Detection and Elimination of Malicious Beacon Nodes in Broadband Based Wireless Networks

Dr.P.Suresh [#1], Jeril Kuriakose [*2], Shekeela N [#3], Ananda Raj. M.D[*4]

[#1] *Head, Department of Computer Science, Salem Sowdeswari College, Salem -10*

[*2] *Assistant Professor, Department of Computer Science, The Kavery College of Engineering, Salem.*

[#3] *Assistant Professor, Department of Computer Science, Bharathidasan University, Trichy.*

[*4] *Assistant Professor, Department of Computer Science, Loyola College ,Chennai-34.*

Abstract: Detecting the cheating or vulnerable beacon node is an essential problem in wireless sensor networks. In wireless sensor networks, beacon nodes are used to locate or trace the exact location of the object. Now-a-days it is challenging to find out the exact location of a beacon node from the existence of a cheating beacon node. Even after finding out the location of cheating beacon node, there are chances of errors that can likely happen. This paper aims to localize the cheating beacon nodes using trilateration algorithm and later compare it with Maximum Likelihood Expectation method to obtain maximum accuracy in localisation. The error obtained during localisation can be reduced. For implementation purpose we installed TinyOS in MICA2 motes and simulated using ns-3 network simulator.

Keywords: Maximum likelihood expectation, trilateration, security, distance-based localisation, wireless networks.

I. INTRODUCTION

The wireless ad hoc and sensor networks are on a gradual rise in the recent decade. This is because of reduced cost in setup, maintenance, etc. Advancements in radio frequency spectrum improve the data rate for communication. Many devices belong to wireless ad hoc and sensor networks; one among them is Beacon Node. Beacon node is a device that looks similar to a wireless modem; and its working is quite related to Light House. A special node or anchor is required for algorithms based on Beacon [1], [2], [3], [4], [5], [6], [7], [8]. Beacon nodes are used to find the current location of any device (mobile phones, objects, people, etc.). It does that by transmitting beacon frames periodically or at regular intervals. Usually beacon frames are used to advertise the occurrence of Wireless modem or an Access Point (AP). Each beacon frame carries some details about the configuration of AP and little security information for the clients.

When the technologies are on a massive upswing, the need for security of the relevant technologies arises. There can be several occasion where the beacon nodes can be vulnerable to security breach. Later due to the security breach the beacon node starts to cheat by giving false information. In the presence of cheating beacon nodes the chances of localisation gradually decreases. Many papers locate cheating beacon nodes but are not sure how accurate the results are. So, to overcome this we locate the cheating or vulnerable beacon node using trilateration and compare the results with Maximum Likelihood Expectation.

II. LOCATING USING TRILATERATION ALGORITHM

Beacon nodes are widely used for tacking and localisation. Beacon nodes can also be used as navigational or route-finding device. With the help of beacon nodes the user can find out the exact location. Beacon nodes emit beacon frames periodically; the location can be identified with the obtained beacon frames.

Consider a scenario like a hotel or museum, there can be many occasions where people go out of track. If there are beacon nodes installed in various locations, people can trace out there location very easily. There are several other uses like tracking lost objects, people etc. Beacon nodes can execute better only when they are truthful. Now-a-days hackers are on a rise; they can easily get into a system and change its settings. They can hack our beacon nodes and change its location to some other place, by doing this people get confused leading to a bad impression about the organization (i.e., hotel, museum etc.).

In the figure 1 [10] given below, beacon nodes B1, B2, B3 and B4 are setup initially and behave honestly at that moment. Later after security breach the beacon change its position as given in figure 2 [10].

