International Journal of Computer Networks and Communications Security

VOL. 4, NO. 5, MAY 2016, 130–140
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Different Aspects of Localization Problem for Wireless Sensor Networks: A Review

Mohammed Farrag[1], Mohammed Abo-Zahhad[2], M.M. Doss[3] and Joseph V. Fayez[4]

[1, 2, 3, 4] Department of Electrical and Electronics, Faculty of Engineering, Assiut University, Assiut, Egypt

E-mail: [1]mfarragm@gmail.com, [2]zahhad@yahoo.com, [3]magdy@aun.edu.eg, [4]j_fayez@hotmail.com

ABSTRACT

This paper describes the wireless sensor networks, which is widely used in the last few decades. The hardware architecture of sensor node as a construction unit for WSN is illustrated with sensor applications. The localization process and its challenges are mentioned. A comparison between algorithms and techniques for sensor localization is presented. The factors that affect design issues including different topologies, mobility matter of sensor nodes, security issues, and finally future work and new trends for wireless sensor network localization.

Keywords: *Wireless Sensor Networks, Localization, Mobility, Security.*

1 INTRODUCTION

Wireless Sensor Network (WSN) consists of sensor nodes which are densely deployed where every node has sensor, processor, transmitter and receiver units. These nodes are low cost, low power, and multifunctional devices to perform a different sensing task. Sensor nodes are deployed throughout the area to monitor specific events (e.g. temperature, fire) in the real-world environment. The WSNs mostly operate in open and unmanaged area. They are envisioned to play an important role in a wide variety of areas (e.g. military surveillance, forest fire monitoring, building security monitoring and industrial process control) [1].

Most applications require more accurate localization process for nodes, to get their coordinates inside the network [2]. This area of research open new horizons of algorithms and techniques to optimize better location estimation for sensor nodes in different areas (e.g. indoor, outdoor). As a matter of fact, target tracking and localization aspects have a very important ratio of all scientific WSN publications [3].

This paper discusses localization problems, algorithms, and applications. The paper is organized as follow: Section (II) presents applications of WSN in multiple fields. Section (III) defines the hardware architecture of sensor nodes and the role of each of them. Section (IV) gives an overview for localization problem. Section (V) lists the challenges and issues that face WSN localization. Section (VI) classifies the techniques of WSN localization and describes the methodology used for each of them including comparison between them. Section (VII) discusses the mobility of sensor nodes as a separate problem that faces network topology and causes localization variation. Section (VIII) presents network security issues that may lead to missed or wrong localization data by defining the idea of each attacking methods and proposed solution techniques. Finally, Section (IX) introduces future works and new trends for research purposes in the field of WSN localization.

2 APPLICATIONS OF WIRELESS SENSOR NETWORKS

The importance of using WSNs grows year after year and overlaps with multiple fields for the purposes of control, surveillance, measurements and many other operation tasks. The fields of application are variable between industrial, medical, scientific, commercial, and home-related. The most famous applications are [4][23][30]:

A. Military Applications:

It requires a well-equipped and solid wireless sensor that can bears the high temperature and probability of breaking down on the battlefield with unnoticeable shape for stealthy purposes from enemies. The tolerance and fault clearance are sensitive conditions for the sensitivity of military scope. The usability of wireless sensors in military field varies between vehicles monitoring (either friendly or opposed one), detection of different types of attacks and many other purposes with a densely deployment topologies to collect more trusted data.

B. Medical Applications:

Wireless sensors are highly preferable nowadays for the reduction of cables and physical links between patient and monitoring equipments. The sensitivity of recorded data requires higher processing capabilities for the sensor nodes. There are also more functions to be performed by the medical sensors like diseases control and drugs administration. Generally all functions require smaller sensor size beside data sensitivity with ability to register the data record of various vital signals of the patients for remote surveillance between doctors and patients.

C. Environmental Applications:

WSNs can be used to measure multiple environmental parameters and features like temperature, humidity, pressure, light intensity, and soil characteristics. It's also used to track and monitor the movement and behaviour of animals, birds and other creatures to make sense of their reactions to certain phenomena.

In most cases the sensor nodes are attached to a moving creature or deployed densely inside the target environment. Some applications need sensor's controllability to manage its movement or to reposition it for better connectivity or to measure in different area. The environmental applications requires a long life power supply with minimum data transmission protocols to help in surveillance and monitoring within a hard to manage and access fields.

D. Home-related Applications:

The beneficiaries list of the WSNs applications extends to the home users as technologies step to the smart home utilization. The management of home/office appliances involves remote controlling ability either inside the target area by direct connection between user and devices or externally by using Internet or Satellite. The interactivity between home appliances and the user requires artificial intelligence through sensor nodes that develop their reactions to adapt with user's needs.

