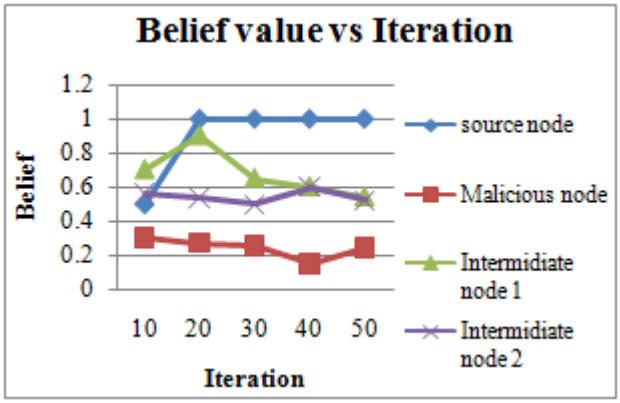
C. Graphs

1. Probability Vs Belief



The graph shows the relation between probability and belief threshold. Probability of detecting the malicious node is 100 percent is shown in the above graph

2. Belief Value Vs Iteration



The above graph represents the graph between iteration versus Belief value. X-axis represents the number of iteration and y-axis represents the belief value. In the network only one malicious node is exist, some intermediate node are exist and some intermediate node also exist. In the graph we will show the different belief values of all the nodes.

4. Conclusion and Future Work

Future Scope: The detection of malicious user from this attack can be extended by considering current constraint. In future malicious user detection from this attack can be use

detection technique by considering size of network; can be taken as a problem statement.

Conclusion

Here in this approach we have seen a latest network layer attack that is RPUattack. The Routing toward primary user attack from cognitive radio network, in whichmalicious node intentionally sends the packet on the way to the primary user. Due tothis it causes the delay in data transmission. And it is hard to detect this attack. Toprevent such type of attack, here uses one strategy is that pre belief propagation baseddefense strategy. In this defense strategy, here without any information of the maliciousnodes, pre belief value is calculated. The table recording of feedback is kept by an eachnode `after' it on the rout. Then in each iteration, the exchanges of m values with its neighbor nodes are done by every node. After converges, on the basis of final belief valuethe source node can detect the malicious nodes. For avoiding a malicious node, a newrout will be found. When we eliminate the malicious node from network then there is nodelay in data transmission. Hence in this way the malicious node is detected from RPUattack.

We also propose a "Finding Preferred Path to Defend RPU Attack by thePre Belief Propagation in Cognitive Radio Networks". Here, initially the belief value iscalculated on the basis of threshold value. From this value suitable path can be found fromwhich packets can be send, source and destination node is selected for communication.

In this way, here routing toward primary user attack and its belief propagation baseddefense strategy from cognitive radio network is described.

