THE NEED FOR LIGHTWEIGHT LOCATION VERIFICATION ALGORITHMS FOR WIRELESS SENSOR NETWORKS

Rekha.K.S[1], Nischitha.M.V[2], Megha.B.S[3], Dr.T.H.Sreenivas[4]

[1]*Assistant Professor, Department of Computer Science & Engineering, N.I.E,Mysore(India)*
[2,3] *Department of Computer Science & Engineering, N.I.E, Mysore(India)*
[4]*Professor, Department of Information Science & Engineering N.I.E, Mysore(India)*

ABSTRACT

The Sensor nodes are important components in Wireless Sensor Networks. Authentication of nodes is a major concern because such nodes are more susceptible to various attacks. The main goal of this paper is to verify whether data coming from sensor is authenticated or not. The two different techniques namely an On Spot Verification and In-Region Verification are discussed. In the On spot verification, the location of the sensor nodes is verified with that of the registered value of that node. In the In-Region verification, the current location of the sensor nodes with respect to its neighbouring nodes is verified with the registered value of the node. If no change in the value has been taken place, then the data coming from that particular sensor is authenticated. The Two algorithms namely GFM (Greedy Filtering using Matrix) and GFT (Greedy Filtering using Trust ability indicator) are discussed. These techniques can be executed with the help of Android phones which have the built-in components that allow these phones to work in the manner similar to that of the sensor nodes. The Personal Computer (PC) is used as the Verification Centre or a Server to monitor the Android phones. This implementation should be cost effective, accurate and easily understandable.

Keywords: In-region, Localization ,Security, Sensor systems, On-spot, Verification Centre (VC), Wireless Sensor Networks(WSN's).

I. INTRODUCTION

WIRELESS sensor networks (WSNs) are a significant technology that has scope in research field [26]. Wireless sensor nodes operate in a cooperative and distributed manner. Such nodes are usually embedded in the physical environment and report sensed data to a central base station; however, for a sensor network to achieve its purpose, it is essential to know where the information is sensed [27].

Wireless Sensor Network is the network of sensors which are connected via Radio Signals. These sensors are controlled in the location known as the Verification Centre (VC). It contains information like GPS Location of the sensors, the location of its neighbouring sensors. Any data coming from the sensors are recorded in the VC. The data coming from the sensors may be hacked or sensors might be misplaced due to environmental changes. The existing system does not have this facility to identify these changes. This project intends to overcome these disadvantages the On spot verification, the location of the sensor nodes is verified with that of the registered value of that node, whereas in the second technique called the In-region verification, the current location of the sensor nodes with respect to its neighbouring nodes is verified with that of its registered value of that node. To deceive the VC into accepting wrong locations, multiple attackers can even collude together. For example, if a sensor has five neighbours and more than three of them are compromised, then the chance that the VC could still correctly verify the sensor's location is small [17].

LOCALIZATION in wireless sensor networks i.e., knowing the location of sensor nodes, is very important for many applications like environment monitoring, target tracking, and geographical routing [17]. The sensor nodes after the deployment cannot be manually maintained and monitored, security becomes critical. In such a scenario maintaining and monitoring of sensor node and their network of communication becomes a major issue in WSN. The data can be sent or accessed by any node in the network and providing authentication to access this data is critical preventing unauthorized users from gaining the information and hence the security becomes the major issue in Wireless Sensor Networks [18][19]. The attackers can compromise sensors and inject false location information; they can also interrupt signal transmission between sensors and contaminate distance measurements. Hence, the locations estimated in the localization process are not always correct sensor nodes typically employ low cost commodity hardware components unprotected by the type of physical shielding that could prevent access to a sensor's memory, processing, sensing and communication components[10].

Although some secure localization algorithms were proposed to help enhance sensors' resistance to attacks they cannot completely eliminate wrong location estimations. Therefore, the location verification is a necessary second line-of-defence against malicious attacks, which becomes the focus of this paper, which classifies previous location verification algorithms into two categories, namely, on-spot verification and in-region verification. On-spot verification is to verify whether a sensor's true location is the same as its estimated location (or with very small errors) whereas, In region verification is to verify whether a sensor's true location with respect to its neighbours is same as the estimated location with them. Since existing verification algorithms either require deployment knowledge or depend on hardware that are expensive a lightweight verification algorithm should be designed that can effectively perform on-spot verifications. Based on the application, the system can use either on-spot or in-region verification results. For On-spot verification, two algorithms can be used namely, the Greedy Filtering by Matrix (GFM) algorithm and the Greedy Filtering by Trust ability indicator (GFT) algorithm [17][14]. Both algorithms exploit the inconsistency between sensors' estimated locations and their neighbourhood observations. To perform in-region verification, initially the sensor is checked as to whether it is in the given range of verification region using probabilistic algorithm.