3 WIRELESS SENSOR NODE HARDWARE ARCHITECTURE

Sensor nodes are the core of WSN beside management systems, and like other electrical devices it consists of two main domains: Software platform and hardware architecture where both fields should serve each other. Software platform consists mainly of the operating system that manages the sensor node. It is related to the procedures and algorithms of measurements techniques that will be loaded to each sensor node. On the other hand the hardware architecture should support the measurement procedures.

The main block diagram of the sensor node architecture is presented in Fig. 1. Each wireless node contains: Power supply, Sensor, Processing unit, and Transceiver portion [16][18]:

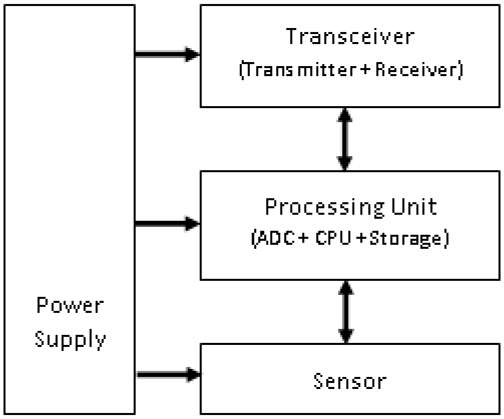


Fig. 1. Sensor node hardware architecture

A. Power Supply:

The sensor deployment in many applications depends mainly on spreading sensors in wide area for data acquisition that may leads to difficulty in changing the power source in schedule way for the short-run. Power supply is considered the main unit for the sensor node as it feeds the other units to perform its functions [19], and the life time of the sensor node is dependent on its power source. One side of the efforts given to maximize the power performance is to develop minimum data processing techniques and to minimize the data flow rate between nodes. On the other hand the physical development for power unit takes place by using different materials that balances the cost to performance to optimum (e.g. Nickel-cadmium, Lithium-ion…).

B. Sensor:

The WSNs are defined by the function that is measured by the sensor part inside its nodes (e.g. temperature, smoke, humidity...). Sensor part inside the nodes translates the physical event that is required for measuring to a meaningful data to be processed and stored [20]. Sensors are divided by the type of the output waveform to: Analog and Digital. Sensor units are supposed to have minimum size and minimum power consumption.

C. Processing Unit:

Processing entity is responsible for handling data received or transmitted by transceiver and also responsible for managing data retrieved by sensor part. This entity contains three main components: Analog to digital converter (ADC), Central processing unit (CPU) and Memory storage [19].

ADC is considered as a part of sensor unit in some papers, but actually it performs a pre-processing task of converting the signal to digital form analog.

CPU is responsible for controlling functionality inside the sensor node with multiple forms of hardware and software: FPGA, ASICS and multiple other forms, and could be replaced in some nodes with Microcontrollers which is lower in power consumption.

Memory storage is the input/output part that controls the flow of data to be stored or processed. The storage part could be: Volatile memory like Random Access Memory (RAM) which stores data to be sent and not keeping it when restart the node, and Permanent memory like Read Only Memory (ROM) which saves the operating system and main algorithm of operation.

D. Transceiver:

It manages a dual transmission function of sending and receiving signals between nodes, node and beacon, or node and management base. This portion uses mainly the Industrial-Scientific-Medical (ISM) band of frequency which is free for user-defined applications and reusable globally. Transmission technology varies from environment to another and between applications and could be in multiple forms like: Optical (Light, infra-red, LASER), Radio Frequency (RF) and many other formats [21]. In all cases the transmission process is not a continuos one but varies between handshaking, sleep mode and transmission time. Whatever the technology used and the modes of operation through transceivers, it should be optimized for lower power consumption either by hardware enhancement or transmission time reduction.

4 OVERVIEW OF LOCALIZATION

Localization means how sensor nodes determine their location inside the network. In another way, localization could be defined as the mechanism that discovers spatial relationships between sensor nodes [5]. Assume the case when we deploy a WSN that consists of N sensors at locations S = {S1, S2, ……. , SN}. Let Sxi, Syi, Szi denotes the x, y and z coordinates of the location of sensor (i), respectively. Limiting Szi to value (0) satisfy the 2D requirements. Some sensors' positions are well-defined for themselves; these nodes are known as (Anchors or Beacons), as shown in Fig. 2. All the other nodes localize their positions with the help of location references received from the anchors. So, to formulate the localization problem it could be defined mathematically as follow: given a multi-hop network, represented by a graph G = (V, E), and a set of beacon nodes B, their positions {xb, yb} for all b ∈ B, we aim to find the position {xu, yu} for all other unknown nodes u ∈ U [5].