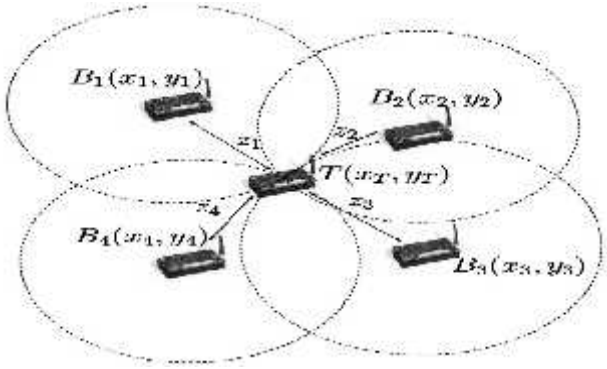

Fig. 1. Initial setup of beacon nodes

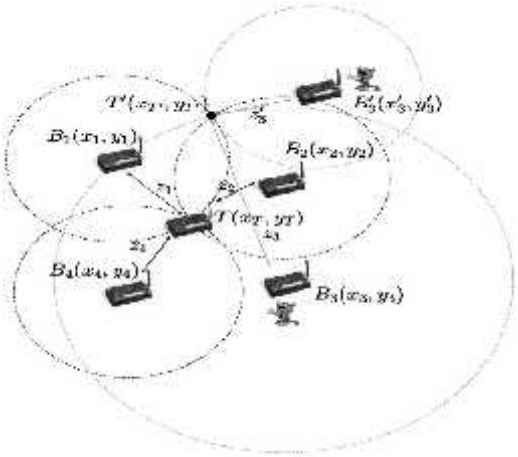

Fig. 2. Beacon nodes after attack

Trilateration is a method of finding a position of an object. The position can be located with the help of coordinates of other three known objects. The trilateration works as follows:

i. Consider I am lost in some place. To find out our exact location we ask three different people. The first person says that I am 15 kilometres away from place 'A' 11 and is towards east direction. With that I plot a circle with radius 15 kilometres as shown in figure 3. In that circle, I can be in anywhere on the circumference.

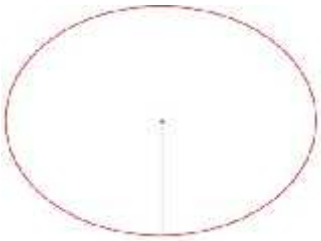

Fig. 3. Circle with radius 15 km

ii. Next I ask some other person and he says that I am 10 kilometres away from place 'B' and is towards south direction. So, I draw a circle with radius 10 kilometres as shown in figure 4. From the new circle we get two points where the circles intersect, from this we can find out that we are located in either one of the two points.

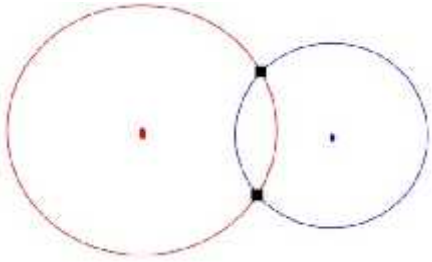

Fig. 4. Two circles with radii 15 km and 10 km respectively

iii. Later I ask some other person and he says that I am 8 kilometres away from place 'C' and is towards west direction. So, again I draw a circle with radius 8 kilometres as shown in figure 10. From this circle I can identify a single position where all the three circles intersect each other. This way I can find out my location logically.

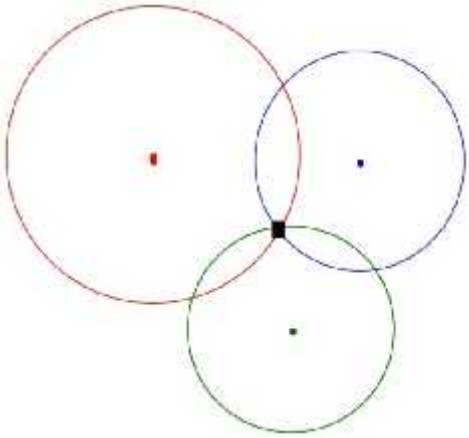

Fig. 5. Three circles with radii 15 km, 10 km and 8km respectively

The mathematical computation of trilateration is as follows

We begin with three circles or sphere with centre C_1, C_2 and C_3, radius Z_1, Z_2 and Z_3 from points B_1, B_2 and B_3 (beacon node location). The general equation of the sphere is

$$\sum_{k=1}^{d} (B_k - C_k)^2 = Z^2$$

The three circles or sphere equation can be modified as follows,

$$Z_1^2 = B_1^2 + B_2^2 + B_3^2 \quad (1)$$

$$Z_2^2 = (B_1 - D)^2 + B_2^2 + B_3^2 \quad (2)$$

$$Z_3^2 = (B_1 - i)^2 + (B_2 - j)^2 + B_3^2 \quad (3)$$

Subtracting equation (2) from equation (1), we get

$$Z_2^2 - Z_1^2 = (B_1 - D)^2 + B_2^2 + B_3^2 - B_1^2 - B_2^2 - B_3^2 \quad (4)$$

$$B_1 = \frac{Z_1^2 - Z_2^2 + D^2}{2D} \quad (5)$$

From the first two circles we can find out that the two circles intersect at two separate points, i.e.

$$D - B_1 < B_2 < D + B_1 \quad (6)$$

Substituting equation (5) in equation (1), we can obtain

$$Z_1^2 = \frac{Z_1^2 - Z_2^2 + D^2}{2D} + B_2^2 + B_3^2 \quad (7)$$

$$B_2^2 + B_3^2 = Z_1^2 - \frac{(Z_1^2 - Z_2^2 + D^2)^2}{4D^2} \quad (8)$$

We can find out the intersection of two spheres in equation (8).

