*International Journal of Engineering Research and Development*
***e*-ISSN: 2278-067X, *p*-ISSN: 2278-800X, www.ijerd.com**
*Volume 4, Issue 1 (October 2012), PP. 88-93*

# Secure Distance-based Localization in the Presence of Cheating Beacon Nodes

Sindhupriya.B[1], Madhuri Devi.K[2], Mrudula.V[3], Ashalatha.M[4], Sukumar Babu.B[5]

[1,2,3,4]*Student, Vijaya Institute of Technology for Women, Vijayawada-521108.*
[5]*Head of the Department, CSE, Vijaya Institute of Technology for Women, Vijayawada-521108.*

***Abstract—localization or location discovery in the presence of cheating beacon nodes is an important problem in mobile wireless ad hoc and sensor networks. Despite many significant research efforts in this direction, there is no sufficient condition to estimate the error bound. Although many algorithms were proposed to calculate the error bound using necessary and sufficient condition there occur some problems which cause the error in correct location discovery. This paper attempts to find a secure distance based location discovery in presence of beacon nodes and verify the accuracy and efficiency of the experiments using practical distance estimation error models.***

***Keyterms—beacon nodes, error bounding, localization, security, target node, wireless networks***

## I. INTRODUCTION

Location discovery in distributed wireless networks is the problem in determining the location of a (mobile) device in the network in an efficient and accurate fashion. The beacon or anchor nodes know their location in the network and can be placed in their position in the network. Distributed localization protocols classified into two categories which are Range-based and Range-free Techniques. The range based technique again divided into beacon-based and beacon free techniques. A target node which is moving in the network can be located using these beacon nodes. This beacon based locating technique helps to trace the movement of target node. Each beacon estimates the distance of their neighboring nodes.

Location information is of a paramount importance for wireless sensor networks. The accuracy of the collected data can significantly be affected by an imprecise positioning of interest. Despite the importance of the location information, real system implementations that do not use specialized hardware for localization purposes have not been successful. The algorithms are not much efficient for locating mobile node because they are not beacon based also the results are consistent for theoretical analysis and in practical they may show a large error. This became the drawback of the system.

## II. PROPOSED METHOD

In this paper, we propose a location estimation scheme that uses a probabilistic approach for estimating the location of a node in a sensor network. The localization scheme makes use of additional knowledge of topology deployment. Specifically, we first show that when the number of beacon nodes is greater than or equal to a given threshold, there do not exist any two-dimensional distance-based localization algorithms that can guarantee a bounded error. Hence occurrence of error is minimized and error bound for large number of beacons employed in real time situations.

## III. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system. The project "Secure distance based localization in the presence of beacon nodes" consisting network, location-based service and beacon movement detection modules.

Client-server computing or networking is a distributed application architecture that partitions tasks or workloads between service providers (servers) and service requesters, called clients. Often clients and servers operate over a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients. One essential research issue in sensor networks is localization, whose purpose is to determine the position of an object or event. In most localization systems, they assume that there are sets of beacon sensors (or simply beacons), which may or may not be aware of their locations and can periodically transmit/ receive packets. Neighbor-based (NB) scheme, beacons will keep track of their nearby beacons and report their observations to the BMD engine to determine if some beacons have been moved.

### A. Beacon Movement Detection

Each beacon reports its observed signal strengths, which are used by the BMD engine to compute each beacon's current location. The result is used to compare against its original location. In the NB scheme, each beacon locally decides if some neighboring beacons have moved into or out of their communication coverage range and reports its binary observations to the BMD engine.

**B. System Design**

A data flow diagram is graphical tool used to describe and analyze movement of data through a system. These are the central tool and the basis from which the other components are developed. The transformation of data from input to output, through processed, may be described logically and independently of physical components associated with the system. These are known as the logical data flow diagrams. The physical data flow diagrams show the actual implements and movement of data between people, departments and workstations.