References

[1] L. Akter and B. Natarajan, “A Two-Stage Power and Rate Allocation Strategy for Secondary Users in Cognitive Radio Networks,” J. Comm., Special Issue on Cognitive Radio Enabled Communication and Networking, vol. 4, no. 10, pp. 781-789, Nov.2009.
[2] L. Akter and B. Natarajan, “Distributed Approach for Power and Rate Allocation to Secondary Users in Cognitive Radio Networks,” IEEE Trans. Vehicular Technology, vol. 60, no. 4, pp. 1526-1538, May 2011.
[3] E. Hossain, D. Niyato, and Z. Han, Dynamic Spectrum Access in Cognitive Radio Networks. Cambridge Univ., 2009.
[4] S. Haykin, “Cognitive Radio: Brain-Empowered Wireless Communications,” IEEE J. Selected Areas in Comm., vol. 23, no. 2, pp. 201-220, Feb. 2005.
[5] J. Mitola III, “Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio,” PhD thesis, KTH Royal Inst. Of Technology, 2000.
[6] N. Nie and C. Comaniciu, “Adaptive Channel Allocation Spectrum Etiquette for Cognitive Radio Networks,” Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Networks, pp. 269-278, Nov. 2005.
[7] R.C. Pereira, R.D. Souza, and M.E. Pellenz, “Using Cognitive Radio for Improving the Capacity of Wireless Mesh Networks,” Proc. IEEE Vehicular Technology Conf., Sept. 2008.
[8] Y. Yuan, P. Bahl, R. Chandra, T. Moscibroda, and Y. Wu, “Allocating Dynamic Time-Spectrum Blocks in Cognitive Radio Networks,” Proc. Eighth ACM Int’l Symp. Mobile Ad Hoc Networking and Computing, pp. 130-139, Sept. 2007.
[9] A. Goldsmith, Wireless Communications. Cambridge Univ., 2005
[10] R.D. Taranto, H. Yomo, P. Popovski, K. Nishimori, and R.Prasad, “Cognitive Mesh Network under Interference fromPrimary User,” Wireless Personal Comm., vol. 45, no. 3, pp. 385-401, May 2008.
[11] K.R. Chowdhury and I.F. Akyildiz, “Cognitive Wireless Mesh Networks with Dynamic Spectrum Access,” IEEE J. Selected Areas in Comm., vol. 26, no. 1, pp. 168-181, Jan. 2008.
[12] D.I. Kim, L.B. Le, and E. Hossain, “Joint Rate and Power Allocation for Cognitive Radios in Dynamic Spectrum Access Environment,” IEEE Trans. Wireless Comm., vol. 7, no. 12, pp. 5517-5527, Dec. 2008.
[13] R. Etkin, A. Parekh, and D. Tse, “Spectrum Sharing for Unlicensed Bands,” Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Networks, pp. 251-258, Nov. 2005.
[14] O. Ileri, D. Samardzija, T. Sizer, and N.B. Mandayam, “Demand Responsive Pricing and Competitive Spectrum Allocation via a Spectrum Server,” Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Networks, pp. 194-202, Nov. 2005.
[15] K. Bian and J.M. Park, “MAC-Layer Misbehaviors in Multi-Hop Cognitive Radio Networks,” Proc. US - Korea Conf. Science, Technology, and Entrepreneurship (UKC ’06), Aug. 2006.
[16] R. Chen, J.M. Park, and J. Reed, “Defense against Primary User Emulation Attacks in Cognitive Radio Networks,” IEEE J. SelectedAreas in Comm., vol. 26, no. 1, pp. 25-37, Jan. 2008.
[17] W. Wang, H. Li, Y. Sun, and Z. Han, “Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Systems,” Proc. Conf. Information Sciences and Systems (CISS ’09), Mar. 2009.
[18] G. Jakimoski and K.P. Subbalakshmi, “Denial-of-Service Attacks on Dynamic Spectrum Access Networks,” Proc. IEEE Int’l Conf. Comm. Workshops (ICC Workshops ’08), May 2008.
[19] X. Chen, K. Makki, K. Yen, and N. Pissinou, “Sensor Network Security: A Survey,” IEEE Comm. Surveys and Tutorials, vol. 11, no. 2, pp. 52-73, June 2009.
[20] A. Sampath, H. Dai, H. Zheng, and B.Y. Zhao, “Multi-Channel Jamming Attacks Using Cognitive Radios,” Proc. 16th Int’l Conf. Computer Comm. and Networks, Aug. 2007.
[21] Z. Jin, S. Anand, and K.P. Subbalakshmi, “Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks,” Proc. IEEE Int’l Conf. Comm. (ICC ’09), June 2009.
[22] R. Maheshwari, J. Gao, and S.R. Das, “Detecting WormholeAttacks in Wireless Networks Using Connectivity Information,”Proc. IEEE INFOCOM, May 2007.
[23] T. Zhou, R.R. Choudhury, P. Ning, and K. Chakrabarty, “P2DAP -Sybil Attacks Detection in Vehicular Ad Hoc

Networks," IEEE J. Selected Areas in Comm., vol. 29, no. 3, pp. 582-594, Mar. 2011.
[24] S. Kurosawa1, H. Nakayama1, N. Kato1, A. Jamalipour2, and Y. Nemoto1, "Detecting Blackhole Attack on AODV-Based Mobile Ad hoc Networks by Dynamic Learning Method," Int'l J. Network Security, vol. 5, no. 3, pp. 338-346, Nov. 2007.
[25] Z. Yuan, J.B. Song, and Z. Han, "Interference MinimizationRouting and Scheduling in Cognitive Radio Wireless MeshNetworks," Proc. IEEE Wireless Comm. and Networking Conf., Apr.2010.
[26] A.T. Ihler, J.W. Fisher, R.L. Moses, and A.S. Willsky, "Nonparametric Belief Propagation for Self-Localization of Sensor Networks," IEEE J. Selected Areas in Comm., vol. 23, no. 4, pp. 809-819, Apr. 2005.
[27] H. Li and D.K. Irick, "Collaborative Spectrum Sensing in Cognitive Radio Vehicular Ad Hoc Networks: Belief Propagation on Highway," Proc. IEEE Vehicle Technology Conf. (VTC), May 2010.
[28] B. Frey, Graphical Models for Machine Learning and Digital Communications. MIT, 1998.
[29] J.S. Yedidia, W.T. Freeman, and Y. Weiss, "Understanding Belief Propagation and Its Generalizations," Exploring Artificial Intelligence in the New Millennium, pp. 2282-2312, Morgan Kaufmann, 2003.

Author Profile

Mrs. Dhanashree Yogesh Jangam received Bachelor of Degree in Computer science & Engineering from Karmveer Bhaurao Patil College of Engineering, Satara, India in 2006. Currently she is pursuing her Master of Engineering in Computer Science and Engineering from Jayawantrao Sawant College of Engineering Hadapsar Pune, India. She has a 7 years of Teaching Experience. She is currently working as Lecturer in Computer Engineering Department of JSPM's Jayawantrao Sawant Polytechnic, Hadapsar, Pune India. Her research interest includes Network Security, Information Security, mobile communication.

Prof. Aruna K. Gupta received Bachelor of Degree in computer engineering in 1998 from Pune University, India and the Master of Technology degree in computer engineering in 2010 from VTU University, India.She has a 14 years of Teaching Experience. She is currently working as Associate Professor in Information Technology Department of JSPM's Jayawantrao Sawant College of Engineering Hadapsar, Pune, India Her research interest includes Network Security, Information Security, mobile communication, wireless communication, Computer Network.