Substituting equation (1) with equation (3), we get

$$Z_3^2 = (B_1 - i)^2 + (B_2 - j)^2 + Z_1^2 - B_1^2 - B_2^2 \quad (9)$$

$$B_2 = \frac{Z_1^2 - Z_3^2 - B_1^2 + (B_1^2 - i)^2 + j^2}{2j}$$

$$= \frac{Z_1^2 - Z_3^2 + i^2 + j^2}{2j}$$

$$B_2 = \frac{i}{j} Z_1 \quad (10)$$

From equation (5) and equation (10) we get the values of B_1 and B_2 respectively. From that we can find out the value of B_3 from equation (1),

$$B_3 = \pm\sqrt{Z_1^2 - B_1^2 - B_2^2}$$

From the above equation we can say that, B_3 can have either positive or negative value. If the circle (having B_3 as a point) intersect any other circle precisely at one point, then B_3 will get a value zero. If it intersects at two or more points it can get either positive or negative value.

The algorithm for setting up the beacon nodes according to trilateration are as follows,

1. Start
2. {
3. Deploy the beacon nodes
4. {
5. Set the initial co-ordinates (latitude & longitude) for each beacon node
6. Cluster beacon nodes into a set of three or more
7. }
8. Trilaterate each group of beacon nodes to a centre point and save the location reference in M1*
9. Individually trilaterate all the beacon nodes with the neighbouring group and save the location references in M2*, M3*, etc.
10. Repeat the above steps for all the beacon nodes
11. }
12. End

(* M1, M2, M3, etc., are different memory with different location reference)

The algorithm for finding out the malicious beacon nodes are as follows,

1. Start
2. {
3. Trilaterate each group of beacon nodes to a centre point and save that location
4. {
5. Compare the obtained location with location reference (M1)
6. If comparison not satisfied
7. {
8. Trilaterate all beacon nodes (individually) of the particular group (which does not satisfy the above comparison) with the neighbouring group
9. Compare the obtained results with the location references (M2, M3, etc.)
10. {
11. Separate the mismatched beacons node location and save the new location in Mn
12. }
13. }
14. If comparison satisfied, no cheating nodes occur
15. }
16. End

There can be many possibilities of getting an error with the above method. In our next section we compare the

obtained results with Maximum likelihood expectation (MLE) method.

III. MAXIMUM LIKELIHOOD EXPECTATION

Maximum likelihood Expectation is a technique that is used in statistics to find the maximum probable value from previously obtained results. The results obtained from maximum likelihood expectation can be used as the parametric values for further experiments or simulations.

A. *Probability density function*

Probability density function (pdf) sorts out the required area for the random variable to occur. Consider a random sample (x_1, x_2, …, x_n) from an unknown population has data vector x = (x_1, x_2, …, x_n). The probability density function *f(x|w)* is

$$f(x = (x_1, x_2, \ldots, x_n)|w) = f_1(x_1|w) f_2(x_2|w) \ldots f_n(x_n|w)$$

where,

x is random sample,

w is parameter.

Consider a scenario where n (number of trials) = 10, w = 0.4 and x = (0, 1, …, 10), then the probability density function will be

$$f(x \mid n = 10, w = 0.4) = \frac{10!}{x!\,(10 - x!)}(0.4)^x (0.6)^{10-x}$$

The parametric value has more number of successive probabilities. The graph below shows the probability density function for the above equation,

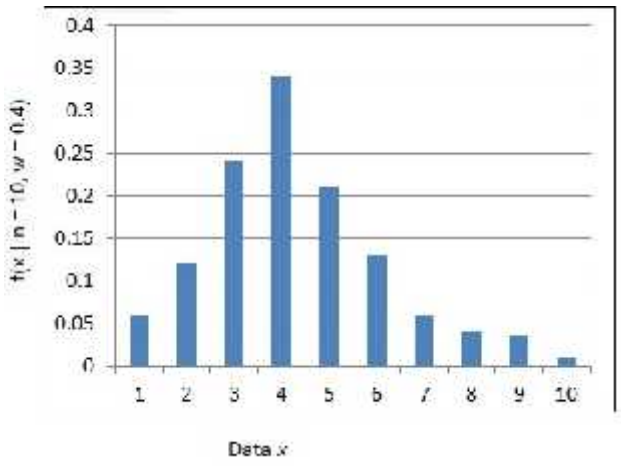

Fig. 6. Probability density function

B. *Likelihood function*

From figure 6 we can find out that pdf with w = 0.5 and x = 4 is more likely to occur, so the maximum likelihood expectation is as follows,

