An Improved Distance Vector by Naming and Protecting from Wormholes in Wireless Sensor Networks

Leelavathy S. R

Abstract*—Node localization becomes an important issue in the wireless sensor network as its broad applications in environment monitoring, emergency rescue and battlefield surveillance, etc. fundamentally the DV-Hop localization mechanism function well with the support of beacon nodes that have the potential of self-positioning. However, if the network is invaded by a wormhole attack, the attacker can tunnel the packets via the wormhole link to cause severe impacts on the DV-Hop localization process. The distance- vector propagation phase during the localization even aggravates the positioning result, compared to the localization schemes without wormhole attacks. In this paper, the impacts of wormhole attack on DV- Hop localization scheme and advanced DV -Hop localization. Based on this a label-based secure localization scheme is proposed to defend against the wormhole attack

***Index Terms*—Localization, sensors, beacons, naming, WSN, Distance vector, improved DV Hop.**

I. INTRODUCTION

A wireless sensor network (WSN) is a network made of numerous small independent sensor nodes. The sensor nodes, typically the size of a 35 mm, are self-contained units consisting of a battery, radio, sensors, and a minimal amount of on-board computing power. The nodes self-organize their networks, rather than having a pre-programmed network topology. Because of the limited electrical power available, nodes are built with power conservation in mind, and generally spend large amounts. With the reward of low cost, large scale, densely distributed, deployment, self-configuration, etc., wireless sensor networks (WSNs) have been applied in many fields to Monitor and control the physical world [1]. In WSNs, sensed data make no sense without the nodes position information. Hence, nodes are required to locate themselves in many WSN applications, such as environment monitoring, emergency rescue, and battlefield surveillance etc. A lot of protocols and algorithms are designed to solve the node's positioning problem, which are categorized into two categories: range-based and range-free [2]. Range based protocols calculate the location using the point-to point distance (or angle) estimates. Range-free solutions do not rely on the availability of range (or angle) estimates, so they need no expensive hardware. Considering that the hardware requirement of range-based solutions is inappropriate for resource-constrained WSNs, researchers are pursuing range-free localization techniques as a cost- effective alternative [2].

Manuscript published on 30 December 2014.
***Correspondence Author(s)**

Leelavathy S. R, Asst. Prof., Department of CSE, Dr. T. Thimmaiah Institute of Technology, Visvesvaraya Technological University, India.

In section II background and related work is discussed, in section III a description of wormholes is given in section IV types of wormholes, in section V the naming methodology is analyzed later in section VI DV hop algorithm for localization and improved DV hop algorithm in section VII and conclusion in section VIII.

II. BACKGROUND AND RELATED WOK

The DV-Hop localization can be applied as a range-free positioning algorithm [12],and works well with the assumption of isotropic networks. First, beacons, as location-known nodes, flood their positions through the network so that all nodes in the network can obtain the hop-counts to each of the beacons. Then each beacon, after receiving the position information from other beacons, calculates the average distance per hop, which is also broadcasted among its neighborhood, by averaging the distances to all other beacons over the hop counts. Sensors, being location unknown, estimate their locations to corresponding beacons, based on the received beacons' locations, average distance per hop and hop counts. As sensor networks usually work in a hostile environment, they are vulnerable to various malicious attacks.

III. WORMHOLE ATTACKS

In a typical wormhole attack[10], the attacker receives packets at one point in the network, forwards them through a wireless or wired link with much less latency than the default links used by the network, and then relays them to another location in the network. A wormhole is bi-directional with two endpoints, although multi-end wormholes are possible in theory. A wormhole receives a message at its "origin end" and transmits it at its "destination end." Note that the designation of wormhole ends as origin and destination are dependent on the context. We also assume a wormhole is passive (i.e., it does not send a message without receiving an inbound message) and static (i.e., it does not move).

Characteristics of a wormhole

The characteristics of wormholes is explained as follows 1. Two powerful adversary nodes placed in two strategic locations, 2.Advertise a low cost path to the sink3.All nodes in the network are attracted to them looking for an optimal route4. This is attack is usually applied in conjunction with selective forwarding or eavesdropping attack. The two adversary nodes advertise a route that's two hops away. Normal route is longer, so it's not used. The adversaries are now in control of all the traffic in the network.

Hard to detect because communication medium between the two bad nodes are unknown. Control and verify hop count. This limits the self-organizing criteria of an ad-hoc network. Use protocol that is not based on hop count. In geographic routing, a route is based on coordinates of intermediate nodes. But if adversary nodes can mimic its location, this doesn't work.