**1) Data Flow Diagram**:

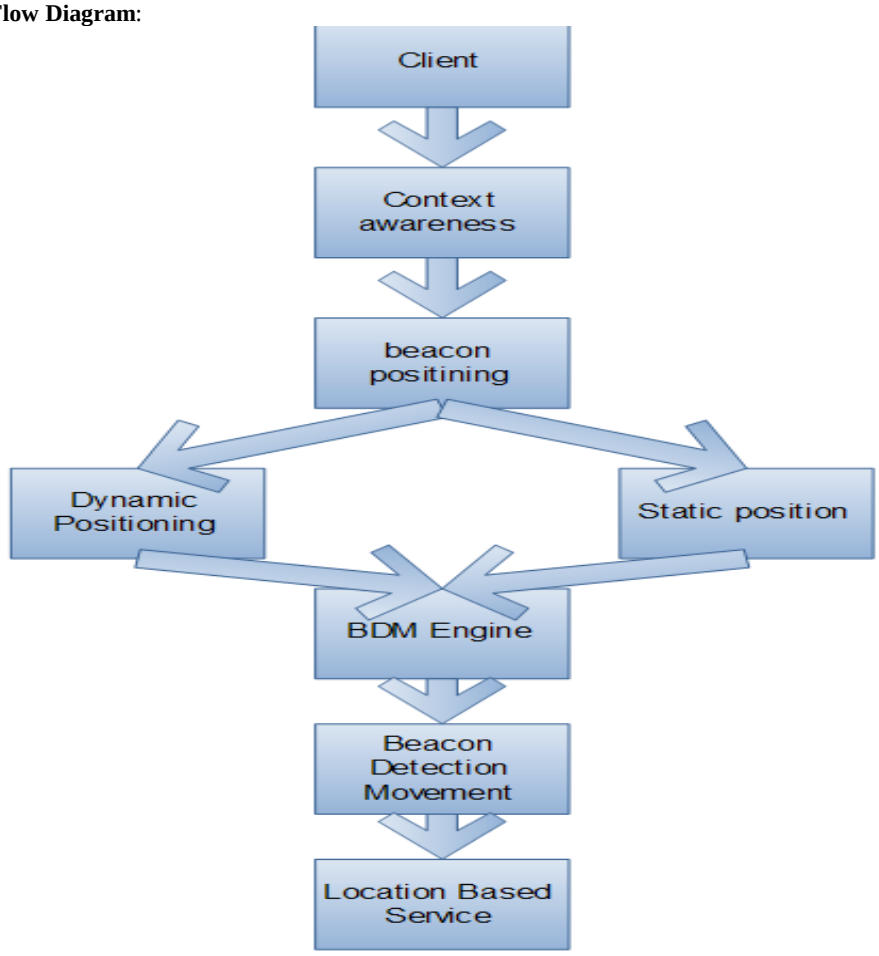


Fig. (a) DFD for Beacon Location Discovery

**C. Security Measures**

The protection of computer based resources that include hard ware, software, data, procedures and people against unauthorized user enters into the system can be protected by a security software.

***1) Security Software:*** system security refers to various validations on data in form of checks and controls to avoid the system from failing. It is always important to ensure that only valid data is entered and only valid operations are performed on the system by the user. The system employees two types of checks and controls to secure the system.

***2) Client Side Validation:*** Various client side validations are used to ensure on the client side that only valid data is entered. Client side validation saves server time and load to handle invalid data. Some checks imposed are:

- VBScript is used to ensure those required fields are filled with suitable data only. Maximum lengths of the fields of the forms are appropriately defined.
- Forms cannot be submitted without filling up the mandatory data so that manual mistakes of submitting empty fields that are mandatory can be sorted out at the client side to save the server time and load.
- Tab-indexes are set according to the need and taking into account the ease of user while working with the system.


Fig. (a) Client Login

***3) Server Side Validation:*** Some checks cannot be applied at client side. Server side checks are necessary to save the system from failing and intimating the user that some invalid operation has been performed or the performed operation is restricted. Some of the server side checks imposed is:

- Server side constraint has been imposed to check for the validity of primary key and foreign key. A primary key value cannot be duplicated. Any attempt to duplicate the primary value results into a message intimating the user about those values through the forms using foreign key can be updated only of the existing foreign key values.
- User is intimating through appropriate messages about the successful operations or exceptions occurring at server side. The server side has the authority to add or delete the customers.


