SECURING THE LOCATIONS OF SENSORS USING VIRTUAL CO-ORDINATES

Pruthvi H.S[1], Thivya G[2]

[1,2]Assitstant Professors, Department of ISE, TJIT

Abstract

A network topology is the design of connections which includes nodes and links. When the nodes change their positions, the topology either increases or decreases and hence methods for obtaining the maps that preserves the topology from the virtual coordinates is presented. Firstly Received Signal Strength(RSS) technique which relies on frequency parameter for distance calculation between the nodes is presented. Next another approach known as Location Aware Routing Technique (LART) which relies on latitudinal and longitudinal values for the distance estimation is presented. Lastly the proposed approach of DALD (Distance based Attack Localization and Detection) which is a counter measure to restore/ preserve the network region and a methodology to overcome the disadvantages of the existing frequency based approaches is implemented. The proposed T&S mapping (Track and Sector) based user check maintains a record of the communicating nodes which tracks the sector in which the node lays. It improves the communication by avoiding hidden node problem which distorts the mapping co-ordinates and other malicious access in the network path. Besides, the AOD (Angle Of Deviation) improves the accuracy of detection and localization based on angular presence verification on each and every transmission, allowing secure nodes to communicate, minimizing the anonymous distortions in the network mapping.

Keywords: *RSS, LART, DALD, AOD*

--***--

I. INTRODUCTION

A Wireless Sensor Network (WSN) is defined as a network of apparatus indicated as nodes which can sense the surrounding and relay the information gathered from the monitored area via wireless links; the information is forwarded to the sink which is confined to the same network through multiple hops or connected to external network (e.g the Internet) via a gateway. Virtual Coordinate Routing (VCR) and Geographical Routing (GR) are the two major categories where the routing is carried out based on the address for variety of networks like Wireless Sensor Networks[1]. Geographical routing mainly depends on the information like location of nodes that can be accessed by a Global Positioning System (GPS) or algorithms based on localization. In many of the applications the use of GPS is too costly and infeasible. Analog measurements like delay in time, strength of the signal are more prone to errors.

VCR relies on Virtual Coordinate System (VCS) that distinguishes each node in the topology by a coordinate vector which has the shortest distance to each of its one hop neighbors and this scheme uses distance as parameter to make the forwarding decisions. Connectivity information such as physical locations of the nodes with respect to X-Y directions are lacking in VCS.

Received Signal Strength technique relies on VCS in order to preserve the map that represents the topology. Since the signals are more prone to errors due to external noise, interference, multipath etc, obtaining the exact location of sensor nodes is difficult and thus Location Aware Routing and Distance based routing are the techniques that provides better accuracy in determining the distances between the nodes.

II. LITERATURE SURVEY

In the paper,―GPSR: Greedy perimeter stateless routing for wireless networks,‖[2] B.Karpand H.T.Kung proposed Greedy Perimeter Stateless Routing (GPSR).Greedy Perimeter Stateless Routing (GPSR), a novel routing protocol for wireless datagram networks that uses the positions of routers and a packet's destination to make packet forwarding decisions. When a packet reaches a region where greedy forwarding is impossible, the algorithm recovers by routing around the perimeter of the region.

In the paper ―Geometric ad-hoc routing: Of theory and practice,‖[3] F.Kuhn, R.Wattenhofer, Y.Zhang and A.Zollinger proposed geometric ad-hoc routing, in which Greedy Other Adaptive Face Routing (GOAFR) is one of the techniques.GOAFR is a combination of greedy routing and face routing.Whenever possible, the algorithm tries to route in a greedy manner, in order to overcome local minima with respect to the distance from the destination, face routing is employed. In face routing mode, GOAFR restricts the searchable area and improves the performance of both average case and worst case networks.

In the paper ―Geological routing in wireless sensor networks‖[4] Dulanjalie C. Dhanapala and Anura P. Jayasumana proposed routing in WSNs. Geo-Logical Routing (GLR) is a novel technique that combines the advantages of geographic and logical routing to achieve higher routability at a lower cost. By switching between geographic routing and logical routing, GLR overcomes local minima in the respective domains. Disadvantages of geographic routing, which relies on physical location information, include cost of node localization or/and use of GPS.

In the paper [5] Dulanjalie C. Dhanapala and Anura P. Jayasumana proposed Clueless Nodes to Network-Cognizant Smart Nodes. A novel scheme that allows individual nodes in sensor networks to achieve network/topology-awareness by listening to regular packets associated with applications. The scheme does not need node localization using unreliable analog measurements or a costly training phase.