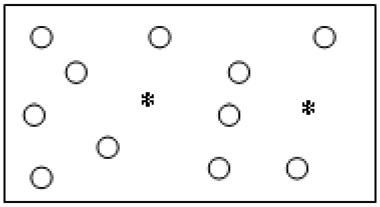


Fig. 2. A Wireless Sensor Network contains sensor and beacon/anchor nodes. Sensor nodes are represented by circles and beacon/anchor nodes are represented by "" symbol.*

5 LOCALIZATION CHALLENGES

The random deployment is the aspect that defines most WSNs, avoiding any pre-configured network. The dynamic nature for network topology is a main characteristic that defines the WSNs, caused by node outage (e.g. energy). The configuration of self-allocation mechanisms then become important to verify a powerful transmission of the localization information. Self-allocation is useful in node distribution and topology self optimization. Self optimization is to consider the application's need before operation and modifying the protocol parameters. This trend is not simple in sensor networks for the unpredicted environment. For efficient design we must accept the use autonomous learning method through surveillance, so that network localization can adjust its own performance periodically. Current methods try to localize nodes before operation based on communication constraints or range estimation. Target tracking add more restrictions that can be used to further reduce the localization error with time. The technique that suits querying of targets or sending data to sinks that have an underlying (unknown) probabilistic location pattern [6]. Other issues in localization with mobility are:

a. Performance: The localization's accuracy, the delay time to estimate location, the capacity (No. of requests to be processed) and coverage.

b. Cost and complexity: In addition for the cost of infrastructure there'll be cost for deploying the sensors. The costs concerning the infrastructure need for more bandwidth just for the localization process. The reduction of infrastructure cost can be available by using umbrella localization system to cover larger area in multiple applications (e.g. Indoor environments [31], urban areas [32]).

c. Security: To keep the privacy of location information is an important matter to keep it away from being tracked. That's a very difficult matter when securing such signals. It might be easier to develop secure protocols to prevent interference from unknown sources. On mobile nodes' movement between controlled boundaries, the security of information becomes more important.

6 LOCALIZATION TECHNIQUES CLASSIFICATION

Localization algorithms can be categorized into multiple classes. Presented below some classification headings, as it's small list, it gives an impression that localization problem can't be solved absolutely rather than optimizing localization's parameters (Cost, Power, …) [7]:

1. Environment: indoor vs. outdoor
2. Positioning: relative vs. absolute
3. Topology: sparse vs. dense, uniform or random
4. Accuracy: fine-grained/coarse grained
5. Beacons: beacon-free vs. beacon-based
6. Input Data: range-free vs. range-based
7. Dynamic vs. Static: mobile vs. fixed
8. Cost: energy, price, memory, computation
9. Tracking: cooperative or passive target
10. Communication: centralized or distributed ranging

The last classification takes place in most recent researches. At follow we will discuss on ranging Communication techniques:

A. *Centralized Ranging Techniques:*

Centralized localization ranging techniques imply data transmission to a central node for location computation for each node. Taking into account that this type of data transmission to a central point is more expensive, as the power supply of every node is limited and sending series of data over time within the network results in latency, and it also consumes network bandwidth and energy [6].

B. *Decentralized Ranging Techniques:*

Decentralized localization ranging techniques means the ability of each node to determine its own location independently from relying on central node for computations, and that classification include classification number (6) of the above classifications which is input data (Range-based and range-free localization) and the both types will be discussed in the next section.

1) Range-based Localization Techniques: These techniques depends on locating the destination sensor node by either finding the point-to-point absolute distance or by angle measurements, which means that the accuracy to estimate such values is subjected to the nature of the transmission medium relying on the complexity of hardware to control the fine resolution outputs [5]. That category involves many techniques in the field of WSN like: Received Signal Strength (RSS), Time of Arrival (TOA), Time Difference of Arrival (TDOA), Angle of Arrival (AOA), and Global Positioning System (GPS) which based on TOA; where the first four techniques are the most usable and takes place in most WSN researches [6][9] and will be in the centre of focus in this discussion:

Received Signal Strength (RSS): Using models of wireless channel characterization, the RSS transforms the radiated signal strength to a meaningful distance (e.g. empirical model, theoretical model, etc.) [2][5]. One of the most known applications for this technique is RADAR [8]. The model of RSS measurement shown in Fig. 3

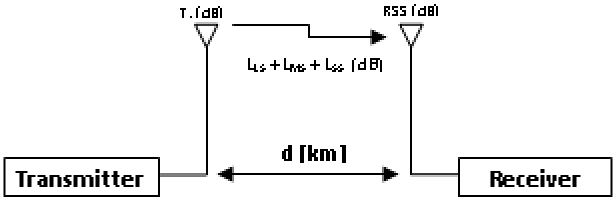


Fig. 3. RSS measurement model for Wireless Localization

The formula of RSS measurement model will be:

$$RSS = T_x - (L_{LS} + L_{MS} + L_{SS}), \quad (1)$$

where RSS is the Received Signal Strength, T_x is the transmitted signal strength and the three other parameters (L_{LS}, L_{MS} and L_{SS}) represent the signal loss through transmission channel due to large, medium and small scale propagation respectively. All measurements in (dB) [10].