II. PROBLEM STATEMENT

In the existing system, the sensor nodes in WSN's are the major source of information in various applications. Such nodes should not be corrupted. But in the current scenario, these nodes are subjected to various attacks and also there is no provision to check the authentication of such nodes. The various ways in which these nodes can be corrupted are hacking, misplace of nodes due to environmental issues, complications within the sensor nodes such as Hardware malfunction, Software crash, virus attack etc. And also these nodes are generally placed in remote areas because of which frequent manual monitoring is not possible. Due to all the above stated reasons, sensor nodes are very vulnerable and sensitive. But in the existing system has new mechanisms to prevent the nodes from these hurdles. Hence, there is a need for a mechanism which can protect these nodes. This paper concentrate on the method which is simple, cost-effective and provides authentication to the sensor nodes that sense the data and send it to the controlling station.

III. RELATED WORKS

In recent years, a large number of localization schemes were proposed for wireless sensor networks. Localization refers to locating the position or area in which the sensor or object to be tracked. Based on the localization, many applications are emerging in the sensor network. One of main challenge in localization is that the process can be made erroneous by launching various attacks. Secure localization [1][2][13] has become a great concern in WSN's. In order to achieve this, various localization schemes have been designed. And also, existing localization schemes of WSNs are classified into two categories: range-based schemes and range-free schemes [1]. For range-based localization schemes, the distance or angle information is measured by RSSI (Received Signal Strength Indicator), TOA (Time of Arrival), Time Difference on Arrival (TDOA) and AOA (Angle of Arrival) [1]. For range-free localization schemes, the localization is realized based on network connectivity or other information, which can be obtained by DV-Hop, Convex Optimization and MDS-MAP [1].

In many tasks like as search, rescue, disaster relief, target tracking, node localization is inherently one of the system parameters. Node localization is required to report the origin of events, assist group querying of sensors, routing and to answer questions on the network coverage [3]. This paper reviews different approaches of node localization discovery in wireless sensor networks. When localization system [4] is node-centric, location verification is needed to verify the claimed locations of sensors. Wireless networks are vulnerable to spoofing attacks [5], which allows for many other forms of attacks on the networks. This project is designed to overcome such attacks. A method for both detecting spoofing attacks and spotting the positions of foes performing the attacks are introduced [6].The main aim is to overcome these hindrances with less software requirements. Due to the decreasing cost and the ease of installation of access points, indoor localization using WiFi signal strengths are becoming more and more popular [25].

Sensor nodes are spatially distributed to sense and monitor the physical changes throughout the environment to collect the data. The nodes also collect data from its surrounding nodes and the environments. These collected data are transmitted from one node to other through the wireless medium. Sometimes nodes are requested data from other nodes, in some cases the collected data of a node may be confidential and only visible to the authenticated nodes [20]. Wireless sensor have special characteristics because of total absence of infrastructure or administrative support these are wireless networks. They have limited bandwidth, energy constraints, self

configurable, low computational capabilities and easy to deploy [22]. Such networks provide a variety of consumer applications such as emergency rescue, disaster relief, smart homes, and patient monitoring, as well as industrial applications such as distributed structural health monitoring and environmental control, and military applications such as target identification and tracking. Many of the applications proposed for WSNs require knowledge of the origin of the sensed information [7].

In [8][12], Smart phones are used as a Sensors. It consists of two components namely Accelerometer and Gyrometer which is used to send the vibrations through Wi-Fi to the location centre(PC) [8]. A probabilistic procedure is designed to supply the self-assurance that a sensor is inside the verification region [9]. Security is important for many sensor network applications. As a result, WSNs are susceptible to many application-dependent and application-independent attacks like node replication attacks [10]. WSNs are often deployed in harsh environments, where an attacker node can physically capture some of the sensor nodes. Once a sensor node is captured then the attacker node can collect all the credentials like keys, identities etc . The attacker can modify the message and replicate in order to overhear the messages or interrupt the functionality of the sensor networks. Sensor network localization is not just trivial extensions to the traditional localization techniques like GPS and LPS. Hence Node self localization [11] is also an important criteria in WSN's.

The algorithm which is being implemented in this project has high fault tolerance to various attacks in WSN's [15]. This project can also be extended to provide a new approach for securing localization and location verification in wireless networks based on hidden and mobile base stations [16].

IV. ALGORITHMS USED

4.1. GFT and GFM

In this section, two algorithms discussed for on-spot verification are Greedy Filtering using Matrix and Greedy Filtering using Trustability-indicator. Both algorithms utilize the inconsistency between sensors' estimated locations and neighbourhood observations. They can be used in different scenarios according to the application's requirements. Suppose there are totally n sensor nodes in the field denoted by S1,S2,.....,Sn. For convenience, we assume sensor Si's ID is integer i where i = 0,1,2,..... [17]. In GFM algorithm, five n*n square matrices are calculated based on the reported information from sensors. In each round, if a sensor's indicator is higher than the threshold, the sensor is accepted as correctly localized sensor. Such iteration stops when all sensors' indicators become stable. Finally, the sensors that have indicator values lower than the threshold are detected and revoked. First, GFM explores the inconsistency directly by comparing the elements in two matrices, i.e., the Estimation Matrix and the Observation Matrix, while GFT detects the location anomalies indirectly based on the indicators which indicate the inconsistencies. Second, the GFM algorithm filters out bad locations as soon as one of the metric values is not accepted according to the threshold. Sensors not revoked will be verified in the final round. In GFT algorithm, instead, the good location claims are accepted first, and after multiple rounds when indicators of remaining sensors become stable, the sensors with indicators below the threshold will be revoked [17].