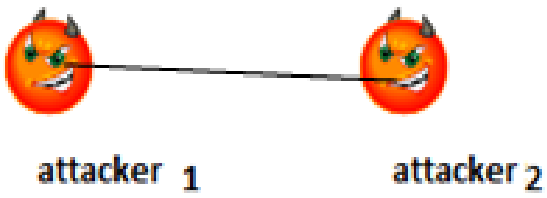

Figure 1: Typical wormhole attack

There are 4 steps to explain about a general wormhole attack.

Step 1: An attacker has two trusted nodes (or two colluded attackers each has one node) in two different locations of a network with a direct link between the two nodes.

Step 2: The attacker records packets at one location of a network.

Step 3: The attacker then tunnels the recorded packets to a different location.

Step 4: The attacker re-transmits those packets back into the network location from step 1. As shown in the figure 1.

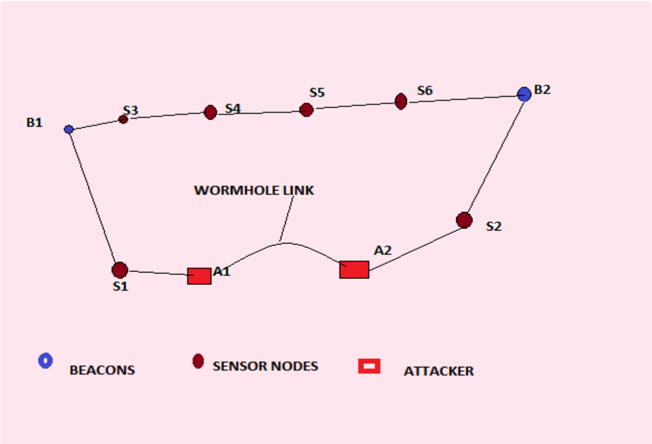

Figure 2. Types of nodes in WSN

The wormhole attack, as a typical external attack, can be easily launched by two colluding attackers without the system's authorization. When such attack is initiated, one attacker tunnels its received packets to another attacker, thus, packets can be delivered through a shorter path.

IV. WORMHOLE TYPES

Duplex Wormhole Attack: If node lies in the common transmission area of the two attackers. Simplex Wormhole Attack: if node lies only in the transmission range of either one attacker but not in the common transmission area of the two attackers. Pseudo Neighbor: A node is a pseudo neighbor if it can be communicated via the wormhole link. In the figure node S4 is under the duplex wormhole attack, node S3 is under the simplex wormhole attack. Node B6 is a pseudo neighbor of node B1.

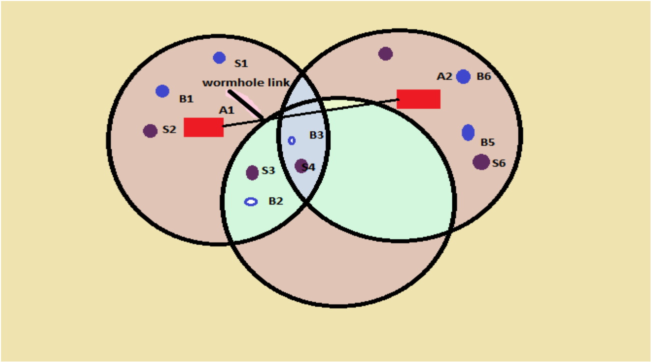

Figure 3 : Wormhole types

The wormhole attack can deteriorate the DV-Hop [3] localization dramatically. It not only reduces the hop-counts to all the beacons in the network, but also contaminates the average distance per hop. As a result, the location estimate will be far away from precision.