Time of Arrival (TOA): Measuring time of signal propagation between nodes to determine the location data. That type of localization techniques require synchronization between nodes' clock, and that clock must be a referential one (usually synchronization process uses Satellites for precise results) [5] or using reference timing from well-known source velocity (e.g. RF). Global Positioning System (GPS) is the most widely used and known technique that depends mainly on TOA measurements, but unfortunately it's not providing efficient results inside indoor environments and costs much more hardware structure [11, 12]. Actually, TOA could be estimated by two main methods:

1. *One way propagation time estimation*: assembled of hardware components as shown in Fig. 4. [13] where radio signal sends first t_{radio}, and after t_{delay} (and might be cancelled) the sound waves are sent (through speakers and microphones in both nodes) t_{sound} where the receiver record the time. Destination *d* could be calculated from the relation:

$$d = \frac{v_{radio} v_{sound}}{v_{radio} - v_{sound}} \left(t_{sound} - t_{radio} - t_{delay}\right), \quad (2)$$

   where v_{radio} and v_{sound} are the signal velocity of RF signal and Acoustic/ultrasound signal respectively.

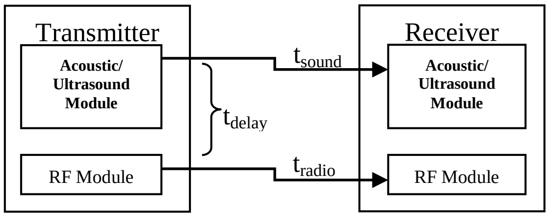


Fig. 4. TOA "One way propagation time estimation" hardware

2. *Round-trip propagation time estimation* (RTT): used to avoid synchronization between nodes using time-stamps which are applied in one-way propagation method. The transmitter send packet to receiver node, after receiving it the receiver wait for delay time and resend it so the trip time is $t_{RT} = 2t_{flight} + t_{delay}$ and from the t_{flight} and velocity of sent signal we can calculate the distance. The most affecting key in this method is clock drift that might change the results slightly.

Time Difference of Arrival (TDOA): Like TOA it returns the location and distance from the measurements of flight time of signals sent between sensor nodes by following steps:

1. Firstly, transmitter node sends signal s(t) that will be received at receiver nodes after delay time (τ) [14].
2. Secondly, cross correlation calculations applied at each node between two received signals (s_i) and (s_j) for period T which is long enough to get results [13]. The formula is:

$$\rho_{i,j}(\tau) = \frac{1}{T}\int_0^T s_i(t) s_j(t-\tau)dt, \quad (3)$$

TDOA returns accurate results under line-of-sight conditions to avoid path-loss problems. It is also affected by the nature of the transmission medium as it used sound and RF signals, which is greatly affected by temperature and humidity. So we might not use it if the application of the sensor node is measuring humidity or temperature [13]. The high cost of each node as TOA method still exist and could be considered a matter of research to lower it.

Angle of Arrival (AOA): Retrieving location information between nodes by comparing angles of received signals in terms of phase and time difference and using simple geometric relationship to calculate node position [2, 5, 6]. Multi antenna system (normally from 3-4 antennas) and radio frequency are used to achieve these measurements, sometimes optical transmission is used to perform the same task. AOA techniques are more accurate than RSS but unfortunately it costs higher, and that matter is one of research branches that requests higher precession and lower cost. The construction of AOA system depends on geometry calculations as mentioned before, so that it depends on triangulation and trigonometry as shown in Fig. 5.[13].

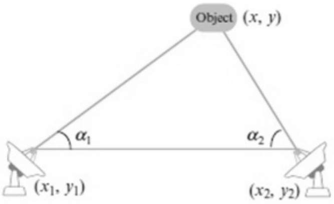


Fig. 5. AOA measurements

Some performance development techniques for AOA method are presented to solve replication issues of sensor nodes and minimization of the clone attack. The enhancement based on aligning the anchor nodes and sensor nodes in special geo-deployment, and the whole network's sensors could achieve the neighbours' angle of incident in conjunction with speed of transmission [34].

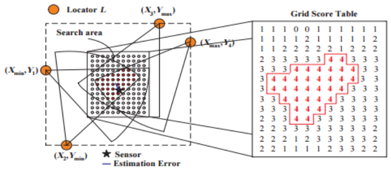
2) Range-free Localization Techniques: Unlike the rage-based techniques, the range-free techniques are not involved in estimating the absolute point-to-point location using the previous methods like (Received signal strength, time, angle, etc.). Accordingly, it leads to cost reduction by simplifying the hardware construction [5] but still preforms badly for irregular network topologies. Many techniques fall under that category like: DV-Hop, APIT, SeRLoc and ROCRSSI; where the first two techniques are the most famous of that category and will be explained under two classes:

DV-Hop (Hop Counting methods): Depends on message flow between nodes specially in the low density networks. Each node register the hop count to another nodes and this counter should be the minimum number of the hops to access the other node. Updates are made due to received messages. The known locations of the beacon/anchor nodes are used for location estimation as it works as bridges between the target nodes and the blind ones. Trilateration method is applied for nodes localization [7].