Fig. (b) Server Login

Due to strict security, only valid clients can login into the network. If there is new user, the user must be register to acquire the services in the net work. Thus reduce the unauthorized users that enter into the network.

## IV. INPUT AND OUTPUT

After the server login into the system, it runs the server page and starts the server for the services that offers to the client by the server.


Fig. 1 Server login

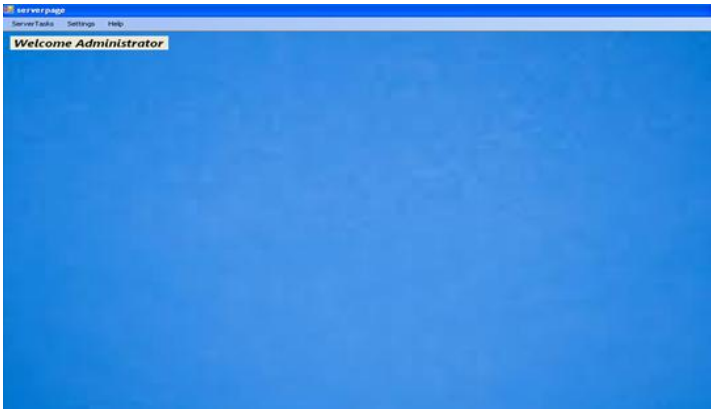


Fig. 2 Server page

After the client login, the client should enter the ip address of the node to find the target node.