In the paper ― Detection of tricking attacks based on cluster analysis‖[6], Srividhya A and Anitha M proposed the analysis based on the clusters that renders the theoretic assist of employing the RSS-based spatial correlation to achieve spoofing intrusion detection. It is even revealed that RSS readings from wireless sensor nodes can vary to the extreme points and hence must cluster together. Partitioning Around Medoids Method is used to accomplish clustering analysis in RSS. In the presence of noise and other disturbances in environment, the PAM method is more vigorous than K-means method.

III. EXISTING SYSTEM

RSS based distance calculation and Attack Detection: The aim is to determine the location of sensor nodes based on the frequency i.e the force required for a packet to be transmitted to the neighboring nodes. The WLAN frequency would be randomly distributed among the nodes in the topology for transfer of packets. The source node broadcasts the packet encapsulating the frequency which it transmits the packet along with the time stamp and its own location. When the neighboring nodes receive the packet, they extract the necessary information to calculate the distance between itself and the node from which it has received the packet. Thus the location of the node that has received the packet can be estimated from the distance and sender’s location parameters. The process repeats until all the nodes in the topology know their own location. All the nodes act as anchor nodes which have a coordinate vector which holds the distances to the neighboring nodes and also their locations. Virtual Coordinate System takes its role when the node in the topology enters into exhaust state when the battery power goes low, memory resource depletion etc. The node that establishes link to such node now determines the next nearest node with the help of vector table and establishes new link to that node and erases the link to the old node. This implies that the node which has depleted has been removed from the topology. Since the signal strength is more prone to errors due to external noise, interferences, multipath fading etc. the distance thus calculated is not highly accurate.

The main aim in attacker detection technique is to design strategies that employ the distinctive spatial information without the direct use of location as the attacker’s positions are not known. For this RSS technique is used. The signal strength is observed at a set of reference points or landmarks even if it is affected by external noise, multipath interference and other environmental conditions. These landmark positions are nearly associated to the transmitter’s physical location and distance to these landmarks is measured. If the transmitters are at the same geographical location then RSS values are identical else values are distinct in physical space. Thus strong spatial correlation properties are presented by the RSS values.

The main strategy used in detecting the attackers is when a node operates in the same frequency as that of sender and send the packet at the same time interval, the distance calculated using RSS technique would be same and hence the location determined would be the same. Hence the technique should detect that node as malicious node which drops the packets which are on the way to the destination. The main disadvantage is, in any network there can be more than one node that operates at the same frequency range and thus there would be the chances of detecting the legitimate nodes as malicious nodes or attackers.

IV. PROPOSED SYSTEM

Location Aware Routing and Detection (LART):

In this technique, the initial assumption is each and every node is aware of their location in terms of virtual coordinates and wishes to share when they broadcast the packets to their immediate neighbors. These coordinates are converted to latitudinal and longitudinal values in order to obtain the distance in the same units using standard formulae. The coordinates are shared by broadcasting the packets to the neighbors within a specific radio range.

Distance based Attack Localization and Detection (DALD):

The main idea behind DALD approach is the distance that each of the data navigates from source to destination, it determines the distance depending on two parameters, the Time Of Arrival (TOA) and source node’s position. Each time when the source transmits the packet, the distance travelled by that packet is calculated. The disadvantages associated with the RSS technique can be overcome in this technique. The frequency parameter where the RSS relied upon is omitted from this design. It implies that the sensor node can accomplish its behavior/work at any frequency and more than a node has the freedom to operate in same frequency region. Hence interference is expelled from the consideration. In contrast with RSS technique, this method ensures every node has dissimilar geographical locations even though they appear in the same frequency region and distribute the common frequency. The sender transmits the packet encapsulating its location and the time stamp. Initial assumption is every node knows their own location and share while broadcasting the packets. The DALD performs as follows:

a) Estimate the source node’s location in terms of co-ordinates.
b) Determine the destination node’s location which is self-known.
c) Figure out the distance between source and destination after employing the coordinate locations of sender and receiver.
d) Maintain a localization table and keep track of difference in distance of the request packet.
e) For each transmission from respective nodes, ensure that the data is turning up from the same source based on the distance already calculated.
f) Suppose the data is arriving from different localization point then decline the packet and dismiss the connection.
Angulation based Localization:

Steps for Delaunay triangulation:-

Step 1: Send a hello message within the distance by using distance formula. Once the message is received, acknowledge the source of the message with the location information.