APIT (Local methods): Unlike the hop counting methods this type is working in high density networks. Radio signal propagates in spherical way that is measured by target nodes and its location is estimated by central measuring for all nodes that access it using triangulation method, so each node location is determined by triangle of beacon nodes and calculations are repeated with other triangle of beacons until reaching the desired accuracy [5]. No need for GPS equipped beacons/anchors and instead of that a high-powered nodes are used as reference points for the network in the main triangles [2].

Although this method is simple in hardware and cheaper than range-based equipments, but it requires high ratio of beacons to nodes and higher power beacons to give more location estimation ranges and hence it requires higher density networks [15].

SeRLoc (Secure Range-independent Localization): Introducing a solution to localization problem in two stages [35]. First stage is "Location Determination" where sensors hear each other then determining the area of search between ($X_{min.\&max.}$, $Y_{min.\&max.}$), followed by overlapping region-Majority vote that applies grid-scoring organization to determine this area in form of grid score table as shown in Fig. [6], the last step in this stage is estimating location [36] .



1	1	1	0	0	1	1	1	1	1	1
1	1	1	1	2	1	1	1	1	1	2
1	1	2	2	2	2	2	1	2	2	2
2	3	3	3	3	3	4	4	3	3	3
3	3	3	4	4	4	4	4	4	3	3
3	4	4	4	4	4	4	4	4	3	3
3	4	4	4	4	4	4	4	3	3	3
3	3	4	4	4	4	4	3	3	3	3
3	3	3	4	4	4	3	3	3	3	3
2	3	3	4	4	3	3	3	3	3	3
2	2	3	3	3	3	3	3	3	3	2
2	2	2	1	2	3	3	3	3	3	2
2	2	1	1	1	1	2	3	3	2	2

Fig. 6. Grid-score table for SeRLoc

The second stage is securing the location using (Encryption & Locator ID authentication) to avoid security threats like "Wormhole attack, sybil attack …etc" which will be discussed further in this paper.

ROCRSSI (Ring Overlapping based on Comparison of Received Signal Strength): Based on overlapping between RSSI (Received Signal Strength Indicator) from anchor nodes this technique diminish the rings of radiation to limited thickness, then increase counters that introduce more rings to the grid so the calculation of the highest values could be calculated [37, 38], finally the gravity center for a region defines the location of the sensor as shown in Fig. [7].

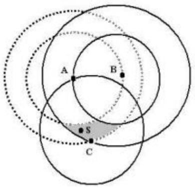


Fig. 7. Process of ROCRSSI

3) Range-combined Localization Techniques: These techniques are working in accompany with the previously described techniques in order to get the target node position after determining its range of communication [5, 6, 16]. The most known measurement ranging combined techniques are shown in Fig. 7. :

Triangulation: It gathers large number of localization techniques. Its idea based on collecting AOA signals at target node from three sources at least, then using the intersection of circles of the three AOA reference nodes in combine with geometric relationships and calculations to estimate the location of the target node.

Trilateration: Similar to triangulation it uses the relative positions of the target node to the source nodes with minimum three references source nodes, but unlike the triangulation it calculates the location by using trigonometry laws including sines and cosines. These calculations are made in 2D in terms of (x,y,d) where d is the distance between each reference node and target one.

Multilateration: Uses the TDOA information and the distances to three or more reference nodes, then by minimizing the error between the estimated location values and the real one it get the localization information. This procedure is repeated multiple times to different three or more references for minimization process.

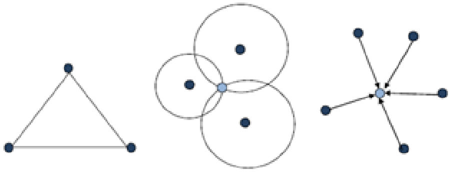

(a) (b) (c)

Fig. 8. Localization Combined techniques
a) Triangulation b) Trilateration c) Multi-Lateration

Table I. represents a comparison between the range-based and range-free techniques that explained previously [16, 17, 39]:

TABLE I
RANGE-BASED VERSUS RANGE-FREE TECHNIQUES

Technique	**Range-based**		
	Accuracy	**Cost**	**Energy Consumption**
RSS	Medium	Low	Low
TOA	Medium	High	High
TDOA	High	Low	Low
AOA	Low	High	Medium
	Range-free		
DV-HOP	Medium	Low	Low
APIT	Medium	Medium	Low
SeRLoc	High	Low	Medium
ROCRSSI	High	High	High

The comparison between the main categories (Centralized and decentralized techniques) leads to higher accuracy for the centralized techniques with higher energy consumption, on the contrary of that decentralized techniques are lower accuracy but lower energy consumption.

7 NODE MOBILITY

The mobility of sensor nodes proposes more difficulties and challenges for Localization estimation; on the other hand the relocating process as a mobility action may enhance the performance of the whole network connectivity or a certain part of it.