4.2 Centralized Localization Algorithms

In this section, the major centralized localization schemes are summarized.

4.2.1 Area Localization Scheme (ALS)

For large scale UWSNs [21], identifying the exact location of every unknown node may not be feasible. Therefore, an efficient Area Localization Scheme (ALS) is proposed for UWSNs. ALS was firstly proposed for terrestrial WSNs . This scheme estimates the position of every unknown node within a certain area rather than its exact location. The main responsibility of anchor nodes is to send out signals with different levels of power to localize unknown nodes. Unknown nodes simply listen to the signals and record the anchor nodes' IDs and their corresponding power levels. Together with collected data, the recorded information is sent to sink node. Sink node is assumed to know the positions of all anchor nodes and their respective transmitted power levels. Therefore, with proper signal propagation algorithms, sink node is able to draw out the map of areas divided by all the anchor nodes' transmitting signals. Then, sink node can localize unknown nodes [29].

4.2.2 Hyperbola-Based Localization Scheme (HLS)

Instead of using the commonly adopted circle-based detection and least squares algorithm based location estimation, this scheme utilizes the hyperbola-based approach for localization and a normal distribution for estimation error modelling and calibration [29].

4.2.3 Sensor Arrays-Based Localization Approach (SLA)

In this approach, the UWSN consists of sensor arrays. Each sensor array is equipped with an array of sensor nodes that are attached to the sensor array via wired connections. Each target waiting to be localized periodically emits a narrow-band acoustic signal. For each sensor array, using the negative log-likelihood function, sensor nodes which have received the signal can obtain the target locations and signal amplitudes. The maximum likelihood estimate of the target location is obtained based on the global likelihood function, which is the sum of the local likelihood function. MLSL approach does not need distance measurement and time synchronization [29].

4.2.4 An Probabilistic Localization Method (PLM)

To mitigate distance measurement error in localization process, multi-iteration measurement and least squares scheme are often adopted in terrestrial applications. However, in underwater applications, the multi-iteration scheme is not practical due to high communication cost. Meanwhile, it has been observed that the probability distribution of distance measurement error often follows a certain pattern, which can be utilized to further improve the localization accuracy. Both the uniform error distribution and normal error distribution are considered. Then, a Probabilistic Localization Method (PLM) is proposed to improve localization accuracy [29].

4.2.5 Large-Scale Hierarchical Localization (LSHL) Approach

In this approach [29], Surface buoys drift on water surface and get their locations from GPS. Anchor nodes can directly communicate with the surface buoys to get their absolute positions. Unknown nodes cannot directly communicate with the surface buoys but can communicate with anchor nodes to localize themselves. The whole

localization process is divided into two sub-processes: anchor node localization and unknown node localization [29].

4.2.6 Reactive Localization Algorithm (RLA)

Instead of localizing every single node in the network, RLA localizes a node that detects an event. Once a sensor node detects an event, RLA which consists of two steps starts. The first step is to find anchor nodes. The sensor node first broadcasts a hello message with its ID and energy level to its neighbours. By the K-Node Coverage Algorithm at least 4 non-coplanar anchor nodes are found. The second step is reactive localization of the sensor node. Once the selected anchor nodes receive localization request message, they reply with their location information. The sensor node hence localizes itself by quadrilateration. Due to additional process for anchor nodes' localization, energy consumption and communication overhead of RLA are high. Furthermore, accumulated localization error exists [29].

V. PROPOSED WORK

Currently, researchers have proposed many techniques to solve the above 2 issues. In this paper, the common attacks against localization are described.

- The verification system that overcomes the shortcomings of previous research.
- The verification system that verifies whether sensor's estimated locations are trustable.
- The verification system to provide On-Spot verification service.
- The verification system to provide In-Region verification service.
- Lightweight systems that do not require any dedicated hardware or infrastructures, and they do not incur high computation overhead at the sensor side, so that the verification system can be applied to low cost wireless sensor networks.

We use Android Phones as sensors, as it contain 2 components called Accelerometer and Gyrometer which are used to sense the vibrations. PC is used as the VC. All the Information will be recorded in PC.

5.1. STEPS TO BE FOLLOWED

We will place the Android Phone that we are using as sensors at the location where the vibrations or movement has to be sensed.

1. The location at where these sensors are placed are recorded in the Location Center(LC) with the help of GPS System by calculating its Latitude and Longitude values.
2. In the next step, if any activities that causes vibration occurs, then sensor will sense those vibrations and sends these signals to LC. Activities that cause the vibrations are footsteps, wind and any motion effect.
3. The VC on receiving these signals, verifies the authentication of data received. In On-spot verification, the authentication of data is carried out by comparing the location of the sensors with the recorded values. In the In-region verification, the location of the sensors is calculated with respect to its neighboring sensors.

4. The location center records the location of the sensors from which data is received, along with the location of its neighbors.
5. The distance between the sensor node and the neighbouring sensor nodes are also recorded. They are compared with the stored values.
6. Comparison is done based on the current GPS location of the sensor by calculating its latitude and longitude. If they are found to be same, then the data is authenticated or else the data is either hacked or misplaced. Such data is rejected.