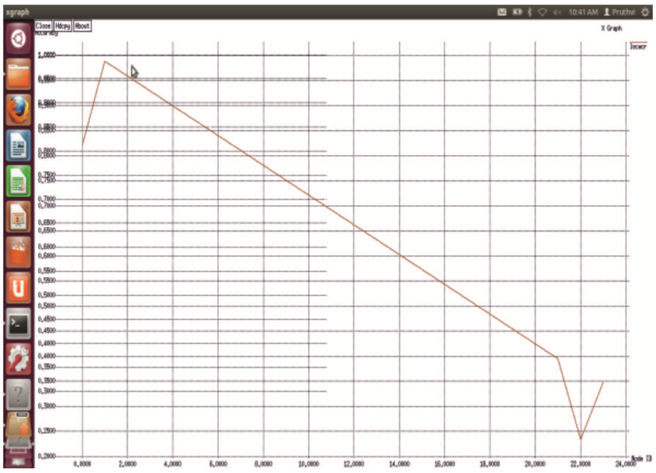
Step 2: Link the source node with its neighboring nodes such a way that it has to form a triangle. Let us denote this graph as G1.

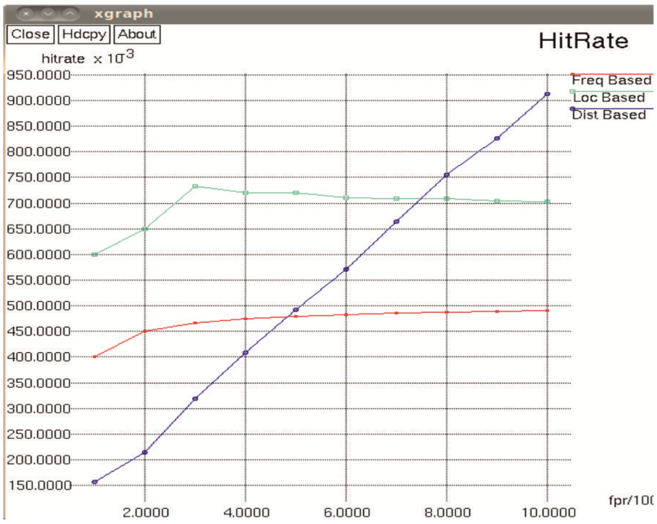
Step 3: The constraint for the Delaunay triangulation graph G is any two nodes are linked if and only if the other node resides within the transmission region of the node. The graph G1 so obtained after step 2 is a non-planar graph and includes few non-Delaunay edges, which lead to the edge crossing. Once the edge crossings are removed in step 3, Delaunay triangulation graph G is obtained which may or may not have non-Delaunay edges but are planar in nature. Once all the steps are carried out, the nodes need not remember all the neighboring nodes but only those that form the edges with it in the Delaunay triangulation graph. The algorithm is quite simple and effective in determining the angle between the nodes.

Equations used in Location Aware Routing Technique:-

Assume that the coordinates of two nodes i and j are (xi,yi,zi) and (xj,yj,zj) respectively. The following formulae are used for distance calculation.
a) lat(i)= sin(zi/ 6371)
b) lon(i)= tan2(xi,yi)
c) lat(j)= sin(zj/ 6371)
d) lon(j)= tan2(xj,yj)
e) latd = lat(j)-lat(i)
f) lond = lon(j)-lon(i)
g) a=((sin(latd/2))*(sin(latd/2))) + (cos(lat(j)) * cos(lat(i))) * ((sin(lon(j)/2))*(sin(lon(i)/2))]
h) c = 2 * tan2((sqrt(a), sqrt(1-a))
i) d = round(6371 * c)
Equation used in Distance based routing technique:-
The distance between the nodes (x1,y1) and (x2,y2) is Sqrt(x2-x1) ^2+ (y2-y1)^2.