Beacon nodes

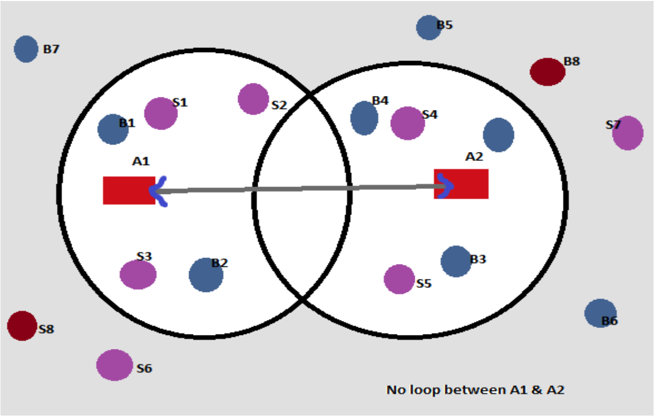

Figure 4: Beacon nodes

The classification of the beacon nodes is according to the following three properties. Self-exclusion property, Packet uniqueness property and Transmission constraint property. Here the focus is on defending against the wormhole attack in the DV-Hop localization process, i.e., overcoming the impacts of the wormhole attack on the DV-Hop localization. A label-based secure localization scheme which is wormhole attack resistant based on the DV-Hop localization process is proposed. The main idea of this scheme is to generate a pseudo neighbor list for each beacon node, use all pseudo neighbor lists received from neighboring beacon nodes to classify all attacked nodes into different groups, and then label all neighboring nodes (including beacons and sensors). According to the labels of neighboring nodes, each node prohibits the communications with its pseudo neighbors, which are attacked by the wormhole attack. Seeing as a wormhole attack is passive, it can have impact only when a message is being transmitted in the region in close proximity to a wormhole.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

To detect a wormhole attack a search procedure that floods the network with messages from a bootstrap node to enable all network nodes to count the hop distance from themselves to the bootstrap node. The search procedure is based on the hop coordinates technique [11].

Bootstrap Node: The bootstrap node x creates a search message with (i = idx) to flood the network. Next, the bootstrap node drops all search messages that originated from itself. The bootstrap node has the hop coordinate hopx = 0 and offsetx = 0.

Other Nodes: The search procedure the node A calculates its hop distance. Node B is a neighbor of node A. Hop A is the minimum number of hops to reach node a from the bootstrap node (x) and its initial value is MAX. The combination of hop_A and $offset_A$ is the hop coordinate for node A. N_A is the set of nodes that can be reached from node a in one hop, and $|N_A|$ is the number of nodes in N_A.

Algorithm: Search procedure for node A.

```
Step 1: INPUT: message (hop $_B$) from node B $\in N_A$
Step 2: for message ($hop_B$) from any B $\in N_A$ and not TIMEOUT do
Step 3: if $hop_B < hop_A$ then
Step 4: $hop_A = hop_B + 1$
Step 5: forward (message ($hop_A$)) to MAC
Step 6: else
Step 7: drop (message ($hop_B$))
Step 8: end if
Step 9: end for
Step 10: if $|N_A| == 0$ then
Step 11: $offset_A = 0$
Step 12: else
Step 13: $offset_A = \frac{\sum PB \in N_A (hop_B - (hop_A - 1)) + 1}{2(|N_A|+1)}$
Step 14: end if
Step 15: return $hop_A$ and $offset_A$
```

V. NAMING METHODOLOGY

Firstly, the beacon nodes are differentiated and labeled according to their geographic relationship under a wormhole attack. The sensor nodes are further differentiated and labeled by using the naming results of neighboring beacon nodes. After eliminating the illegal connections among the labeled neighboring nodes which are contaminated by the wormhole attack DV Hop can be conducted as shown in the figure 5.

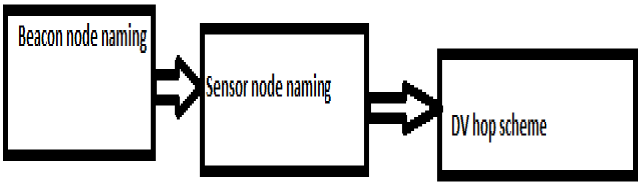

Figure 5: Flow diagram of naming

Wormhole attack detection algorithm

Basic Beacon Node Naming

```
Step 1: Each node Bi periodically broadcasts a Hello message to its neighbors and receives Hello messages to build its neighbor list.
Step 2: Each beacon node is initially labeled with 'N'.
Step 3: if Bi detects the duplex wormhole attack using scheme BL1 then
Step 4: Bi is labeled with 'D'.
Step 5: end if
Step 6: if Bi detects the simplex wormhole attack using schemes BL2 and BL3 then
Step 7: Bi is labeled with 'S'.
Step 8: end if
```

Sensor Nodes Naming

Sensor naming scheme SL1 is used to detect if a sensor node is under the duplex wormhole attack. Sensor Naming Scheme SL1: Each sensor node labeled with 'U' checks whether it violates the self-exclusion property. If yes, it determines that it is under the duplex wormhole attack. The sensor node will mark itself with label 'D'. Sensor nodes can use the following schemes to label themselves if they are under the simplex wormhole attack. Sensor Naming Scheme SL2: For a sensor labeled with 'U' but not 'D', if it receives two copies of the same message from its neighbor node, it can conclude that it is under the simplex wormhole attack and labels itself with 'S'. Sensor Naming Scheme SL3: For a sensor labeled with 'U' but not 'D', if it receives messages from two beacon nodes, it can calculate the distance between these two beacon nodes as their coordinates can be obtained from the messages. If the distance is larger than 2R, the sensor node can conclude that it is under the simplex wormhole attack and labels itself with 'S'.

