A Hybrid Fuzzy System Based Cooperative Scalable and Secured Localization Scheme for Wireless Sensor Networks

Abhishek Kumar

iNurture Education Solutions Private Limited, India

Abstract

Localization entails position estimation of sensor nodes by employing different techniques and mathematical computations. Localizable sensors also form an inherent part in the functioning of IoT devices and robotics. In this article, the author extends[1] a novel scheme for node localization implemented using a hybrid fuzzy logic system to trace the node locations inside the deployment region, presented by the Abhishek Kumar et. al. The results obtained were then optimized using Gauss Newton Optimization to improve the localization accuracy by 50% to 90% vis-à-vis weighted centroid and other fuzzy based localization algorithms. This article attempts to scale the proposed scheme for large number of sensor nodes to emulate somewhat real world scenario by introducing cooperative localization in previous presented work. The study also analyses the effectiveness of such scaling by comparing the localization accuracy. In next section, the article incorporates security in the proposed cooperative localization approach to detect malicious nodes/anchors by mutual authentication using El Gamel digital Signature scheme. A detailed study of the impact of incorporating security and scaling on average processing time and localization coverage has also been performed. The processing time increased by a factor of 2.5s for 500 nodes (can be attributed to more number of iterations and computations and large deployment area with small radio range of nodes) and coverage remained almost equal, albeit slightly low by a factor of 1% to 2%. Apart from these, the article also discusses the impact of adding extra functionalities in the proposed hybrid fuzzy system based localization scheme on processing time and localization accuracy. Lastly, this study also briefs about how the proposed scalable, cooperative and secure localization scheme tackles the type of attacks that pose threat to localization.

Keywords

Sugeno Fuzzy Inference Systems, Mamdani Fuzzy Inference Systems, Localization algorithms, Gauss Newton method, Cooperative localization, Mutual authentication, Elgamel Digital Signature

1. Introduction

The unprecedented surge in the usage of sensors and thus the sensor networks in new avenues such as cyber physical systems, smart homes, smart cities etc. has attracted the attention of multitude of researchers across the globe. Sensor networks are autonomous collection of tiny, resource constrained sensor nodes, which operate in ad hoc manner and forwarding data and

[1] This article is extended version of paper titled "A Sugeno- Mamdani Fuzzy System Based Soft Computing Approach Towards Sensor Node Localization with Optimization" presented in 3rd International Conference on Next Generation Computing Technologies (NGCT 2017), Dehradun India

DOI: 10.5121/ijwmn.2018.10305

information sensed or gathered to base station or sink node. The manner in which they are constructed, these nodes and the network are subjected to challenges such as limited battery or power source, limited coverage region, no support in terms of available infrastructure, susceptible to interferences in communication due to open nature of media of transmission, channel constraints in terms of available bandwidth etc.

Localization refers to the computation process of figuring out the position of sensor nodes in the rectangular deployment area by the aide of some known nodes called anchors/landmarks. Categorically speaking, any localization technique can be either range based or range free. Range based schemes rely on and utilize explicit ranging information in terms of Received Signal Strength Indicator (RSSI), Time of Arrival (ToA), Time Difference of Arrival (TDoA) etc to measure the range or distance in terms of variation in parameters of signal such as signal strength and latency in signal reception. Range free schemes, on the other hand, utilize the connectivity information in terms of hop count. Their computation is simpler and does not require antenna arrays, but need more anchors/landmarks (nodes whose position is already known to us and would be used to compute the location of other unknown sensors in the deployment region).

Secure localization is an imperative task as the sensor operations are typically unattended and media of communication is insecure. Thus any adversary can tamper with the sensor operation or any malicious node can be added into the deployment region and can attack as genuine node/anchor. In context of localization, the security is particularly important because any imprecise or fake location information can affect the routing process (any position broadcasted as unreachable from a particular node might corrupt the entire routing table of that node), data aggregation, packet forwarding (a malicious node can collude with another node to create a wormhole and thus intercept all packets forwarded via that wormhole link). Other attacks such as Sybil attack, masquerading attacks etc. pose similar threat to localization and the overall topology of wireless sensor network. It is the node's task to compute the location information, considering distributed localization scheme but the onus lies on the base station to ensure that such information is accurate because the resources at the disposal of individual sensor nodes are not sufficient to verify the location and validate the other sensors nodes from which it is receiving data or anchor nodes from which it is receiving beacons to compute location.

Another issue in localization is how to scale or extend the existing localization algorithms to large number of sensor nodes. Most of the existing work on localization take into consideration 50-150 nodes and then deploy their approach to find their location. The study presented by the author in [1] tackles location determination of 100 nodes efficiently with cost effective, low latency, low overhead. In this extended version we are formulating cooperative and scalable localization scheme having hybrid Sugeno-Mamdani fuzzy system as its core, to tract localization of 500 nodes deployed in a particular region.

The organization of the rest of the paper is in following manner: Section 2 presents an intensive literature review on existing works done on hybrid fuzzy systems, secured localization and cooperative localization schemes. Section 3 covers the hybrid fuzzy logic system based localization scheme presented by the Abhishek Kumar et al**.** in [1]; Section 4 discusses a cooperative localization scheme; Section 5 incorporates security with digital signature scheme to achieve node validation via mutual authentication; followed by conclusion and future research directions in Section 6.