Mobility reasons varies between natural effects (by wind or other environmental causes) or controllable (Automatically programmable algorithms, or event driven by human management) [22]. In other words the movement is classified to passive movement that means that sensor nodes movement affected by external force, while active movement is done by the sensor itself as planned. The natural effects that causes mobility are extremely random and the network topologies of this kind changes multiple times, while the controllable mobility is reasonable with calculated algorithms or humanly adapted with certain event [23].

The forms of network due to mobility case could be divided to three schemes: moving nodes and fixed beacons/anchors, moving anchors and fixed nodes, and mobility of both kinds the nodes and anchors. All types of network mobility involve general and partial movement for anchors or nodes [2, 24].

Localization techniques in mobility conditions is a continuos process performed periodically. These techniques could be categorized to three main ideas [13]:

Using referential anchor nodes equipped with GPS processor; these referential nodes could track the mobility variations to remap the network topology. It faces the same troubles as all GPS-based techniques including expensive hardware, higher energy consumption and low performance in some environments especially indoor.

Re-computation of algorithms in periodic way is also another point of view to manage mobility topologies, but this method require huge number of computations to record the changes in the network topology and that leads to power consumption and higher processor performance.

The last trend is to use predefined information about the nature of sensors mobility. This method is more preferable than the other ideas for the matter of power optimization and compatibility with large-scale networks with minimum computations. It also contains multiple known techniques falls below this idea, the most three famous techniques for mobility in this case are [6]:

- *Monte Carlo Localization (MCL):* It's also defined as particle-filter method. That name denotes that the technique is using a particle filter to represent the distribution of similar cases after estimating the location and orientation of mobile node by a well-known predefined map [25].

- *Convex Approximation Localization (CAL):* The network is divided to smaller convex regions. Then these subregions define the angle at concavity spot which indicates the localization error. Measurements are done to define sharpness and depth of the concavity region to be refined from errors [26].
- *Moving-Baseline Localization (MBL):* That method mainly used when unavailability of reference coordinates for nodes to align themselves. Thus each node starts to build its own spatial map in collaboration with the moving group by exchanging signals in UWB (Ultra Wide Band) [27].

8 LOCALIZATION SECURITY

Security issues in the WSN are linked to the different layers of the communication system of the sensor node architecture (Physical, Links, Network protocols …), so each entity should be secured well from being attacked or any accidental loss of data. The higher the sensitivity of the data transmitted due to sensor's application (e.g. temperature information), the higher the importance of securing networking layers.

The main issues of security involve authentication (Only the trusted elements of the network could register themselves and no other intruders take place in registration process), privacy (Keeping the boundaries of the network elements without interaction with another networks and hence the networks elements with each others) and integrity (Data is confidentially received and stored to the authenticated elements with no missed or replaced parts) [28].

There are multiple reasons for threats that attack the physical layer of the network elements including physical damage or signal interference or jamming; that leads to replacement of a network original element signal with fallacious source [22]. Beside that there are another types of attacks other layers [5, 28, 29]:

- *Denial of Service (DoS):* A general term that denotes the failure/absence of network elements due to some kind of attack and may be defined of a trial to lower the network's capacity. It may occur in all layers of communication system. In physical layer by jamming or tampering. For the data link layer it may be caused by exhaustion, data collision, and unfairness. In network layer by greediness or neglecting for packets. For transport layer it's a result of de-synchronization or malicious flooding. In all cases this kind of attack could be managed by enhanced authentication or ID handling.

- *Attacks of Information on transit:* As known for the mechanism of WSNs, all nodes reports their data to beacon/anchor nodes for data collection. During the report transmission, the transit mode of information transmission includes vanishing, spoofing, replaying and altering of data. In this stage any intruder that has high capabilities of power and processing can take place to modify the data by any form. This type of network attack could be avoided by some kind of powerful authentication or data aggregation.

- *Replay Attack:* The simplest way for attacker with limited efforts; where one node is jammed by attacker and then replaced by this foreign element that acts as sender then it replays the message.

- *Sybil Attack:* This type of attacking is more complicated than previous one. The attacker is pretending of multiple IDs of network nodes that affects the data integrity of the routing algorithm. The validation methods are used to prevent this attack which mostly targets peer-to-peer topologies.

- *Hello Flood Attack:* The attacking elements here deceive the original nodes through hello packets sent by highly transmitted power within a widely spread network. These packets are sent as if from genuine node, so the other nodes deal with it as network part and paths data through it. This type of attack could be managed by blocking techniques.

- *Wormhole Attack:* The higher complicated technique of all. Through tunnelling mechanism the attacker register packets between two or more nodes inside the WSN then takes place inside this tunnel. It mostly performed at the initiation stage of message exchange between nodes to discover each others.

- *Blackhole/Sinkhole Attack:* Where a wily node takes a blackhole role between nodes and the base station by attracting the data flow then managing the working routing protocol when it takes control of other nodes that based on presenting itself as the shortest path and better choice as a hop between nodes and base stations. This type can control even the nodes that are not nearby the base stations.