Sensor nodes naming Algorithm

Sensor Nodes Naming

```
Step 1: Initially, each sensor node is labeled with 'N'.
Step 2: Each sensor labels itself with 'U' if it receives an Alert message from a neighboring beacon.
Step 3: if Sensor Si is labeled with 'U' then
Step 4: Si builds the two attacked beacon sets based on the received Alert messages.
Step 5: Si conducts the sensor nodes naming schemes SL1, SL2, SL3 and SL4.
Step 6: if Si is labeled with 'S' then
Step 7: Si conducts the extended sensor nodes naming schemes ESL1, ESL2 and ESL3.
Step 8: end if
Step 9: end if
```

VI. DV-HOP ALGORITHM

Conventional DV-Hop algorithm [9] positioning process is divided into three phases

Unknown node and compute nodes each beacon minimum hops.

1）Beacon nodes broadcast their locations to the neighbors of information packets, including the jump number field is initialized to 0. Receiving node records to each beacon nodes having the minimum number of hops, ignoring a beacon node from the same large number of hops a packet.

Then hop count plus one, and forwarded to the neighbors. Through this method, all nodes in the network to be able to record each beacon node under the minimum number of hops. Calculate unknown node and beacon node's genuine hop distance. Each beacon nodes according to the first stage record other beacon nodes position information and the distance hops, using the equation (i) estimate the average hop actual distance.

Calculate and obtain the unknown node average hop distance.

Beacon nodes by saving the coordinates of the other beacon nodes and the minimum number of hops using the equation (i) in the network calculate the average hop distance:

$$c_i = \sum_{i \neq j} \frac{\sqrt{(x_i - x_j)^2 - (y_i - y_j)^2}}{\sum_{i \neq j} hop_{ij}} \qquad \text{-------(i)}$$

Among $(x_i,y_i),(x_j,y_j)$, are the beacon coordinates of node i and j, hop_{ij} is a beacon nodes i and j, the minimum number of hops between. Then, the beacon node will calculate the average distance per hop fields with a packet with a lifetime of broadcasting to the network, the unknown node record only received the first average distance of each jump, and forwarded to the neighbors. This strategy ensures that the most recent beacon node from the node receives the value of the average distance per hop. Unknown node receives the average hop distance; according to the recorded number of hops to each beacon node calculate the hop distance. Using Trilateration measurement or maximum likelihood estimation method to calculate its own position. Unknown node uses the second phase to each record jump distance beacon nodes using Trilateration measurement or maximum likelihood estimation method to calculate their coordinates.

DV-Hop algorithm analyzes the deficiencies

In the DV-Hop algorithm, taken between beacon nodes as the average distance per hop beacon nodes unknown node to the average distance per jumping, jumping distance and jumping through each multiplied by the number to represent the unknown nodes and beacon nodes the distance between. However, in actual network topology beacon node to the unknown node is often not a straight path; use the DV-Hop algorithm will bring a greater distance error [7].