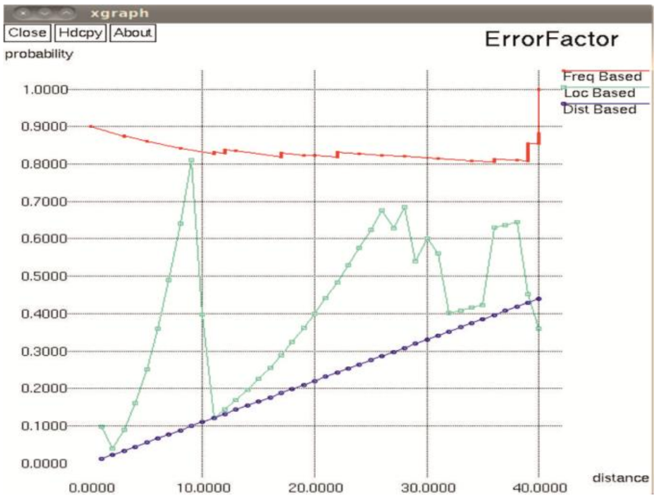
V. SIMULATION RESULTS





Graph that shows the hit rate comparison of RSS, LART and DALD techniques.

In the above graph, false positive rate is taken along x-axis and hit rate along y-axis. Hit rate is the probability of detecting false packets generated by the attacker. False packets are those that are generated by the attacker and that flood the network. In this graph, Distance based localization has a maximum hitrate of 91% which is 42% better than frequency based and 21% better than location aware routing techniques.



Graph that shows the error factor comparison of RSS,LART and DALD techniques. In the above graph, distance is taken along x-axis and the probability of error is taken along y-axis. Error factor is the drop in accuracy in finding the node location. The overall error factor of distance based localization is only 40%. Whereas the overall localization error of location aware and frequency based techniques are 80% and 90% respectively. Localization error increases as the distance increases.

VI. CONCLUSION

Existing system relies on Received Signal Strength technique in order to determine the location of sensor nodes that also uses frequency as basis to determine the attackers. If two nodes are operating at the same frequency then it will be detected as malicious node, but in the real world more than one node can operate at the same frequency or frequency region.

Proposed system relies on Location Aware Routing Technique (LART) and Distance based Attack Localization and Detection(DALD) technique. LART uses latitudinal and longitudinal values to determine the distance between the nodes and DALD uses Euclidean’s distance to determine the distance and this distance is used for detecting the attackers for each of the transmissions. Track and sector method efficiently determines the number of hops the node is laying from the source and the quadrant in which it lies.

The simulation is carried out using the NS2 simulator. Firstly the sensor nodes have been deployed in the topography of the network. Each of these nodes is assigned with the unique node-id. Assumption is each node is aware of its own location and shares it with other nodes, finally the malicious nodes are detected and only data from the authenticated nodes is received at the destination.

Finally the distance calculated between the nodes is more accurate and efficient using the DALD than LART and the existing RSS techniques. Results of graph also reveal that the number of drop packets detected in DALD is maximum than LART and RSS techniques.

REFERENCES

[1] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, ― Wireless Sensor Networks Security‖ , Auerbach Publications, CRC Press 2006.

[2] B.Karpand H.T.Kung,―GPSR: Greedy perimeter stateless routing for wireless networks,‖ in Proc. 6th ACM MobiCom, 2000, pp. 243–254.

[3] F. Kuhn, R. Wattenhofer, Y. Zhang, and A. Zollinger, ―Geometric ad-hoc routing: Of theory and practice,‖ in Proc. 22nd ACM PODC , Jul. 2003, pp. 63–72.

[4] Dulanjalie C. Dhanapala and Anura P. Jayasumana proposed ―Geological routing in wireless sensor networks‖, in Proc. 13th ACM Int. Workshop Geo. Inf. Syst., 2005, pp.71-78.

[5] Dulanjalie C. Dhanapala and Anura P. Jayasumana proposed ―Clueless Nodes to Network-Cognizant Smart Nodes‖, Proc. 27th IEEE IN- FOCOM, pp. 789–797, 2008.

[6] Srividhya A and M Anitha , ― Detection of tricking attacks based on cluster analysis‖, International Journel of Innovative Research in Computer and Communication Engineering.

[7] A. Rao, S. Ratnasamy, C. Papadimitriou, S. Shenker, and I. Stoica, ―Geographic routing without location information,‖ in Proc. 9th Int. Conf. Mobile Computer Networks, 2003, pp. 96–108.

[8] Q. Cao and T. Abdelzaher, ―Scalable logical coordinates framework for routing in wireless sensor networks,‖ Trans. Sensor Netw., vol. 2, pp. 557–593, Nov. 2006.

[9] J.BachrachandC.Taylor,―Localization in sensor networks,‖in Handbook of Sensor Networks. Hoboken, NJ, USA: Wiley, 2005, ch. 9.