The Fig .1 represents the general operation of a Wireless Sensor Networks. In this, S1, S2, S3, S4 represents the Sensor nodes.

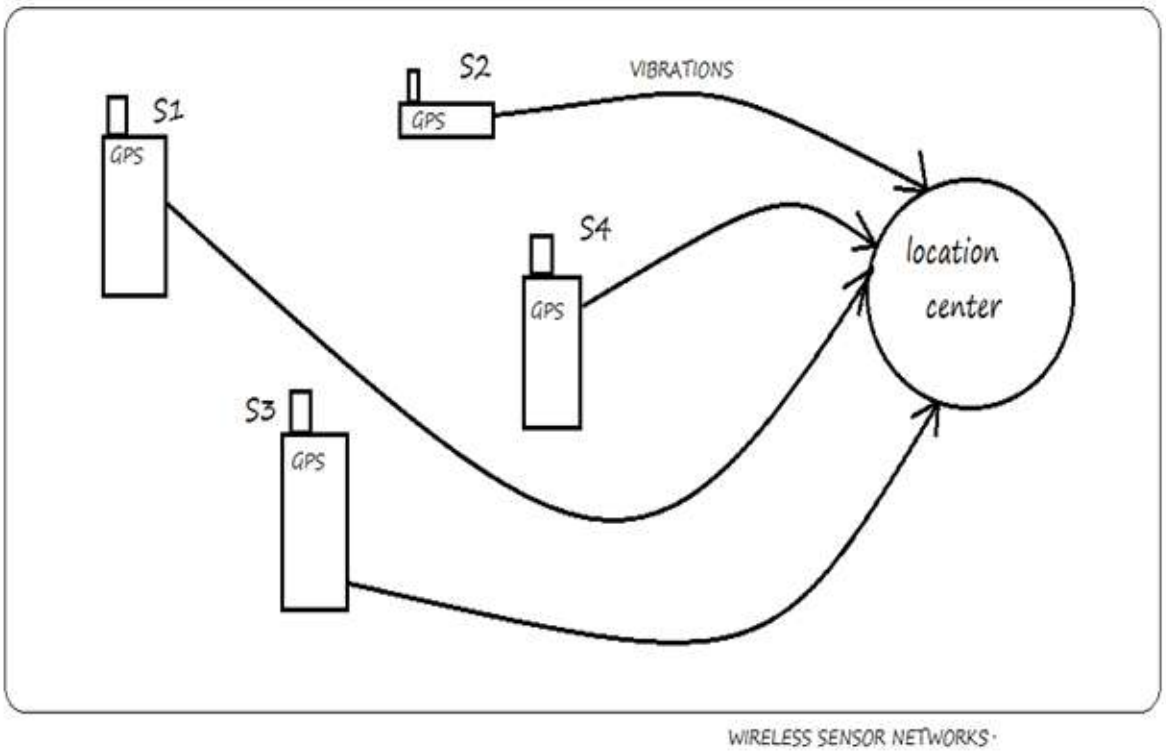

Fig 1. General operation of the sensor network

i). Module—1

Android app

Accelerometers are used as hardware sensors. They are the simple MEMS (Micro Electro Mechanical System) devices which are used to measure position, motion, tilt, shock, vibration, and acceleration (the rate of change of velocity – m/s2). They are available with one, two, or three axes. A 3-axis accelerometer senses the orientation of the phone and changes the screen, images, web browser, music player accordingly, allowing the user to easily switch between portrait and landscape mode. In this module data read from the accelerometer is encrypted using Symmetric algorithm using IMEI number and at the verification centre decrypt using IMEI number.

ii) Module-2

Symmetric key encryption is a cryptography technique that uses a shared secret key to encrypt and decrypt data. Symmetric encryption algorithms are very efficient at processing large amounts of information and

computationally less intensive than asymmetric encryption algorithms. Having agreed upon and exchanged a shared secret key, the sender and the recipient are able to exchange encrypted data.

The steps are as follows:

- Create a Symmetric Algorithm derived object and specify the Key (IMEI).
- Create Stream objects that will interface with the Symmetric Algorithm object.
- Create an ICryptoTransform object by calling the SymmetricAlgorithm.CreateEncryptor method (when encrypting) or SymmetricAlgorithm.CreateDecryptor method (when decrypting).
- Create a CryptoStream object using the Stream object and the ICryptoTransform object as defined.
- Read from or write to the Crypto Stream object depending on the context of the operation.

iii) Module-3

At the verification centre it is necessary to register all the remote devices from where we are excepting sensitive data. This module is used while receiving data , we need to decrypt using all the IMEI stored at VC with the data received as symmetric key , whichever IMEI matches , we will treat as Valid sensor nodes to receive data. In this module, we have sub modules like Device registration (XML serialization) Google map association with device input Update or Delete or Modify Device parameters.