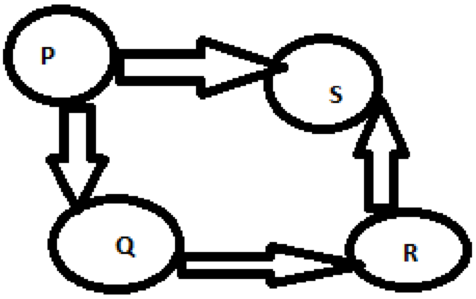

Figure 6: Node path

As Shown in Figure 6, take any four nodes P, Q, R, S. assuming the beacon node a node, the distance between the beacon nodes of 1m. Since DV-Hop algorithm, for unknown node d, a beacon nodes to the unknown node d is the distance 4m. However, this distance is much larger than the actual distance between two points, as the beacon node a to unknown node d paths that are not straight connection. However, in practical wireless sensor network environment, the majority of the beacon nodes and unknown nodes are connected to form a polygonal line, Therefore, using the average hop distance and the product of the number of hops is defined as the distance of a beacon node to an unknown will cause large errors. DV-Hop localization algorithm assumes that the network average hop distance is the same, thereby reducing the positioning accuracy, especially when unknown beacon node under test and beacon node is one hop distance. In fact, one hop distance can be shorter or longer, not completely equal. And the beacon nodes for a single hop communication unknown nodes, the actual distance between them may be much smaller than or is much larger than the average hop distance, The DV-Hop algorithm average hop distance is instead of the actual distance between them, which will bring a larger positioning error.

VII. IMPROVED DV-HOP ALGORITHM

DV-Hop Exist improved algorithm For DV-Hop itself instead of the average distance of each average hop distance limitations. Literature [4] proposed a weighted average hop distance improved method .The set threshold, the unknown node accepts M hop within anchor nodes and weighted according to the hop count to calculate the integrated average hop distance. And literature [5] in consideration of the angle between the three adjacent nodes on the distance, and puts forward a set of adjacent nodes overlap angle calculation methods to improve the positioning accuracy. These two are from the original DV-Hop algorithm to calculate the average distance limitations to start, but have increased the unknown node to an anchor node distance complexity.

Concrete steps to improve the process described below:

Procedure 1: Broadcast packets anchor node and compute the distance between the anchor node and neighboring nodes. Anchor nodes broadcast packets containing numbers, location coordinates, the number of hops and priority information. Ordering Priority equals 0 means that the first stage of anchor nodes, the highest priority. Because of this study taking into account the first non-distance ranging, and within one hop distance may be far less than the average distance, Based on the reference ranging RSSI[8] approach within a hop distance of the measurement more accurate. When you want to locate unknown nodes and anchor nodes to one hop, the RSSI can directly calculate the distance between them and save. So within one hop gained the unknown node hops, and priority information, and the new position of these nodes can be used as the next anchor node, the number of effective expansion anchor node.

Procedure 2: Unknown node will get the information to upgrade to the new anchor node, Using trilateration measurement to fix its location, when the unknown nodes to obtain three or more of the anchor node information, through trilateration measurement [9] to calculate the coordinates of its positioning. The node has been located as a new anchor node.

First, the unknown node within hop upgraded to anchor node, while the newly generated priority anchors anchor node set lower than the original priority. Therefore, the new anchor node Priority equals 1. The lower the priority value, the higher the priority. Low priority anchor nodes only in the high priority the number of anchor nodes are considered insufficient to complete the positioning when coming up as the reference node. And these new anchors also can be help to solve the previous positing problem. It should be noted that, if the number is less than three anchor nodes, the node can't locate the unknown, but can keep the node information to be used again when the next condition is satisfied, but also improve the location accuracy.

Procedure 3: Average hop distance estimates First, from the unknown node with the nearest anchor node to each of the other anchor node distance divided by the minimum number of hops between them to get the average number of hops. And the obtained average hop distance and the original average hop distance to the arithmetic mean of the average hop distance instead of the original. Using equation (2) obtained more accurate average hop distance, closer to the actual position.

D^1=D/2+d_{ab}/2hop$_{ab}$--------------------------(ii)

Among D is the original average hop distance,d_{ab} is the distance between beacon node and b, Hop$_{ab}$ is the hops between anchor nodes, D^1 is the average hop for the final correction hops.