The security of WSN is a rich field for researches. There is some proposed solutions include [5]: SeRLoc (for wormhole and sybil attacks), Beacon Suite (to avoid malicious anchors and detecting replayed signals), Attack resistant location estimation (by estimating minimum mean square error or by voting-based location), and SPINE (by distance bounding to at least three anchors). There are many other methods and schemes and the security trend attracts more and more enhancements.

9 FUTURE WORK AND NEW TRENDS

Wireless sensor networks generally and the field of localization particularly are still engaging a wide area of research and development like:

- Developing new techniques that rationalize GPS usage as it's not energy efficient and costs much for hardware construction with low performance inside indoor environments (Line-of-sight propagation problems).
- Error minimization to increase accuracy of estimation the sensor node location, which includes using mathematical and geometrical relationships and developing new measurement techniques (may be hybrid technique between old techniques).
- Mobility of sensor nodes in some applications may change network topology that leads to new field of researches that could track the changes and keep location estimation.
- Enhancements for network topologies density to reduce number of anchors/beacons required to estimate good coverage for all other sensor nodes.
- The 3D localization still an area of interest of some researches as most of researches concentrates on plan surfaces which may be not efficient to simulate in the real world.
- New implementation for lower cost hardware with higher power efficiency especially for high precise techniques in range-based category, that also involving enhancements for performance keys (Longer battery life, higher processing speed, more storage memory and minimizing sensor node hardware size).
- Security threats and attacks are subjected to more researches, to enhance the current securing schemes and to develop more secured protocols with powerful detection algorithms.

In addition of the previously mentioned area of researches there are many new trends and points of view for localization problem, one of these trends is using Social Network Analysis (SNA).SNA deals with any network as a set of relationships between players (in our case it's the sensor nodes) and ties (links between sensor nodes). That field is promising and takes place in many researches not only in electrical communication track, includes metrics of measurements between nodes to be accessible with multiple layouts to contribute sensor nodes. SNA based mainly on graphic theory which gives new aspects to deal with WSN efficiently [33].

10 REFERENCES

[1] M. Maksimović and V. Milošević, “Evaluating the Optimal Sensor Placement for smoke detection,” Yugoslav Journal of Operations Research, p. 1, Jan. 2015.

[2] P. Amitangshu, “Localization Algorithms in Wireless Sensor Networks: Current Approaches and Future Challenges,” Network Protocols and Algorithm, vol.2, No.1, pp.46-48, 2010.

[3] K. Sohraby, D. Minoli & T. Znati, “Wireless Sensor Networks – Technology, Protocols and Applications,” Hoboken, New Jersey: John Wiley & Sons., 2007.

[4] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. CayirciS., “Wireless sensor network: a survey,” Computer Networks, vol. 38, p.394, 2002.

[5] A. Srinivasan and J. Wu, “A Survey on Secure Localization in Wireless Sensor Networks,” Florida Atlantic University, Boca Raton, FL, USA, pp. 4-11, 2010.

[6] M. Vojdani, M. Dehghan, “Localization in Anchor less Wireless Sensor Network,” in International Conference on Computer Engineering and Applications, Singapore, 2011, vol.2, pp. 365-368.

[7] C. Başran, “A hybrid localization algorithm for wireless sensor networks,” M. Science. thesis, Yeditepe University, Istanbul, Turkey, 2007.

[8] P. Bahl, and V. N. Padmanabhan, “An In-Building RF-Based User Location and Tracking System,” in Proc. IEEE INFOCOM’00, March 2000

[9] L. Zhetao, L. Renfa, Y. Wei, and T. Rei, “Survey of Localization Techniques in Wireless Sensor Networks,” Information

Technology Journal 9, vol. 8, pp. 1754-1757, 2010.

[10] P. Brida, P. Cepel, and J. Duha, “Geometric Algorithm for Received Signal Strength Based Mobile Positioning,” Radio Engineering, vol. 14, pp. 3, Apr. 2005.

[11] B. H. Wellenhoff, H. Lichtnengger and J. Collins, Global Positions System: Theory and Practice, 4th ed., Springer-Verlag, 1997.

[12] N. Patwari, A. O. Hero, M. Perkins, N. S. Correal, and R. J. Odea, “Relative Location Estimation in Wireless Sensor Networks,” IEEE Transactions on Signal Processing, vol. 51, No.8, Aug. 2003.

[13] Y. Lio and Z. Yang, Location, Localization, and Localizability Location- awareness technology for Wireless Network, 1st ed., Ed. New York, USA: Springer-Verlag, 2011.

[14] F. Gustafsson, and F. Gunnarsson, “Positioning using time-difference of arrival measurements,” in Proc. ICASSP’03, 2003, vol. 6, pp. 553–6.

[15] T. He, C. Huang, B. Blum, J. Stankovic, and T. Abdelzaher, “Range-free localiaztion schemes in large scale sensor networks,” in Proc. MobiCom’03, Sep. 2003, pp. 81-95.