VI. METHODOLOGY

6.1 Localization Techniques

Self-localization capability is a highly desirable characteristic of wireless sensor networks. In environmental monitoring applications such as bush fire surveillance, water quality monitoring and precision agriculture, the measurement data are meaningless without knowing the location from where the data are obtained. Sensor network localization algorithms estimate the locations of sensors with initially unknown location information by using knowledge of the absolute positions of a few sensors and inter-sensor measurements such as distance and bearing measurements. Sensors with known location information are called anchors and their locations can be obtained by using a global positioning system (GPS), or by installing anchors at points with known coordinates. Because of constraints on the cost and size of sensors, energy consumption, implementation environment (e.g., GPS is not accessible in some environments) and the deployment of sensors (e.g., sensor nodes may be randomly scattered in the region), most sensors do not know their locations. These sensors with unknown location information are called non-anchor nodes and their coordinates will be estimated by the sensor network localization algorithm [26].

6.1.1 Measurement Techniques

Measurement techniques in WSN localization can be broadly classified into three categories: AOA measurements, distance related measurements and RSS profiling techniques [26].

6.1.1.1 AOA measurements

The angle-of-arrival measurement techniques can be further divided into two subclasses: those making use of the receiver antenna's amplitude response and those making use of the receiver antenna's phase response. Beam

forming is the name given to the use of anisotropy in the reception pattern of an antenna, and it is the basis of one category of AOA measurement techniques. The measurement unit can be of small size in comparison with the wavelength of the signals. The beam pattern of a typical anisotropic antenna is shown in Fig. 2. One can imagine that the beam of the receiver antenna is rotated electronically or mechanically, and the direction corresponding to the maximum signal strength is taken as the direction of the transmitter. Relevant parameters are the sensitivity of the receiver and the beam width [26].

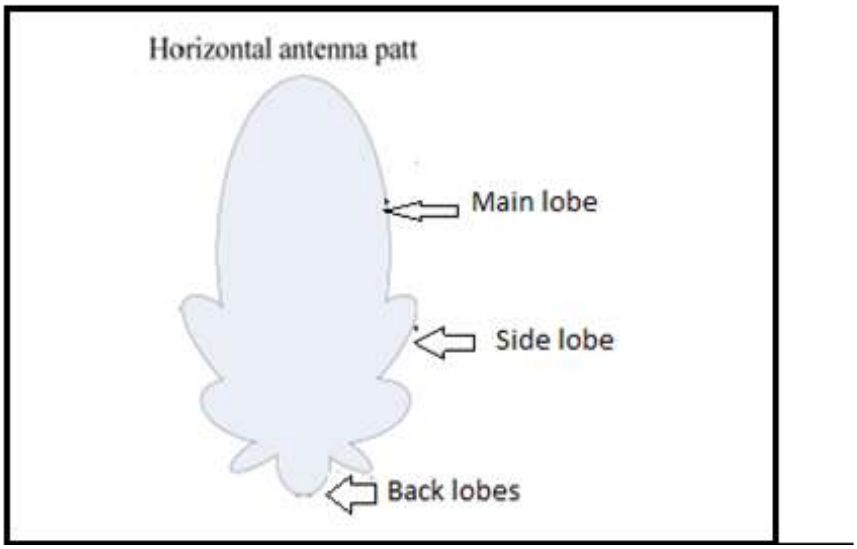

Fig 2. An illustration of the horizontal antenna pattern of a typical anisotropic antenna

6.1.1.2 Distance Related measurements

Distance related measurements include propagation time based measurements, i.e., one-way propagation time measurements, roundtrip propagation time measurements and time difference-of-arrival (TDOA) measurements, and RSS measurements [26]

1). One-way propagation time measurements: It measures the difference between the sending time of a signal at the transmitter and the receiving time of the signal at the receiver. It requires the local time at the transmitter and the local time at the receiver to be accurately synchronized. This requirement may add to the cost of sensors by demanding a highly accurate clock and/or increase the complexity of the sensor network by demanding a sophisticated synchronization mechanism. This disadvantage makes one-way propagation time measurements a less attractive option than measuring roundtrip time in WSNs [26].

2). Roundtrip propagation time measurements: It measures the difference between the time when a signal is sent by a sensor and the time when the signal returned by a second sensor is received at the original sensor. Since the same clock is used to compute the roundtrip propagation time, there is no synchronization problem. The major error source in roundtrip propagation time measurements is the delay required for handling the signal in the second sensor [26].

- There is a category of localization algorithms utilizing TDOA [26] measurements of the transmitter's signal at a number of receivers with known location information to estimate the location of the transmitter. Fig. 3 shows a TDOA localization scenario with a group of four receivers at locations r1*;* r2*;* r3*;* r4 and a transmitter at r*t*. The TDOA between a pair of receivers *i* and *j* is given by:

FORMULA:

$$\triangle t_{ij} \triangleq t_i - t_j = \frac{1}{c}\left(||\mathbf{r}_i - \mathbf{r}_t|| - ||\mathbf{r}_j - \mathbf{r}_t||\right), \quad i \neq j \tag{1}$$

Where ti and tj are the time when a signal is received at receivers i and j respectively, c is the propagation speed of the signal, and jj ¢ jj denotes the Euclidean norm [26].