2. RELATED WORK

The work done by Ashok Kumar et al. in [2] [3] devised a fuzzy based localization scheme by feeding RSSI and Link Quality Indicators (LQI) as inputs to the constructed fuzzy model (the rule set) and weight as output. The weight was then utilized into weighted centroid algorithm to compute the position coordinated of unknown sensors. The authors have comprehensively studied Sugeno type fuzzy system, Mamdani type fuzzy system, a hybrid of their combinations and ANFIS trained Sugeno type fuzzy system. The localization error of their experiments and simulations varies from 0.76m to 0.95m, depending upon the type of fuzzy inference system used. The work presented in [1] has drawn motivation from the study done by above authors, as an attempt to improve the localization accuracy and cost by using least number of anchors/ landmarks to achieve the localization of unknown sensor nodes.

A somewhat similar study has been done by Arbabi Monfared in [4]. The author modelled a nine rule-set based Sugeno type fuzzy system to compute weigh values in range [0, 1] corresponding to a RSSI value in range [-80 dB, 0 dB]. Taking into the account the Additive Gaussian White Noise (AWGN) with Signal to Noise ratio value of 10 dB, the average localization error was 0. 30m.The same study conducted in outdoor experiments led to localization error of 0.53m.

The study done by Gharghan et al. in [5], the authors constructed an ANFIS (Adaptive Neuro Fuzzy Inference System) trained Mamdani fuzzy system with three, five and seven membership functions. For the purpose of training, a ratio of deployed nodes was put in training set and rest of the nodes in testing set. The study was performed in indoor environment and was replicated in outdoor conditions. The localization error, both mean and root square error, was greater in case of indoor experiment scenario as compared to experiment conducted in outdoor environment, largely due to effects of multipath propagation and scattering. Also, it was observed that with increase in the number of membership functions and rules, the localization error reduced gradually.

A few more existing works on fuzzy system based location estimation have been done in [6] [7]. All of these works model the range component such as RSSI or ToA and weight as set of rules. The Fuzzy system, then, depending on whether it is a Sugeno fuzzy logic or Mamdani fuzzy logic, is implemented on set of rules modelled.

In their study, Nan et al. in [8] least square estimation and maximum likelihood computation techniques cannot effectively tackle location estimation in cooperative manner as they do not consider position of neighbour nodes. The situation gets more troublesome in sparse networks in harsh environments as we have lesser number to nodes to gather information from. Authors proposed a distributed and cooperative location estimation technique incorporating Gaussian Message Passing (GMP) by non-linearly modelling the network as factor graphs. Since the network was modelled non-linearly, Taylor expansion was used to approximate non-linear factors. Authors compared their scheme with existing Monte Carlo scheme and Sum Product Algorithm (SPA) to claim that complexity and communication overhead of their proposed technique was 50-70% lower than SPA and MCL.

In the study done by [9] authors took into consideration distance and direction to propose hybrid message passing based location determination technique. Authors then used Bayesian estimation to approximate Minimum Mean Square Error (MMSE). The position of neighbor nodes was also taken into consideration as posterior distribution. The algorithm was numerically stable as convergence was achieved in lesser than 10 iterations. Computational complexity was directly proportional to square of number of neighbor nodes. The mean localization error was 0.45cm, better than any other message passing based localization algorithm. T.Chowdhary in his PhD Thesis [10] studied distributed cooperative localization technique based on Gaussian Modelling of sensor networks. The author implemented several algorithms namely: Expected Maximization (EM), Gaussian Mixture Model (GMM), Broyden- Fletcher- Goldfrab- Shanno (BFGS) Quasi Newton (QN), and Davidan- Fletcher- Powell (DFP). All of the proposed algorithms approximate the maximum likelihood estimates and scale well with large sensor networks. The proposed scheme in this paper has been compared against all the above mentioned techniques. Here it must be noted that all the above mentioned algorithms take into consideration Cramer Rao Lower Bounds (CRLB) whereas, our scheme outperforms them without any consideration of lower bounds.

DV hop localization technique [11] is a connectivity based scheme where localization is achieved by exploiting connectivity information of nodes rather than relying on source signal strength. Liu et al. [12] in their study propose robust DV Hop scheme secure against flooding attacks and node captures. The proposed technique comprised of 4 phases: Initialization phase in which base station creates random keys for each anchor and a hash chain is generated based on connectivity of that anchor; Hop count calculation phase in which each unknown sensor node was ensured minimal hop count to a particular anchor; Hop size calculation phase in which unknown sensor node computed average weighted distance to an anchor node; and last phase was location estimation phase where with the help of three anchors an unknown node localizes itself. Simulations showed that in a deployment region of 100×100 m2, radio communication range of being 15m and 20% anchor ratio, the average localization error was 0.4m. Same study duplicated for radio range of 10m and 500 sensor nodes with 100 anchors showed mean localization error of ~0.9m.

Chen, Honglong, Wang et al [13] has proposed secure localizing algorithm based on DV-Hop known as SDV-Hop. The authors distinctly devised two methods: first method to tackle against the masquerading attack and second constituted average-per-hop-distance calculation method on the behalf of security-processing. In their approach, authors emphasized on the features of the DV-Hop and proposed a new improved symmetric-code-encryption algorithm for encryption in communication. As the basic DV-Hop algorithm is attackable so there is need to choose appropriate average-per-hop-distance for correct and secure positioning. The new proposed approach SDV-Hop finds the hop-count and path-length for appropriate distance. WeightedAverage method was used in this approach to find the correct hop-distance and it efficiently removed the errors resulted due the worm-hole attack and increased the location-accuracy. In new approach, the localization error- rate was 21.32% less, error-rate in the case of worm-hole attack was 18.96% lower in comparison to the basic DV-Hop and in case of block-attack, and error–rate was 22.12% less. A simulation results narrated that the proposed algorithm warranted higher location accuracy and prevented attacks such as worm-hole attack, masquerading-attack and block-attack.