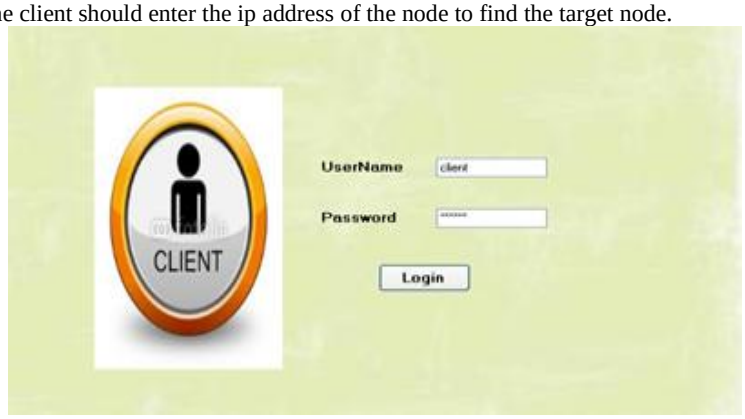


Fig. 3 Client login

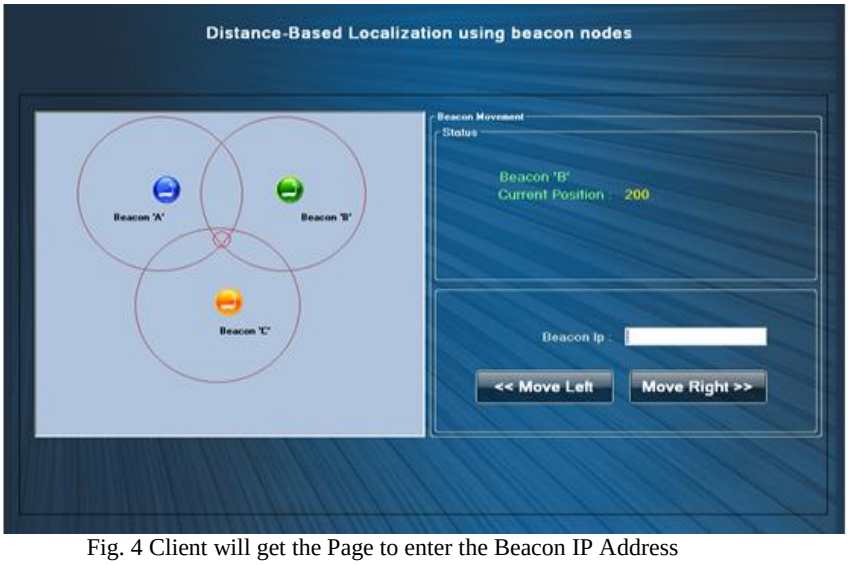


Fig. 4 Client will get the Page to enter the Beacon IP Address

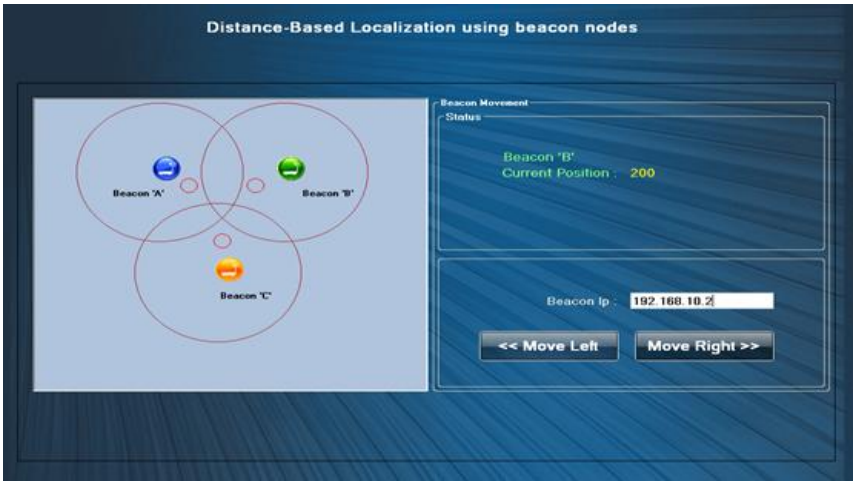


Fig. 5 Client will enter the ip address.

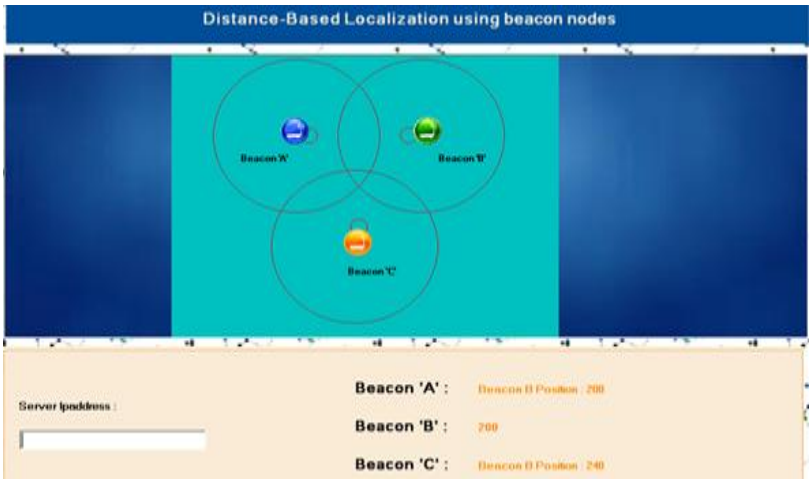


Fig. 6 After Client enters the Beacons IP Address it asks for the Server IP Address.