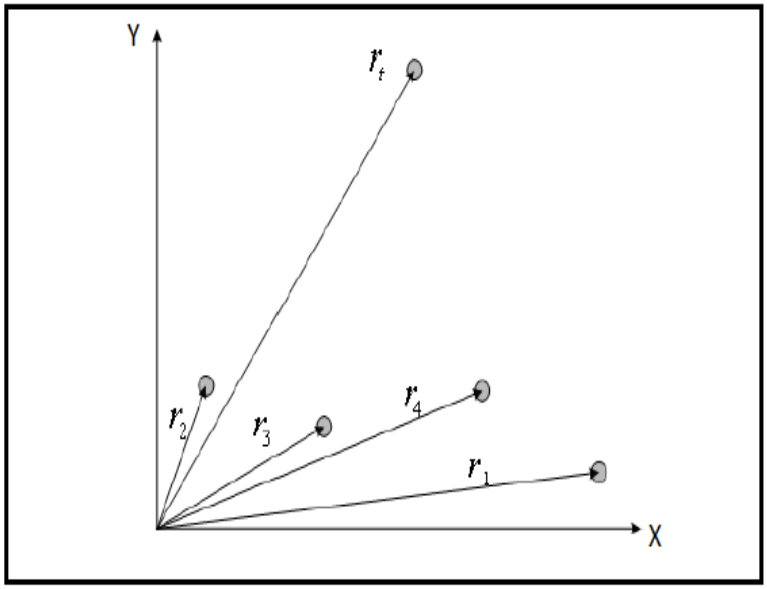

Fig 3- localization using time difference of arrival measurements [26].

- Yet another category of localization techniques, i.e., the RSS profiling-based localization techniques, work by constructing a form of map of the signal strength behaviour in the coverage area. The map is obtained either offline by a priori measurements or online using sniffing devices deployed at known locations. They have been mainly used for location estimation in WLANs, but they would appear to be attractive also for wireless sensor networks. In this technique, in addition to there being anchor nodes (e.g., access points in WLANs) and non-anchor nodes, a large number of sample points (e.g., sniffing devices) are distributed throughout the coverage area of the sensor network. At each sample point, a vector of signal strengths is obtained, with the jth entry corresponding to the jth anchor's transmitted signal. Of course, many entries of the signal strength vector may be zero or very small, corresponding to anchor nodes at larger distances (relative to the transmission range or sensing radius) from the sample point. The collection of all these vectors provides (by extrapolation in the vicinity of the sample points) a map of the whole region[26].

6.1.2 Probabilistic Approach

The probabilistic position estimation algorithm is used that considers the range measurement inaccuracies. Nodes in a sensor network can belong to two different classes, namely beacons and unknowns. It is assumed that the beacons have known positions (either by being placed at known positions or by using GPS), while the unknown nodes estimate their position with the help of beacons. The first step in RF-based localization is range

measurement, i.e., estimating the distance between two nodes, given the signal strength received by one node from the other. The unknown node initializes its position estimate to the entire space. The node then waits to receive beacon packets from its neighbouring nodes, and upon receiving a beacon packet, updates its position estimate by computing the constraint and intersects it with the current estimate to obtain the new estimate. If the position estimate improves, it will wait for a specific period of time and will broadcast its new estimate to all of its neighbours . If the unknown node estimates mean and standard deviation from the signal strength of the beacon message, the constraint is a Gaussian normal distributed surface of mean and standard deviation. This is equivalent to a Gaussian function rotated 360 degrees around the coordinates of the beacon [27]. If S1 and S2 are the two consecutive measurements, then the new shifted measurement is computed as:

S1= (μ_1,σ_1) S2= (μ_2,σ_2)

$$\mu_{shift} = \frac{\mu_1\sigma_2^2 + \mu_2\sigma_1^2}{\sigma_1^2 + \sigma_2^2}$$

$$\sigma_{shift} = \frac{\sigma_1\sigma_2}{\sqrt{\sigma_1^2 + \sigma_1^2}}$$

(2) , (3)

The Current Estimate is given by the formula:

$$P(x,y) = \frac{P(x,y) \times C(x,y)}{\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} P(x,y) \times C(x,y)dxdy} \quad (4)$$

6.2 Localization in Open Space

6.2.1 Visual Localization

To expand the working range of this localization system, it is sufficient to provide occasional on-demand Updates only when the open-space configuration fails. Visual pose estimation algorithms are well poised to do that. By acting less frequently and on demand, they can be allowed more time for image processing operations which can be used to increase the robustness of the overall system [23].

6.2.2. Localization Using All Sensors

Finally, a test will be performed to confirm that the entire localization system works well together, that is, it uses the visual localization as needed and that it actually improves the performance [24].

6.2.3 Mobile beacon based localization

The proposed localization approach starts from the stage of sensor node deployment. After the sensor deployment planning process, the user that carries the mobile beacon starts to deploy sensor nodes. When a sensor node is placed, the user turns its power on, and sets the mobile beacon to transmit a set of beacon signals. Any previously deployed nodes that are within the transmission range of the mobile beacon will receive the beacon signals and estimate their distances to the current mobile beacon location (or the location of the sensor

node under deployment). The user then moves to deploy the rest of the sensor nodes and repeats the same procedures until all sensor nodes are deployed. After all sensor nodes are deployed, each sensor node will have a set of distance measurements to its neighbours, which are then passed to a central node for localization using the MAP localization algorithm [28].

6.3 Programming Approaches for WSNs: A Classification

In the following subsections the characteristics of each group are detailed and several proposals are identified.