Wei Shi et al [14] proposed algorithm that was designed to work in decentralized manner to find the position of the unknown-node in the presence of the colluder. This approach permitted the sensor to identify its position and identify the colluder those are within the bi-directional transmission range. Colluders were identified on the basis of threats created and posed by them. This approach did not rely on any authentication and cryptography primitives. It used verification lists called cross check lists (CRR). Three types of colluders could be identified by this approach and to which category attacker is related depended on the how the attacker published its position. Type one attacker performed the attack by communicating forgery detail. Type two attackers communicated the forgery detail with collaboration of the other two malicious-nodes. Type of three attacks implemented the evil-ring attack techniques. All these three types of attacks and description of the algorithm has been extensively studied by the authors. A simulation result narrated that two different types of environments were validated as random-distribution and uniform-deployment of the nodes.

A trust valuation based secured localization scheme has been proposed in [15] which was studied to be robust against spoofing, node duplication and Sybil attacks. The proposed scheme comprised of different types of trusts: Comprehensive trust (derived from average localization error and latency of anchors); direct trust (derived from belief of unknown sensor node in that beacon); and indirect trust (derived from location information an unknown node receives from its neighbors). All these trust values were framed on a set of attributes. Simulation results showed that for a 100×100 m2 deployment region of 100 nodes with 40% anchors, radio range of 20m, the average localization error was ~1m when malicious nodes were less than 20, but increased exponentially to ~4.5m when malicious nodes were about 40. After implementing the trust values, the average localization error was normalized to ~0.6m. We duplicated this study for 500 sensors deployed in same area with radio range of 10m and 50 malicious nodes and found the average localization error to be ~1.2m after applying the trust values. Without trust values the error peaked to ~30m.A comparison of this scenario with our proposed scheme has been presented in Section 5.

3. A Hybrid Fuzzy System Based Localization With Optimization

This section summarizes the work proposed by the **Abhishek Kumar et al.** and presented in [1]. The study comprised of five rule-set based hybrid fuzzy inference system modelled using combination of both Mamdani fuzzy logic and Sugeno fuzzy logic. RSSI was fed as input in hybrid fuzzy system and weight was obtained as output. The weight reflected the farness or nearness of an anchor with respect to unknown sensor node. It is worth mentioning that there exists a trade-off between number of rules formed and performance in terms of localization accuracy. Prima facie and empirical studies conducted through experiments suggested that with increase in number of rules and membership functions in the fuzzy logic, more fine grained results could be obtained and accuracy could be improved. However, that also puts memory burden on already resource constrained sensor nodes. This study attempts to achieve better accuracy with lesser number of rules and membership functions. The rule set used for this study is as follows:

Table 1: RSSI vs Weight Rule set

	RSSI	**Weight**
Rule 1	Very_Low	Very_Low
Rule 2	Low	Low
Rule 3	Medium	Medium
Rule 4	High	High
Rule 5	Very_High	Very_High

Algorithm 1: Fuzzy System based Localization with Optimization

```
1: **Procedure** Position Estimation using hybrid fuzzy logic
2:     Select a regular square-shaped deployment region of dimensions 10*10m.
3:     Deploy one anchor each at four corners of the region
4:     Distribute unknown nodes randomly using Gaussian or normal distribution
5:     Compute Euclidean distance between each unknown with every anchor.
6:     Compute RSSI value with path loss exponent factor (n) as 3.25

           $RSSI\ [dBm] = RSSI_{src} - 10 * n * log_{10}(\frac{dist}{dist_{src}})$

7:         distsrc is taken to be 1m and RSSIsrc is RSSI value at a distance 1m
8:     Use RSSI [dBm] as input to Sugeno FIS
9:     Use RSSI [dBm] as input to Mamdani FIS
10:    Calculate average weight= (Weight_Sugeno + Weight_Mamdani) / 2
11:    Estimate position using weighted centroid technique
12:    Formulate Least Square Problem function as :

           $f(x, y) = \frac{1}{A}\sum_{i=1}^{A}(\sqrt{(\hat{x}_{est} - x_i)^2 + (\hat{y}_{act} - y_i)^2} - \tilde{d}_i)$

13:    $\tilde{d}i$ is distance corresponding to additive noise and standard deviation approximated as
       distance measurement    error of 0.1
14:    Apply Gauss Newton method with number of iterations equal to 100, to compute the
       minimum of the function in Step 12
15:    Compute Average Localization Error (ALE) after employing Gauss Newton Optimization.
16: **End Procedure**
```

The proposed approach was implemented in MATLAB 2015a using the fuzzy logic tool box. The deployment area was 10*10m 2-D region. Each of the 4 anchor was placed at 4 corners of the network region i.e. the anchors were at (0, 0), (0, 10), (10, 0), (10, 10). The unknown nodes were randomly deployed using Gaussian distribution. Both Mamdani type fuzzy sytem and Sugeno type fuzzy logic were individually modelled using fuzzy logic tool box available in MATLAB. The output weight from each was then averaged together to get the net weight as depicted in algorithm 1.

Figure 2 shows the localization before employing the Gauss Newton optimization. The cluttered behaviour of localization can be attributed to uncertainty modelling of fuzzy systems which, tried to limit the weight to a particular value in corresponding to a particular range of RSSI [dBm] values and hence the position obtained seemed to be overlapping for multiple unknown sensors. The mean estimation localization error ranged from 3 to 4m, varying as the numerous simulations were run.