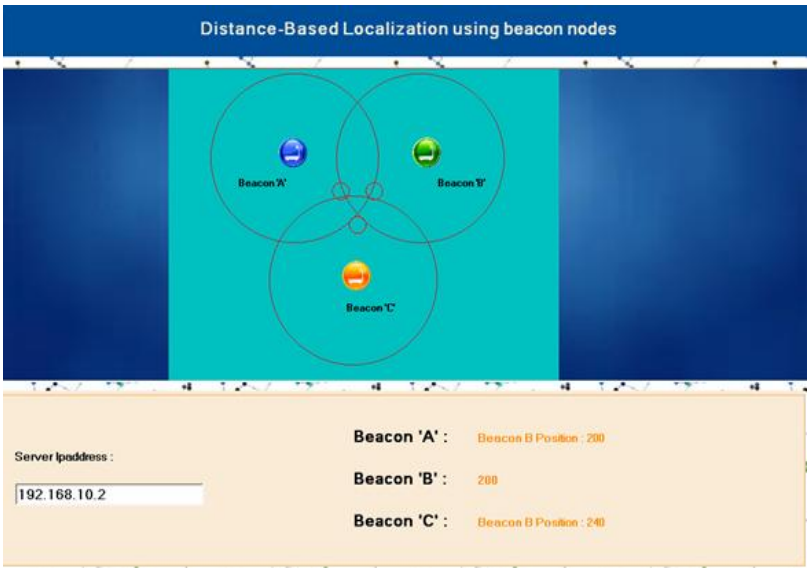


Fig. 7 Display (output) to the client

After entering the server ip address the output to the client is as shown above.

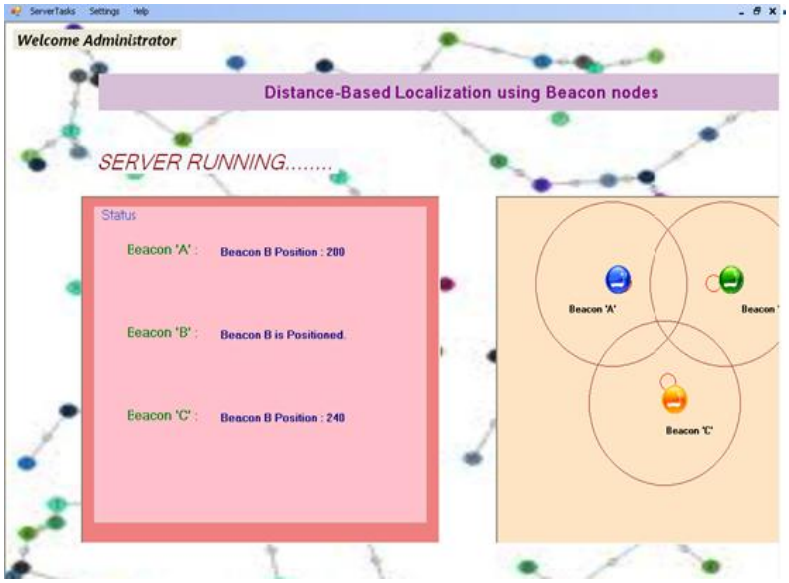


Fig. 8 Display to the Server

## V. ADVANTAGES

Distance based localization is the accurate localization technique in beacon based sensor network. Also, the fewer is the Beacon number, the better they can acquire their position knowledge either from a GPS device or by virtue of being manually placed and If beacons are higher in number they can be trapped and may produce wrong position result. In such conditions also distance based localization produce accurate results by providing some conditions.

## VI. CONCLUSION

In this paper, we have addressed the problem of secure distance-based localization in the presence of beacon nodes. By means of a sound mathematical analysis, we have derived the secure and robust distance-based localization in the presence of cheating beacons. Due to this client-server method the presence of cheating beacons can be reduced. Specifically, we have outlined the necessary and sufficient conditions for achieving a bounded localization error and to achieve the accurate results.

## REFERENCES

[1]. Behrouz A Forouzan, *Data communications and networking*, Fourth Edition.TMH.
[2]. S.Keshav, *An Engineering Approach to Computer Networks*-, 2nd Edition, Pearson Education
[3]. Abraham Silberschatz, Peter B. Galvin, Greg Gagne *Operating System Concepts*, 7th Edition, John Wiley.
[4]. Jochen Schiller,"*Mobile Communications*", *Addison-Wesley*. Second edition, 2004.
[5]. Charlie Kaufman, Radia Perlman and Mike Speciner, *Network Security - Private Communication in a Public World*, Pearson/PHI.
[6]. http://www.sourcefordgde.com
[7]. http://www.networkcomputing.com/