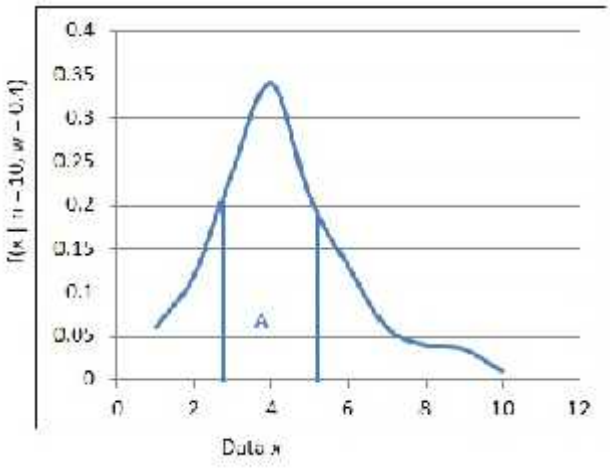

Fig. 7. Maximum Likelihood Expectation

Area covered by 'A' in figure 4 is the maximum probable value that can occur. Finding out the 'most likely' function is the principle of Maximum Likelihood Expectation. Probability distribution function sorts out the most probable value, which leads for the estimation of expected value.

IV. SIMULATION AND RESULTS

Our simulation was carried out in 600m x 600m two dimensional environment. Deploying the beacon node accurately is very important. First three beacon nodes were placed randomly and the trilateration point is found. A beacon node is placed on the trilateration point. Any one of the first three nodes is selected and it acts as the trilateration point of the newer nodes that are going to be deployed. The above process is repeated until the final node is deployed. We deployed around 59 nodes (around 1 node for every 8m x 8m), spread evenly from the above method. Figure 8 shows the deployment of the beacon nodes.

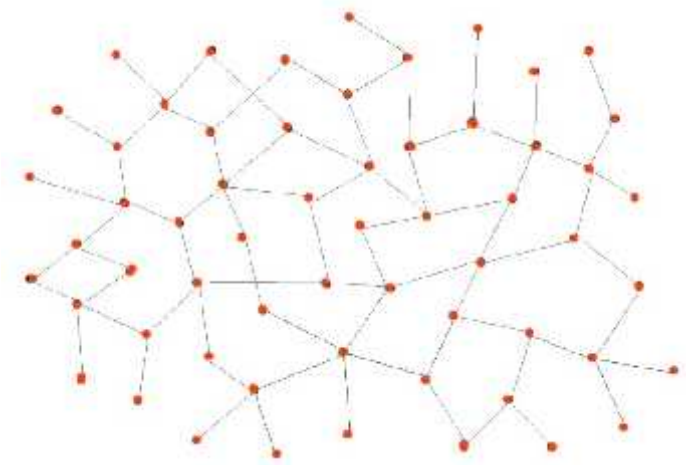

Fig. 8. Deployment of beacon nodes

A. *Experiment using trilateration technique*

Beacon nodes were compromised (making it transmit false information regarding its current location) randomly and the malicious beacon nodes were found out using trilateration technique. The error occurred during finding out the malicious beacon nodes from random samples were noted down. Figure 9 shows the error in location discovery and figure 10 shows the time taken to locate the malicious beacon nodes during simulation.