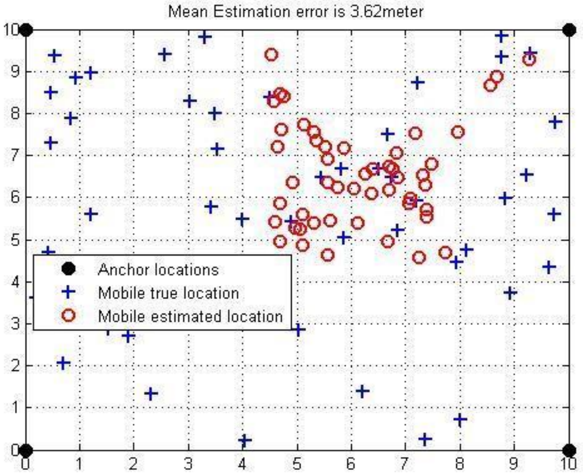

Figure 2: Average Localization Error without Gauss Newton Method

Figure 3 depicts the node localization after employing the Gauss Newton optimization. The localization error was being reduced very significantly i.e. from 3.62m to 0.42095m and that led to a very considerable improvement in localization accuracy. Furthermore, the operation efficiency of GN method largely contributed to low complexity as the least square problem formulated in GNO contained only two variables and only first order derivative was needed to be calculated. So the overhead involved is also low.

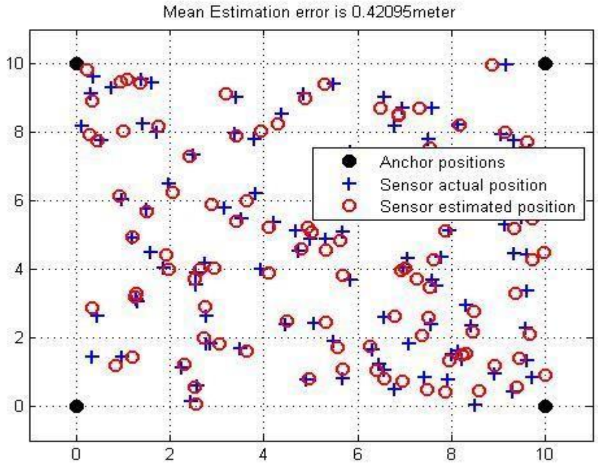

Figure 3: Average Localization Error with Gauss Newton Optimization

A tabular representation of comparison of existing schemes with proposed one has been depicted in below table 2:

Table 2: Comparison of localization error of various techniques

Technique	Mean Estimation Error (in meters)	Number/Ratio of anchors
Simple Centroid	1.6080	66.8%
Mamdani Fuzzy Logic	0.8956	66.8%
Sugeno Fuzzy Logic	0.9462	66.8%
Sugeno- Mamdani ANFIS	0.7664	66.8%
Probabilistic Fuzzy	1.9928	121
3 *trimf* ANFIS	3.5810	-----
Proposed scheme	0.4295	4

4. COOPERATIVE LOCALIZATION SCHEME

The proposed work in Section 3 accomplished localization with 4 anchors. But this situation presents a bottleneck if we have to deploy sensors in the range of thousands. Creating clusters of 100- 200 nodes offer good solution, but data forwarding from different clusters and gathering at the base station induces some latency. So a good solution is to formulate cooperative localization scheme. In such scheme, whenever an unknown node gets localized, It acts as anchor/landmark for next iteration and transmits beacon to other unknown node (Since it has already been localized it is aware of its position now and can broadcast beacons which contain its position, identity to be received by other unknown nodes in its radio transmission range).

The parameters for the simulation have been provided below considering the scaled version of the Algorithm 1 presented in section 3. The following algorithm represents cooperative localization incorporated into hybrid fuzzy based localization scheme shown in Algorithm 2.

4.1 Proposed Scheme

Set {U} = (U1, U2, U3……) is the set of unknown sensor nodes and set {A} is the set of anchors/landmarks. Algorithm begins with four anchors (A1, A2, A3, A4). Let ℿ(U) be the number of unknown sensor nodes at any given instant and ℿ(A) be the number of anchors at any instant of time.

Table 3. Simulation Parameters

Number of Unknown Sensor nodes {U} = 500
Deployment region = 100×100 m^2
Radio range= 10m
Mode of node deployment: Randomly deployed
Topology: Regular Square shaped
Initial number of Anchors {A}: 4
Mode of communication: Time Division Multiplexing (TDM)

Below is the algorithm for cooperative localization. Observe that algorithm given in section 3 serves as primitive localization algorithm for the deployment.

Algorithm 2: Cooperative Localization

```
1: **Routine** Position Estimation with Cooperative Scheme
2:              Input:- Set {U} of unknown sensor nodes
3:           Set {A}= {A1,A2,A3,A4} of known anchors
4:      Run Step 1 to 11 of Algorithm 1
5:      Assume $\Delta$ is the number of unknown sensors localized in Step 4.
6:            $\Pi(A)= \Pi(A)+\Delta$
7:            $\Pi(U)= \Pi(U)-\Delta$
8:      **for** i= 1 to $\Delta$
9:          do
10:             Add $U_i$ ( $1\le i\le \Delta$) to {A}
11:             Remove Ui ($1\le i\le\Delta$) from {U}
12:     **End for**
13:      Update {A}
14:      Update {U}
15:     Repeat step 1 to 14 till {U} = $\phi$, $\Pi(U)= 0$. (This means all the unknown sensor nodes has
        been successfully localized and have become anchors)
16:     Run Step 12 to 15 of algorithm 1 to optimize the localization accuracy using Gauss
        Newton Optimization.
17:     End Algorithm 1
18: **End routine**
```

