**INTRODUCTION**

Wireless Sensor Network (WSNs) have become the epitome of Pervasive Technology. They have an endless array of potential application in both Military and Civilian applications. The common factor being the Vitality of Sensor location. The Core function being to detect and report event which can be assimilated and responded only if the accurate location of the event is known. The advantages of knowing the location information of sensor nodes are as below.

First, Location information is needed to identify the location of an event of interest. For instance, the location of an enemy tank in a battlefield is important for deploying rescue and relief troops.

Second, facilitates numerous Application services, for instance providing doctors with information on nearby medical equipment and personnel in smart hospital.

Third, System functionalities such as geographical routing, Network coverage Checking and location – based information querying. With these advantages and more, the location – aware Sensor devices become standard in WSNs for all application domains that provide location – based service.

A straight forward solution is to equip the sensor with a GPS receiver. However, this is not a feasible solution from an economic perspective. Hence, localization in sensor network is very challenging. Over the years, many protocols were devised for location discovery proves in WSNs. The focal point being set of specialty nodes known as *Beacon Nodes*. These nodes know their location through a GPS receiver or through manual configuration which are provided to other sensor nodes.

It is critical that the malicious beacon nodes are prevented from providing false location information since Sensor nodes completely rely on the details for computing the location. The metrics associated with localization are Energy Efficiency, Accuracy and Security. The first two Metrix have been researched extensively. However, the Security Metric has not been addressed adequately.

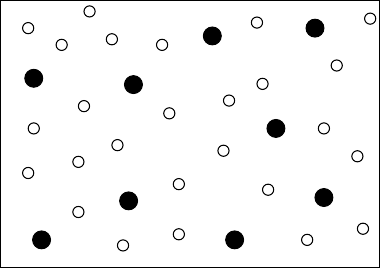
**OPERATIONAL CHALLENGES IN WSNs**

WSNs are often deployed to operate in Unattended and Hostile environments, rarely encountered by a computing devices. They have to operate autonomously and consequently and are faced with unique challenges. An advisory can capture and compromise one or more sensors physically. The advisory can tamper with the sensor node by injecting malicious code, forcing a malfunction. The advisory can launch attacks from within the system as an insider and most existing system would fail for the inside attacks.

For instance, consider a beacon – based localization model. Sensor nodes are not capable of determining their own location. There could be a malicious node giving false location information to sensor nodes compelling them to compute incorrect location. The situation in which one entry has more information than the other is referred to as *Information Asymmetry.* Theinformation asymmetry in beacon – based localization modes presents an effective way or resolving insider attacks.

**OVERVIEW OF LOCALIZATION PROCESS**

Localization is a mechanism for discovering spatial relationship between objects. The various approach taken in literature to solve this localization problem.



**Figure 1**: *A network with sensor and beacon nodes. Sensor nodes are represented by hollow circles and beacon nodes are represented by shaded circles.* *The idea of beacon-based localization is presented.*

The list of assumptions made include assumptions about device hardware, signal propagation models, timing and energy requirements and composition of network, operational environment, beacon density, time synchronization, communication costs, error requirements and node mobility.

Different scenarios in node mobility is as mentioned. First, both the sensor and beacon nodes are static. Second, Sensor node are static while beacon nodes move. Third, sensor nodes move while beacon nodes are static. Fourth, both sensor and beacon nodes move.

The localization process is straight forward in models that use GPS as the source. However; in models that use beacon nodes to help sensor nodes for location discovery, the nodes are either manually configured or equipped with a GPS receiver to determine their location. Beacon Nodes provide the location information to Sensor nodes for computing the location.

**Figure 2**: (a) *Triangulation* (b) *Trilateration* (c) *Multilateration*

The localization process can be classified into two stages. Frist Stage, the node estimates its distance to other nodes in its vicinity using the features of the received signals. Second Stage, The node uses the distance estimates to compute the actual location. To compute the actual location depends on the features used in stage one, they can be classified into three mail groups as follows.

***Triangulation***: This is a method of gathering Angle of Arrival (AoA) measurements at a sensor node form at least the source.

***Trilateration***: This is a method of determining the relative positions of objects using the triangles similar to Triangulation. Trilateration involved gathering a number of reference tuples of the form (a,b,d) where d represents the distance between the source providing the reference location from (a,b) and the sensor node.

***Multilateration***: This is a process of localization by solving for mathematical intersection of multiple hyperbolas based on the Time Difference of Arrival (TDoA). In Multilateration, the TDoA of a signal emitted from the object to three or more receivers is computed accurately with tightly synchronized clocks.

Secure localization in sensor networks has become a major focus of research. Localization also has security requirements listed below.

1. ***Authentication***: Information for localization must be provided by accredited sources.
2. ***Integrity***: The information provided by the source should be untampered before the sensor node can use it to find the location.
3. ***Availability***: All the details required for computing the location must be available with the sensor node when required
4. ***Non – Repudiation***: Neither the source nor the Sensor node that provides the location information should be able to deny the information exchange at a later time.
5. ***Privacy****:* The source should onlyprovide its location to the sensor node. Neither the source not the Sensor Node’s location should be disclosed at any point.