[16] N. A. Rajeh, M. Bashir, and B. Shams, “Localization Techniques in Wireless Sensor Networks,” International Journal of Distributed Sensor Networks, vol. 2013, pp. 1–9, June. 2013.

[17] S. Singh, R. Shakaya, and Y. Singh, “Localization Techniques in Wireless Sensor Networks,” International Journal of Computer Science and Information Technologies, vol.6, pp. 844–850, 2015.

[18] M. Aboelaze, and F. Aloul, “Current and Future Trends in Sensor Networks: A Survey,” in Proc. WOCON’05, 2005, paper 10.1109, pp. 551-555.

[19] R. Manzoor, “Energy efficient localization in wireless sensor network using noisy measurements,” M. S. thesis , Jan. 2010.

[20] F. Hu and X. Cao, Wireless Sensor Networks: Principles and Practice , 1st ed., FL, USA: Auerbach Publications, 2010.

[21] Y. Xu, J. Heidemann, and D. Estrin, “Geography-informed energy conservation for ad hoc routing,” in Proc. Mobicom’01, 2001, pp. 70-84.

[22] J. Sen, “A Survey on Wireless Sensor Network Security,” International Journal of Communication Networks and Information Security, vol. 1, pp. 55-78, Aug. 2009.

[23] K. Romer ,and F. Mattern, “The Design Space of Wireless Sensor Networks,” IEEE Wireless Communications, vol. 11, pp. 54-61, Dec. 2004.

[24] Y. Chraibi, “Localization in Wireless Sensor Networks,” M. thesis, KTH, Stockholm, Sweden, 2005.

[25] I. Rekleitis, “A Particle Filter Tutorial for Mobile Robot Localization,” Center of Intelligent Machines, McGill University, Montreal, Quebec, Canada, Tech. Rep. TR-CIM-04-02, 2004.

[26] W. Liu, D. Wang, H. Jiang and W. Liu, “Approximate convex decomposition based localization in wireless sensor networks,” in Proc. INFOCOM’12, 2012, paper 10.1109, pp. 1853-1861.

[27] P. Jun-geun, E. D. Demaine, and S. Teller, “Moving-Baseline Localization,” in Proc. IPSN’08, 2008, paper 10.1109, pp. 15-26.

[28] A. K. Pathan, H. W. Lee, and C. S. Hong, “Security in Wireless Sensor Networks: Issues ans Challenges,” in Proc. ICACT’06, 2006, paper 89-5519-129-4, pp. 1043-1048.

[29] A. Pandey, and R. C. Tripathi “A Survey on Wireless Sensor Networks Security,” International Journal of Computer Applications, vol.3, No.2, pp.43-49, 2010.

[30] J. L. Hill, “System Architecture for Wireless Sensor Networks,” PhD. thesis, University of California, Berkeley, USA, 2003.

[31] S. A. Mitilineos, D. M. Kyriazanos, O. E. Segou, J. N. Goufas and S. C. A. Thomopoulos “Indoor Localization with Wireless Sensor Networks,” Electromagnetic Research, vol.109, pp.441-474, 2010.

[32] K. Mondal, P. S. Mandal, and B. P. Sinha “Localization in Presence of Multipath Effect in Wireless Sensor Networks,” in Proc. WWIC’12, 2012, paper 10.1007, pp. 138-149.

[33] A. Papadimitriou, D. Katsaros, and Y. Manolopoulos Ed., Next Generation Society. Technological and Legal Issues: Social Network Analysis and Its Applications in Wireless Sensor and Vehicular Networks, ser. Lecture Notes of the Institute for Computer Science, Social Informatics and Telecommunications Engineering. Athens, Greece: Springer, 2010, vol. 26, pp.411-420.

[34] D. Verma, S. Umrao, R. Verma, and A. Kumar “A Localization Technique in Wireless Sensor Network based on Angle of Arrival,” International Journal of Computer Applications, vol.98, No.7, pp.26-29, 2014.

[35] A. Shrivastava, and B. Bharti “Localization Techniques in Wireless Sensor Networks,” International Journal of Computer Applications, vol.116, No.12, pp.13-18, 2015.

[36] L. Lazos, and R. Poovendran, “SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks,” in Proc. WiSe’04, 2004, pp. 21-30.

[37] C. Liu, and K. Wu, “Performance Evaluation of Range-Free Localization Methods for Wireless Sensor Networks,” in Proc. IPCCC’05, 2005, pp. 59-66.

[38] C. Liu, K. Wu, and T. He, “Sensor localization with Ring Overlapping based on Comparison of Received Signal Strength Indicator,” in Proc., IEEE Mobile Ad-hoc and Sensor Systems’04 , 2004, pp. 516-518.

[39] G. S. Klogo, and J. D. Gadze, “Energy Constraints of Localization Techniques in Wireless Sensor Networks,” International Journal of Computer Applicationss, vol.75-No.9, pp. 44-52, 2013.