4.2 Results and Discussion

The algorithm proposed and implemented in Section 3 considered 100 nodes deployed in area of 10×10 m^2. The above algorithm extends and scales the proposed scheme in Section 3 to a network of 500 nodes deployed in a region of 100×100 m^2. We implemented the Algorithm. 2 to achieve the cooperative localization. The localization accuracy was then optimized using Gauss Newton Method by formulating the least square problem as shown and implemented in Algorithm. 1. The following results were observed after implementing the aforementioned algorithm as per set parameters:

The localization coverage was 79 % when the percentage of anchor was 5% i.e. 25 nodes became anchor and then were able to localize 79% of remaining 475 nodes. The coverage increased to 97% when the percentage of anchors became 40-45%. One can easily contrast it with the proposed scheme in section 3 where the localization coverage was 97% for 100 nodes. Here we have been able to scale our approach to achieve 97% coverage for 500 nodes by increasing the number of anchors via implementing Cooperative approach. This can be visualized from Figure 4. Here it must be noted that the existing works mentioned in the line graph incorporating cooperative localization did not consider Coverage as one of the factors to judge effectiveness of their scheme. The author implemented those algorithms also as a part of this study and found out percentage of coverage on the mentioned parameters in Table 3 to compare with our proposed scheme.

It can easily be visualized that the coverage percentage of our proposed scheme is several factors better than the existing cooperative localization schemes.

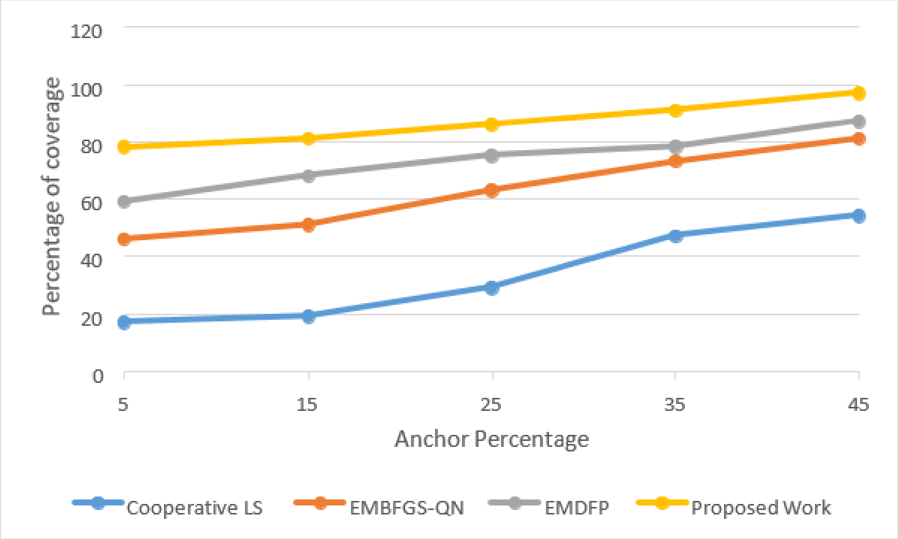

Figure 4: Line graph of coverage vs anchor placement

- The approach is also cost effective as we actually started with only 4 anchors and we increased the number of anchors by not actually adding physical anchors (i.e. deploying GPS on them). Instead more anchors were added by localizing unknown nodes and treating them as anchors.
- The processing time complexity increases from ~1.5s-2s in the previous algorithm (Algorithm 1) to ~4.5s- 5s since the number of iterations have increased with increase in number of nodes and also the deployment region has also been increased from 10×10 m^2 to 100×100 m^2 but the radio communication range is same as 10m. Hence some latency in sending and receiving beacons are inevitable. Existing algorithms did not consider average processing time as a measure of effectiveness.
- A comparison of accuracy in terms of Average Localization Error (ALE) of proposed work with existing cooperative localization scheme is presented in Table 4:

Table 4. Comparison of ALE of proposed scheme with existing cooperative techniques

Algorithm	Deployment area	ALE (in meters)
Cooperative LS	100×100 m^2	1.8638
EM BFGS-QN	100×100 m^2	0.6708
EM DFP	100×100 m^2	1.4320
Proposed Scheme (Before optimization)	100×100 m^2	4.3212
Proposed Scheme after optimization	100×100 m^2	0.6108

The average localization error before employing the Gauss Newton method was nearly 4.3212m. It was largely due to the fact that radio range was very small as compared to the deployment area. That led to less number of beacons being received by unknown sensor nodes and incorrect computation of position values. Employing the GN method minimized the value of average localization error by pruning the values of inaccurate computations as depicted in step 10 of Algorithm 1. The principal reason because of which the proposed scheme outperforms LS, EM BFGS QN and EM DFP is that these algorithms involve lots of computations and approximations and consequently inaccuracy in one iteration is propagated to multiple iterations leading to greater cumulative average localization error.

5. Secure Localization With Node Authentication

As discussed in Section 1 security is also imperative to localization issue in wireless sensor networks. Any node can act as anchor maliciously and broadcast fake/incorrect position information to other sensor nodes in its radio range. That would lead to inaccurate location computation by those nodes and hence could affect other processes such as routing, data forwarding and data gathering at Base Station or Sink Node (SN). Hence it is important that nodes must validate or authenticate the identity of anchor node from whom it has received beacon, before it can proceed with localization process. In this section, the author proposes a novel secure localization scheme incorporating mutual node authentication with El Gamel digital signature scheme. This study decided to choose El Gamel as it is the simplest signature scheme among available authentication methods, and thus would not put too much additional burden on Nodes computational efficiency and constraint on resources at their disposal.

The key generation part of the algorithm is taken care by SN as it required computations in finite fields. Any computation in finite field (GF (Z)) is hard and requires extensive resources which only base station or SN can possess. Rest of the parts of algorithms can be implemented on each node independently.