6.3.1. Programming Languages

The first option to develop an application for WSNs is to directly use an existing programming language. They are also used to implement the runtime support and infrastructures needed in most of the approaches discussed in the following sections [23].

6.3.1.1. Programming Abstractions

By programming abstractions we mean high-level abstractions that, supported by a suitable programming model, compiler and runtime support, liberate the programmer from having to address the low-level WSN mechanisms such as messaging and routing protocols, data caches and neighbour lists. Basically, we can establish two main types of programming abstractions: Node-centric or local behaviour approaches, which are centred on individual nodes, and macro programming or global behaviour approaches, which focus on the behaviour of a WSN as a whole. In node-centric programming, the programmer has to translate the global application behaviour in terms of local actions on each node, and individually program the sensor nodes using the corresponding programming model. Proposals such as Hood, Abstract Regions, Logical Neighbourhoods and Virtual Nodes belong to this class. In a WSN, a node is able to exchange data directly only with the surrounding nodes located within its communication radius (physical neighbourhood)[23].

6.3.1.2. Middleware

The middleware is used to support the development, maintenance, deployment and execution of applications, filling in the gap between the application layer and the hardware, operating system and network stack layers. In the case of a WSN, this includes mechanisms for formulating complex high-level sensing tasks, communicating them to the WSN, coordination of sensor nodes to split tasks and distribute them to the individual nodes, data fusion for merging the sensor readings into high-level result, and reporting it. Moreover, appropriate abstractions and mechanisms for dealing with the heterogeneity of sensor nodes should be provided [23].

Virtual Machines

Virtual machines provide a run-time environment that isolates the execution of applications from the underlying platform. The execution engine proposes a set of high level instruction set, enabling a compact representation of the application code. Therefore, size of applications is reduced in this way and software updates can be distributed more easily. However, since execution takes place within a virtual machine, execution cost is higher compared to native code.

This category allows the developers to write applications in separate, small modules. The system injects and distributes the modules through the network using tailored algorithms, and therefore overall energy consumption and resource use are minimized [23].

VII CONCLUSION AND FUTURE ENHANCEMENT

The Security is one of the major concern in the area of Wireless Sensor Networks . This paper presents a method of providing authentication to the sensor nodes thereby enhancing the trustability of the network. We discussed two familiar verification algorithms that brings out easy method of data authentication. These methods would be simple, effective and resistant to various attacks. But, there is still a requirement for Light Weight Algorithms. The advantage of designing a Lightweight systems is that they do not require any dedicated hardware or infrastructures, and they do not incur high computation overhead at the sensor side, so that the verification system can be applied to low cost wireless sensor networks. Finally, we can conclude that this paper presents a simple way to protect the data of sensor nodes.

FUTURE ENHANCEMENT

- A webpage application can be created through which the authentication of data from various sensors can be displayed.
- This application can be uploaded to the cloud to allow the users from various locations to access it.

REFERENCES

[1] JinfangJiang ,Guangjie Han, Chuan Zhu , Yuhui Dong , Na Zhang, "Secure Localization in Wireless Sensor Networks: A Survey(Invited paper)", JOURNAL OF COMMUNICATIONS, VOL. 6, NO. 6, SEPTEMBER 2011 465.

[2] WaleedAmmar, Ahmed ElDawy, and Moustafa Youssef, " Secure Localization in Wireless Sensor Networks: A Survey", Computer and Systems Engineering Department Alexandria University , Egypt ,July 7, 2009.

[3] Amitangshu Pal, "Localization Algorithms in Wireless Sensor Networks: Current Approaches and Future Challenges" ,Macrothink Institute , Network Protocols andAlgorithmsISSN 1943-3581 2010, Vol. 2, No. 1.

[4] YingpeiZeng,Jiannong Cao, Jue Hong, Li Xie, "Secure Localization and LocationVerification in Wireless Sensor Networks", State Key Laboratory for Novel Software Technology Nanjing University, Nanjing, P.R. China and Department of Computing Hong Kong Polytechnic University, Hong Kong.

[5] M.Loganathan, V.Navaneethakrishnan , " Detecting and Localizing Wireless Spoofing Attacks", International Journal of Advanced Research in Computer Science and Software Engineering,ISSN: 2277 128X,Volume 4, Issue 2, February 2014.

[6] K.SureshBabu, 2Swetha Gurram, "Survey of Detection and Localization of Multiple Spoofing Attacks in Wireless Networks", IJCSMC, Vol. 3, Issue. 7, July 2014, pg.13 – 17.

[7] LOUKAS LAZOS and RADHA POOVENDRAN, "SeRLoc: Robust Localization for Wireless Sensor Networks", ACM Transactions on Sensor Networks, Vol. 1, No. 1, August 2005, Pages 73–100..

[8] MostafaUddin, Tamer Nadeem, "SpyLoc: A Light Weight Localization System for Smartphones", 978-1-4799-4657-0/14/$31.00 c 2014 IEEE .

[9] Parthiban. M , "Secure Location Verification using Localization Algorithms ", International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014) © 2014, IJARCST , Vol. 2, Issue 2, Ver. 1 (April - June 2014) .