Error in estimated location of a sensor can be classified into two groups. *Intrinsic Errors*: These errors are most often caused by abnormalities in the hardware and software of the node. *Extrinsic Errors*: This is attributed with the physical effects on the measurement channel like shadowing effects, change in signal propagation speed and Obstacles.

**CLASSIFICATION OF LOCALIZATION TECHNIQUES**

Classification Techniques and their merits and demerits is as mentioned below.

* ***Direct Approach****:* This is also called as ***Absolute Localization***. This can be further classified into ***Manual Configuration****:* Thismethod is expensive and neither particle nor scalable for large scale WSNs. *GPS – Based Localization*: This method adapts well for WSNs with node mobility. However, it is not economically feasible to equip each sensor with a GPS receiver. Also, such WSNs cannot be used for underwater monitoring applications.
* ***Indirect Approach****:* This approach is also known as ***Relative Localization*** since the node positions themselves relative to other nodes in the vicinity. This approach was introduces to overcome the drawbacks of the GPS – based direct localization. In this approach, a small subset of beacon nodes in the network are equipped with GPS receiver. They compute the location and send signals providing the location to all the sensor nodes in their surrounding area. This allows sensor nodes to compute their location. However, the beacon nodes are also operating in the same aggressive environment as the sensor nodes, they are vulnerable to various threats.

The indirect approach in the localization process can be classified into the below categories.

* ***Range – Based****:* The location of a node is computed relative to other nodes in the surrounding. This depends on the assumption that the absolute distance between a sender and a receiver can be estimated by one or more features of the communication signal from the sender to the receiver. However, the accuracy is subjected to the transmission medium and the surrounding vicinity. The features of the communication signal that are frequently used in literature for range-based localization are as follows:

1. ***Angle of Arrival (AoA):*** *Range* information is obtained by estimating and mapping relative angles between neighbors.
2. ***Received Signal Strength Indicator (RSSI):*** Use atheoretical or empirical model to translate signal strength into distance.
3. ***Time of Arrival (ToA):*** The signal propagation from source to destination is measured.
4. ***Time difference of Arrival (TDoA):*** An Ultrasound is used to estimate the distance between the node and the source.

* ***Range – Free:*** This localization never tried to estimate the absolute point – to – point distance based on the received signal strength. This greatly simplifies the design of hardware making the method cost – effective alternative for localization in WSNs.

**Attacker Model**

The attacker can be either an insider or an outsider. An insider attack is potentially dangerous as they have access to all the cryptographic keying material held by a node. Outsider attack model, the attacker will not have the cryptographic keys for authentication. They can only capture a node but cannot retrieve the sensitive information and this method is comparatively less harmful. The most common attacks against localization schemes are as given below.

* ***Replay Attack***: In this attack, the attacker’s capability is limited to one node. The attacker merely jams the transmission between the sender and receiver and replays the same message posing as the sender. A simply way to launch a replay attack is as shown in the below figure.

Figure 3: (a) Replay attack example. Node A replays to C the message it receives from B. (b) Wormhole attack example. Nodes C and tt have a wormhole link.

Malicious node A retransmits to node C the message it received from node B. A Replay attack has a two – fold consequence. When replay attacks are launched, a localizing node will receive an incorrect reference there by localizing incorrectly.

* ***Sybil Attack***: In this attack, a node claims multiple identities in the network. When launched, the nodes can receive multiple references from a singly node leading to incorrect location estimation.
* ***Wormhole Attack***: To launch the attack, the attacker needs to compromise at least two nodes. The concluding nodes in the network tunnel messages transmitted in one part of the network to their concluding partners in other of the network.

**Existing Secure Localization System**

We will review the existing secure localization techniques, throwing light on their strengths and weakness.

**SeRLoc**

SeRLoc is a range – free, distributed, resource – efficient localization technique in which there is no communication requirement between nodes for location discovery. They are tough against various attacks like wormhole attacks, Sybil attacks and sensor compromise. SeRLoc is equipped with directional and omnidirectional antennas and the sensors determine the location based on the information transmitted.

An attacker has to imitate several beacon nodes to compromise the localization process. Sector uniqueness property and communication range violation property help thwart Wormhole attacks in SeRLoc.

**Beacon Suite**

The Beacon Suite include detection of malicious beacon signals, identification of malicious beacon node, detection of replayed beacon signals, avoiding false detection and revoking malicious beacon nodes. The two main properties of beacon nodes are to provide location information to sender nodes and for detection on the beacon signal from other beacon nodes. The beacon node being detecting is called as *target node* and the node performing the detection is called as *detecting node*. The detecting node use a non-beacon ID while requesting location information from target to observe true behavior of the target node.

There are two counter maintained in each beacon node, Alert counter: to record suspiciousness of the corresponding beacon node. Report Counter: to record the number of alerts this node reported and accepted by the base station. The two counters works on a discrete scale and the revocation mechanism is centralized.