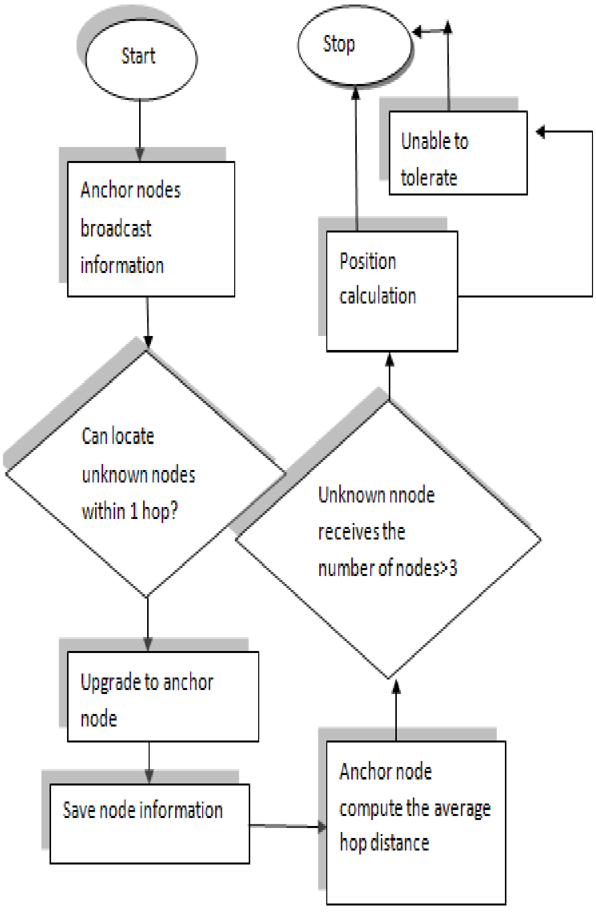
Start
Stop
Unable to tolerate
Anchor nodes broadcast information
Position calculation
Can locate unknown nodes within 1 hop?
Unknown nnode receives the number of nodes>3
Upgrade to anchor node
Save node information
Anchor node compute the average hop distance

Figure 7: improved algorithm flow chart

VIII. CONCLUSION

In this paper, the severe impacts of the wormhole attack on the Hop based localization in wireless sensor networks are analysed. To tackle this secure problem, A name-based secure localization scheme to detect and resist the wormhole attack for the DV-Hop localization process. The proposed scheme works well in the scenario when the network has no packet loss, and the transmission ranges of all nodes are identical. In future work will extend the secure localization scheme to tolerate the packet loss. Also will consider the scenario when different types of nodes have different transmission ranges. Also This paper first introduces the original through the DV-Hop algorithm, pointing out its deficiencies, and analyzing the reasons for its deficiencies, as well as areas for improvement. Based on this, a new algorithm for DV-Hop algorithm, the broadcast data packet priority increasing, effectively to expanse the anchor nodes. Also optimizes network average hop distance estimates the new calculation of the average hop distance calculation is more accurate, realistic position than the original algorithm, effectively reduce the error, given the improved algorithm for DV-Hop flowchart .

REFERENCES

1. N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low cost outdoor localization for very small devices," pp. 28–34, 7 2000.
2. T. He, C. Huang, B. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-Free Localization Schemes for Large Scale Sensor Networks," in Proc. of ACM MOBICOM, 2003, pp. 81–95.
3. D. Niculescu and B. Nath, "Ad Hoc Positioning System (APS) using AOA," in Proc. of IEEE INFOCOM, 2003.
4. Hu Yu, Li Xuemei based on DV-HOP algorithm for wireless sensor network node positioning technology. Shanxi: Taiyuan University of Technology, 2012,5
5. Zhang Xiaolong, Xie Hui-ying wireless sensor networks in an improved DV-Hop localization algorithm Hunan: Wuhan University of Technology, 2008,3.
6. D Niculescu,B Nath. Ad-Hoc Positioning System(APS)[J].IEEE GlobalTelecommunications, 2001, 5: 2926-2931.
7. Zhang Xiaolong, Xie Hui-ying, Zhao Xiaojian wireless sensor networks in an improved DV-Hop localization algorithm [J]. Journal of Computer Applications, 2007,27 (11) :2672 -2674.
8. YunWang,XiaodongWang,DeminWang,Agrawal,D.P.ARSSIbasedDVhopAlgorlthimforWirelessSensorNetworks[J].IEEETransaetions011ParallelandDistributedSystems,2009,20(10):1540.1552.
9. Zhangshu Peng wireless sensor network positioning technology research [D]. Guangzhou: South China University of Technology, 2010.
10. Detecting Wormhole Attacks In Wireless Sensor Networks Yurong Xu, Guanling Chen, James Ford and Fillia Makedon
11. Y. Xu, J. Ford and F. Makedon, A variation on hop counting for geographic routing, Proceedings of the Third IEEE Workshop on Embedded Networked Sensors, 2006.
12. K. Langendoen and N. Reijers, "Distributed localization in wireless sensor networks: a quantitative comparison," Compute. Networks, vol. 43, no. 4, pp. 499–518, 2003.

AUTHOR PROFILE

Leelavathy S. R, Assistant Professor, Department of CSE, Dr.T.Thimmaiah Institute Of Technology, KGF. her area of interest is Wireless Sensor Networks, attended many national and international conferences and had published many papers in national and international journals.