[10] R.M.Sinthiya, 2J.Vijipriya, "An Optimized Localization Algorithm against Node Replication Attacks in Wireless Sensor Networks ",International Journal Of Engineering And Computer Science ISSN:2319-7242Volume 3 Issue 2 February, 2014 Page No.3817-3821 .

[11] Yuan Zhang, ShutangLiu ,Xiuyang Zhao , ZhongtianJia, "Theoretic analysis of unique localization for wireless sensor networks ",www.elsevier.com/locate/adhoc. Ad Hoc Networks 10 (2012) 623–634.

[12] H. Muthukrishnan1 and S. Anandamurugan2, "Light Weight Security Attack in Mobile Ad Hoc Network (MANET) ",International Journal of Computer Sciences and Engineering Open Access ,volume-2, issue-8 .

[13] Ahmed Abdulqader Hussein AL-Qaysi1,2 and Tharek A. Rahman1, "A Survey on Secure Range Based Localization Algorithms in Wireless Sensor Networks ",Research Journal of Recent Sciences Vol. 3(11), 103-109, November (2014).

[14] M.M.Chithra1, A.Gayathri2, S. SelvaBirunda , " Securing and Region Based Algorithms For Wireless Sensor Networks", International Journal of Innovative Research in Computer and Communication Engineering(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014 .

[15] Xiaofeng Han, Xiang Cao, Errol L. Lloyd, and Chien-Chung Shen, Member, IEEE ," Fault-Tolerant Relay Node Placement in Heterogeneous Wireless Sensor Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 5, MAY 2010.

[16] SrdjanCapkun, Kasper Bonne Rasmussen,MarioCagalj, and Mani Srivastava, "Secure Location Verification with Hidden and Mobile Base Stations ",IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 7, NO. 4, APRIL 2008.

[17] YawenWei , Yong Guan , "Lightweight Location Verification Algorithms for Wireless Sensor Networks", IEEE Computer Society VOL. 24, NO. 5, MAY 2013.

[18] ShantalaPatil , Dr Vijaya Kumar B P, SonaliSingha, RashiqueJamil, "A Survey on Authentication Techniques for Wireless Sensor Networks", International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 7 No.11 (2012).

[19] Rickard Söderlund," Energy Efficient Authentication in Wireless Sensor Networks",LinköpingsuniversitetDepartment of Computer and Information Science.

[20] Abdullah Al-Mahmud, RumanaAkhtar," Secure Sensor Node Authentication in Wireless Sensor Networks," International Journal of Computer Applications (0975 – 8887) Volume 46– No.4, May 2012.

[21]TassosDimitriou, Ahmad Sabouri," Pollination: A Data Authentication Scheme for Unattended Wireless Sensor Networks".

[22] Prof N.R.Wankhade, JadhavAshvini B.," A Survey Paper on Hop by Hop MessageAuthentication in Wireless Sensor Network", N.R.Wankhade et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 8321-8324.

[23] Bartolom´e Rubio, Manuel D´ıaz and Jos´e M. Troya," Programming Approaches and Challenges forWireless Sensor Networks", Second International Conference on Systems and Networks Communications (ICSNC 2007) 0-7695-2938-0/07 $25.00 © 2007.

[24] AtanasGeorgiev,Peter K. Allen, "Localization Methods for a Mobile Robot in Urban Environments".

[25] DikLun Lee and Qiuxia Chen," A Model-Based WiFi Localization Method".

[26] Guoqiang Mao, Barıs¸ Fidan and Brian D.O. Anderson,"Wireless Sensor Network Localization Techniques".

[27] VaidyanathanRamadurai, Mihail L. Sichitiu,"Localization in Wireless Sensor Networks: A Probabilistic Approach".

[28] Yifeng Zhou and Louise Lamont,"A Mobile Beacon Based Localization Approach for Wireless Sensor Network Applications",SENSORCOMM 2011 : The Fifth International Conference on Sensor Technologies and Applications.

[29] Guangjie Han,Jinfang Jiang, Lei Shu, Yongjun Xu, and Feng Wang, "Localization Algorithms of Underwater Wireless Sensor Networks: A Survey",Published online 2012 Feb 13. doi: 10.3390/s120202026.

Biographical Notes

Rekha.K.S. holds Master's degree (2007) in Software Engineering, from Visvesvaraya Technological University, Belgaum. Currently she is working as an Assistant Professor in the Department of CS&E, The National Institute of Engineering, Mysore. She is pursuing her Ph.D. Her research interests include Wireless Sensor Networks, Middleware design, Software Engineering ,Software Architecture, Embedded Systems and Distributed Systems.

Nischitha.M.V. is currently pursuing B.E final year in Computer Science and Engineering, NIE,Mysore, India.

Megha.B.S. is currently pursuing B.E final year in Computer Science and Engineering, NIE,Mysore, India.

Dr.T.H.Sreenivas holds a Master's Degree(1986) from IIT,Khanpur and Ph.D (1999) from IIT,Madras. Currently he is working as a Professor in the Department of Information Science & Engineering, The National Institute of Engineering, India. His research interest includes Operating systems, kernel development and programming, real-time kernels, Real-time operating systems and Wireless Sensor Networks.