5.1 Proposed Scheme

STEP 1) Input: A set of anchors/landmarks {A} and set of unknown sensor nodes {U} deployed randomly as per the parameters provided in Section 3.

SN provides ID_{ai} to each anchor and ID_{uj} to each unknown node in {A} and {U} respectively.

STEPT 2) Key Generation Subroutine

```
Subroutine Key Generation
        Input:- large prime number p in $<Z_p, *>$
            Generator g1 in $<Z_p, *>$
        SN generates private key $PR_{ai}$ for every anchor $A_i$
        Select random number ɖ
            if
                (ɖ<p-1)
                    Proceed
            else
                    Chose different ɖ
        Compute   $g2 = g1^{ɖ} \bmod p$
        Public key of $A_i$ , $PU_{ai}$= ( g1, g2, p)
        Private key $PR_{ai}$= (ɖ)
End Subroutine
```

STEP 3) Signature Subroutine

```
Subroutine Signature
    Input: - $A_i$ selects secret r generated by PRNG unique for each beacon
            broadcasted
        Compute $SIGN_1 = g1^{r} \bmod p$
        Compute $SIGN_2 = (ID_{ai} - ɖ \times SIGN_1) * r^{-1} \bmod (p-1)$
        $A_i$ broadcasts ($ID_{ai}$, $SIGN_1$, $SIGN_2$) to each unknown $U_j$ within its radio range.
End Subroutine
```

STEP 4) Verification Subroutine:

```
Subroutine Verification of Signatures
        Input:- p, SIGN1, SIGN2, IDai, {U}
          Uj determines if  $0 < SIGN_1 < p$
          Uj determines if $0 < SIGN_2 < (p-1)$
              if
                  ($SIGN_2 < (p-1)$)
                      Proceed
              else
                      Discard beacon received. Anchor is malicious
          Exit
          $U_i$ computes $ʂ1 = g_1^{ID_{ai}} \bmod p$
          $U_i$ computes $ʂ2 = g_{2SIGN1} \times SIGN_1^{SIGN_2} \bmod p$
              If ( ʂ1==ʂ2)
                      Genuine Anchor

              else
                      Malicious Anchor
                      Exit
Exit Subroutine
```

After the signature verification is complete, unknown sensor node is assured that the beacon it received was from a genuine anchor in the deployment area. It can then proceed with localization process by employing the Algorithm 2.

5.2 Results and Discussion

The proposed secured localization scheme was simulated in MATLAB 2015a with parameters mentioned in Table 3. The nodes were deployed randomly and some of the anchors were malicious. With the help of digital signature scheme the unknown sensor nodes were able to authenticate the true or genuine anchors/landmarks. In case of malicious anchors (denoted by red dot in simulation diagram), the unknown sensor nodes in its radio range discarded the beacons received from that malicious landmark. But they too were localized by another true anchor by deploying the cooperative localization scheme proposed in algorithm 2. Figure 5 below represents the scenario with true anchors, malicious anchors and unknown sensor nodes along with radio communication range of each node.

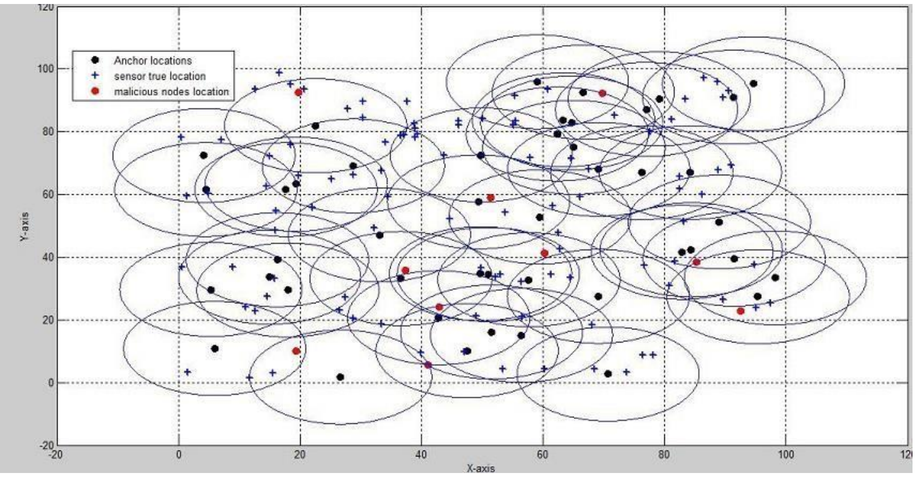

Figure 5: Secure Localization in presence of malicious anchors

5.2.1 Effect induced on processing time

The average processing time of the algorithm 1 that we presented in section 3 was 1.5s ~2s. After we incorporated the scaling and cooperative localization routine (algorithm 2), the processing time increased to ~3.5 to 4s. This was, as discussed earlier in section 4, due to increase in number of iterations and operations. Now, in the next phase, the research work has incorporated digital signature scheme to achieve a scalable, cooperative and secure localization scheme. Since key generation was done by SN beforehand, so this study did not consider its latency into average processing time. The average processing time after completion of signature and verification subroutine only was taken into consideration and it increased from ~4s to ~5.7s. The average computation time of El Gamel digital signature scheme for a message of 9 bits (512 decimal values possible and we have 500 sensor nodes, so we checked it for 9 bits) was ~ 1.4s. Therefore, incorporating authentication scheme is not putting any significant overhead on the cooperative scalable localization scheme presented in Algorithm 2. The line graph drawn in Figure. 6 below summarizes this discussion:

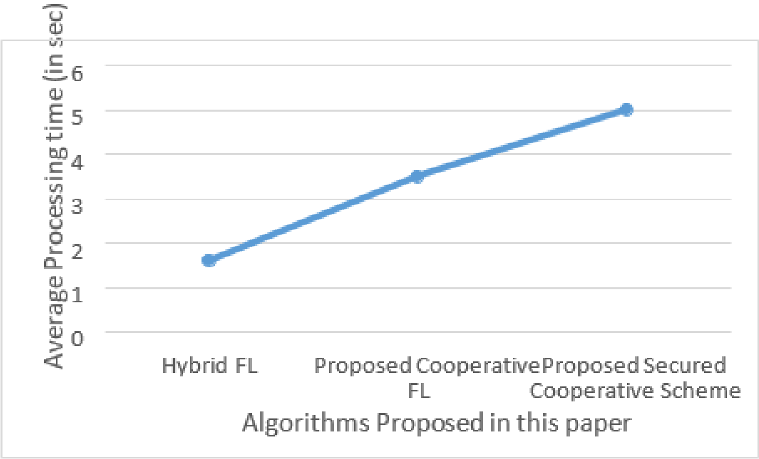

Figure 6: Overhead on processing time with adding additional capabilities

5.2.2 Attacks and Prevention Mechanism

As discussed in Section 1, localization process is susceptible to various security incapability and threats. The following Table. 5 presents the type of attacks that can perturb localization process [16] their brief description and how our proposed scheme protects such attacks.

Table 5. Description of attacks and prevention by proposed scheme

Type of Attack	Brief Description	Protection by proposed scheme
Sybil Attack	A node broadcasts with multiple identities	Not possible as IDs are predetermined by SN and authentication is also used.
Flooding Attack	An anchor opens too many half connections by sending repetitive SYN	Limited probability as radio range is very small and once anchor sends SYN its ID_{ai} is identified
Collision	Transmitting jamming signal on operating frequency and Interference	Limited scope as TDM is used as mode of operation
Stale packets	Sending old beacons/packets to violate data property	If same value of '*r*' is used, that means stale beacon
Exhaustion	Transmitting un necessary beacons to consume receiver's resources	Limited radio range ensures no scope for such attack
Tampering	Broadcasting false beacons	Authentication via digital signature is used
Key Related Attacks	Using brute force or factoring techniques to find Public and Private keys	Keys are with SN and computation done in Z_p finite field which is hard to factor.

5.2.3 Impact induced on localization accuracy

As more functionalities and capabilities are added to any process, some inefficiencies are inevitable to be induced. In this subsection we examine the impact on localization accuracy after incorporating cooperative scheme and security in the proposed Fuzzy Logic based localization algorithm shown in Algorithm 1.

The average localization error of the proposed Sugeno-Mamdani Fuzzy system based scheme (Algorithm 1) was ~0.43m. When the algorithm was scaled for larger number of nodes with cooperative scheme, the ALE was ~0.61m after optimization and similarly after incorporating the authentication scheme, the ALE became ~0.79m. We can conclude that even after increasing the number of sensors by significant amount (from 100 to 500) and adding more iterations and computations, there was not that much impact of average localization error. As it can be visualized from Figure 7, that localization error was normalized between 0.6m to 0.8m. It can be due to the fact that we implemented Gauss Newton optimization which is more computationally efficient and precise. And for security, we chose El Gamel scheme for authentication which is the simplest, equally robust than other authentication schemes and computationally complex operations such as key generation were done at SN.

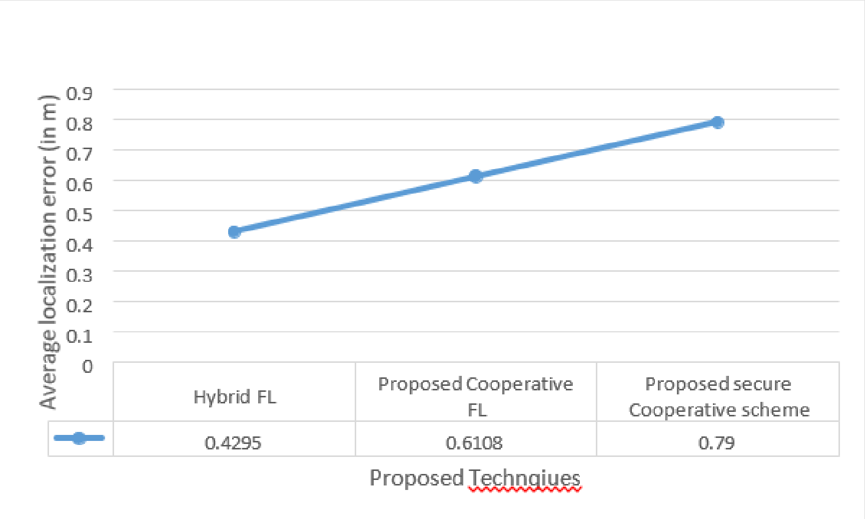

Figure 7: Impact on accuracy in terms of ALE

5.2.4 Comparison of Average Localization Error (ALE)

We compared the average localization error of the proposed scheme with some existing secure localization technique under simulation parameters mentioned in Table 3. SerLoc [17] focused directional antennas relying on source signal strength thus involved computational inaccuracy due to path loss and leading to high localization error. Secured DV hop and trust valuation schemes did not scale well for large number of sensor nodes and parameters mentioned in Table 3. Comparison of ALE has been presented in Table 6 below:

Table 6. Comparison of localization error of various schemes

Algorithm	Average Localization Error (in Meters)
SeRLoC	~1.45
Secured DV hop	~0.9
Trust valuation based scheme	~1.2
Proposed scheme	~0.79

6. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

Localization often requires modelling of the network which is a non-deterministic problem. The study done in this paper, attempted to tackle localization issue by modelling the network in to fuzzy logic systems, since fuzzy systems are apt at handling uncertainties. Results obtained were then optimized to ascertain better accuracy. Furthermore, a scalable cooperative scheme was proposed to offer a cost effective solution for large networks with greater number of node. Security was incorporated by adding an authenticated scheme so that unknown sensor nodes can differentiate between true and malicious anchors. Various parameters to judge the scheme such as localization accuracy, time complexity, coverage and cost were also discussed. The limitations upon which future work can be carried out is summarized below:

- The proposed schemes consider two dimensional deployment region. Its effectiveness in three dimensional deployment plane must be assessed. It would provide a real world emulation scenario.
- The anchors and unknown sensor nodes were assumed to be static. A mobility situation can be modeled where either or both the anchor and unknown nodes are mobile.
- Most of the localization algorithms consider regular deployment region with Line of Sight (LoS) communication. In real world, sensors are often deployed in irregular terrains. Modelling such networks are very difficult and rife with computational inaccuracies. The existing works must be assessed against irregular deployment regions where topology is not square shaped but rather S and C shaped.
- Underground acoustics sensor networks are the future of sensor networks. These networks are more resource constrained than conventional wireless sensor networks. An efficient and accurate position determination system must be designed that offer cost effective solution with lower computational complexity.
- Future work can also be done to unify other issues such as Media access, energy conservation and dynamic routing into localization process to come up with one single solution that can be deployed on sensors.
- Predictive analytics techniques using machine learning and reinforcement learning with neural networks can be studied to model the sensor networks efficiently. Such solutions could come handy for underground sensor networks and networks with irregular deployment.

REFERENCES

[1] Kumar A., Saini B. (2018) A Sugeno-Mamdani Fuzzy System Based Soft Computing Approach Towards Sensor Node Localization with Optimization. In: Bhattacharyya P., Sastry H., Marriboyina V., Sharma R. (eds) Smart and Innovative Trends in Next Generation Computing Technologies. NGCT 2017. Communications in Computer and Information Science, vol 828. pp 40-55, Springer, Singapore.

[2] A. Kumar, N. Chand, V. Kumar, and V. Kumar, "Range Free Localization Schemes for Wireless Sensor Networks," Int. J. Comput. Networks Commun., vol. 3, no. 6, pp. 115–129, 2011.

[3] A. Kumar and V. Kumar, "Fuzzy Logic Based Improved Range Free Localization for Wireless Sensor Networks," vol. 177005, no. 5, pp. 534–542, 2013.

[4] M. A. Monfared, "Range Free Localization of Wireless Sensor Networks Based on Sugeno Fuzzy Inference," no. c, pp. 36–41, 2012.

[5] S. K. Gharghan, R. Nordin, and M. Ismail, "A wireless sensor network with soft computing localization techniques for track cycling applications," Sensors (Switzerland), vol. 16, no. 8, 2016.

[6] M. Kadkhoda, M. A. Totounchi, S. Member, M. H. Yaghmaee, and Z. Davarzani, "A Probabilistic Fuzzy Approach for Sensor Location Estimation in Wireless Sensor Networks," 2010.

[7] L. Mallu and R. Ezhilarasie, "Live migration of virtual machines in cloud environment: A survey," Indian J. Sci. Technol., vol. 8, no. July, pp. 326–332, 2015.

[8] B. Li, N. Wu, H. Wang, P. H. Tseng, and J. Kuang, "Gaussian message passing-based cooperative localization on factor graph in wireless networks," Signal Processing, vol. 111, no. April, pp. 1–12, 2015.

[9] H. Naseri and V. Koivunen, "A Bayesian algorithm for distributed network localization using distance and direction data," pp. 1–11.

[10] Tashnim Jabir Shovon Chowdhury, "A Distributed Cooperative Algorithm for Localization in Wireless Sensor Networks Using Gaussian Mixture Modeling," University of Toledo, 2016.

[11] Kumar A., Prashar D. (2018) A Novel Approach for Node Localization in Wireless Sensor Networks. In: Singh R., Choudhury S., Gehlot A. (eds) Intelligent Communication, Control and Devices. Advances in Intelligent Systems and Computing, vol 624. pp 419-428, Springer, Singapore

[12] X. Liu, R. Yang, and Q. Cui, "An Efficient Secure DV-Hop Localization for Wireless Sensor Network," System, vol. 9, no. 7, pp. 275–284, 2015.

[13] H. Chen, W. Lou, Z. Wang, J. Wu, Z. Wang, and A. Xi, "Securing DV-Hop localization against wormhole attacks in wireless sensor networks," Pervasive Mob. Comput., vol. 16, no. PA, pp. 22–35, 2015.

[14] W. Shi, M. Barbeau, J. P. Corriveau, J. Garcia-Alfaro, and M. Yao, "Secure localization in the presence of colluders in WSNs," Sensors (Switzerland), vol. 17, no. 8, 2017.

[15] P. Li, X. Yu, H. Xu, J. Qian, L. Dong, and H. Nie, "Research on secure localization model based on trust valuation in wireless sensor networks," Secur. Commun. Networks, vol. 2017, 2017.

[16] G. Kumar, M. K. Rai, H. J. Kim, and R. Saha, “A Secure Localization Approach Using Mutual Authentication and Insider Node Validation in Wireless Sensor Networks,” Mob. Inf. Syst., vol. 2017, 2017.

[17] L. Lazos and R. Poovendran, “SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks,” Netw. Secur., pp. 21–30, 2004.