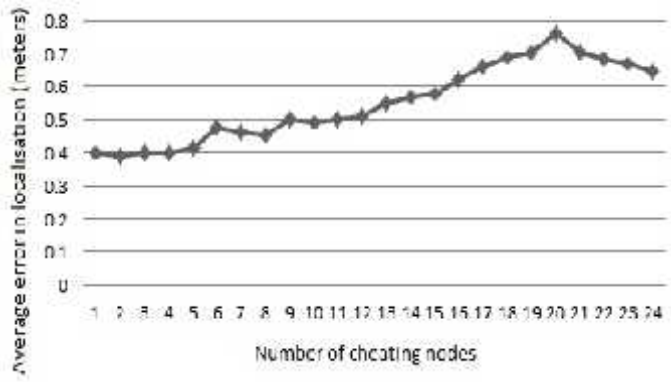

Fig. 9. Average error in location discovery

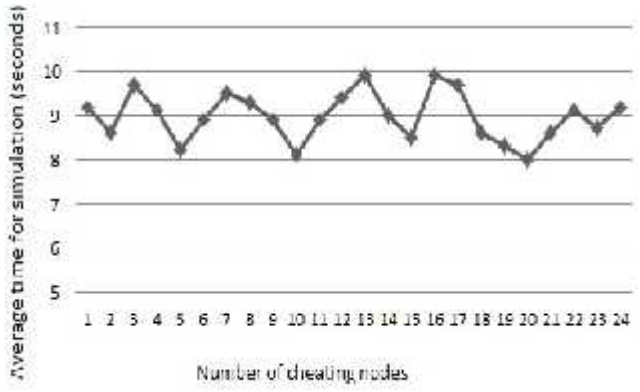

Fig. 10. Average time for simulation

B. *Comparing with Maximum Likelihood Expectation*

Maximum likelihood function has a list of initial location references of the beacon nodes. The malicious beacon nodes obtained are compared with the maximum likelihood function. Comparing the results obtained reduces the error in location discovery. Figure 11 shows the average error in locating malicious beacon nodes.

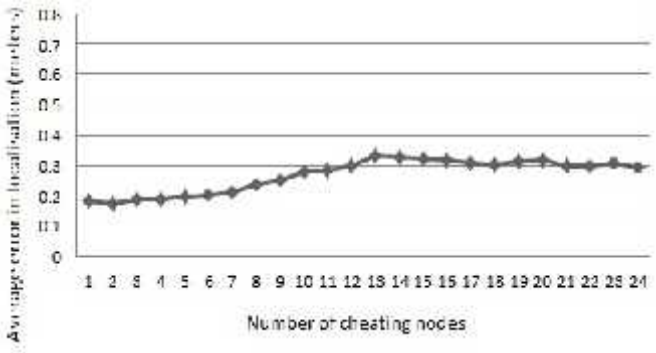

Fig. 11. Average error after comparing with maximum likelihood function

V. CONCLUSION

We have discussed about locating malicious beacon nodes using trilateration technique and compared the results obtained with Maximum Likelihood Expectation. This way we were able to reduce the error attained during localisation. Using Maximum Likelihood Expectation we can obtain consistent and efficient results. Our results show that as the malicious beacon nodes increases the simulation time and error obtained during location discovery slightly increases. The accuracy obtained can be used as assistance in some wireless applications.

REFERENCE

[1] R. Want, A. Hopper, V. Falcao, and J. Gibbons, "The Active Badge Location System," *ACM Trans. Information Systems*, vol. 10, pp. 91 - 102, 1992.

[2] J. Liu, Y. Zhang, and F. Zhao, "Robust Distributed Node Localization with Error Management," *Proc. ACM MobiHoc*, 2006

[3] M.W. Carter, H.H. Jin, M.A. Saunders, and Y. Ye, "SpaseLoc: An Adaptive Subproblem Algorithm for Scalable Wireless Sensor Network Localization," *SIAM J. Optimization*, 2006.

[4] P. Bahl and V.N. Padmanabhan, "RADAR: An In-Building RFBased User Location and Tracking System," *Proc. IEEE INFOCOM*, 2000.

[5] D. Niculescu and B. Nath, "DV Based Positioning in Ad Hoc Networks," *J. Telecomm. Systems*, vol. 22, pp. 267-280, 2003.

[6] N. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket Location-Support System," *Proc. ACM MobiCom*, 2000.

[7] R. Stoleru and J.A. Stankovic, "Probability Grid: A Location Estimation Scheme for Wireless Sensor Networks," *Proc. First IEEE Conf. Sensor and Ad Hoc Comm. and Networks (SECON '04)*, 2004.

[8] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-Less Low Cost Outdoor Localization for Very Small Devices," *IEEE Personal Comm. Magazine*, vol. 7, no. 5, pp. 28-34, Oct. 2000.

[9] In Jae Myung, "Tutorial on maximum likelihood estimation," *Journal of Mathematical Psychology*, 2003.

[10] Murtuza Jadliwala, Sheng Zhong, Shambhu Upadhyaya, Chunming Qiao and Jean-Pierre Hubaux, "Secure Distance-Based Localization in the Presence of Cheating Beacon Nodes," *IEEE Transactions on Mobile Computing*, 2010.

[11] http://en.wikipedia.org/wiki/3-sphere

[12] http://en.wikipedia.org/wiki/Trilateration