International Journal of Engineering & Technology, 7 (2.33) (2018) 1025-1030

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Mobility Based Secure Localization in Underwater Wireless Sensor Networks

Ms. Shanthi M B[1] and DR. Dinesh K Anvekar[2]

[1]Department of CSE,CMRIT, Bengaluru, E-mail: shanthi.mb©cmrit.ac.in
[2]Director R & D/Product Innovation Cell, VVIT, Bengaluru
**Corresponding author E-mail: dinesh.anvekar@gmail.com*

Abstract

Currently, many applications require environmental sensing inside water bodies; Underwater Wireless Sensor Network (UWSN) is a new breed of sensor networks which achieve this sensing task. However, UWSN faces unique challenges due to signal problems associated with water medium. Most of the UWSN nodes have limited resources, and require Node Localization technique to identify their location. Many effective node localization techniques have been proposed in the literature. However, a new challenge has emerged related to security of the node localization technique; intruder or compromised sensor nodes provide incorrect localization information to the localization process, which may result in network disconnection. Currently, effective solution to address this problem in the literature is still lacking. In this work, a secure localization technique based on node mobility and probabilistic model is presented. This proposed localization technique, substantially outperforms the contemporary technique in-terms of security effectiveness when demonstrated empirically.
.

1. Introduction

1.1. Overview of UWSN

In multiple applications such as—military tasks, natural disaster warning, submarine exploration, ocean protection and monitoring; UWSN [1-6] has gained popularity. Since, UWSN operate inside the water medium; node communication is carried out through acoustic signals, which have lower bandwidth, large propagation delay and high error rate.

Figure 1 illustrates the network model of UWSN. There are three classes of UWSN nodes— surface buoys, beacon nodes and unknown nodes. The surface buoys float on the water surface, and are equipped with location trackers such as—GPS. Most of the sensing activity is performed by beacon and unknown nodes. The beacon nodes are more powerful than unknown nodes in-terms of energy reserves, computational ability, communication range and network resources. However, excessive monetary cost of these nodes prevents large scale deployment. Hence, the less expensive and resource weak unknown nodes are deployed in bulk. The beacon nodes have the ability to communicate with surface buoys, and estimate their location coordinates; the unknown nodes, usually, are unable to communicate with surface buoys, and depend on beacon nodes for their location coordinates estimation.

Node Localization is a technique by which the unknown nodes estimate their location coor-dinates by communicating with neighborhood beacon nodes. The first step for unknown node to perform localization is to communicate with the neighborhood beacon nodes. Each commu¬nicated beacon node estimates its distance from the unknown node, and transmits a message to the unknown node, which contains this estimated distance and the corresponding location coor-dinates of the beacon node. The unknown node after receiving location information from all the beacon nodes, estimates its corresponding location which best fits the obtained data. Currently, many effective localization solutions [7-9] based on meta-heuristic techniques such as—Particle Swarm Optimization (PSO), Binary PSO e.t.c. have been proposed in the literature.

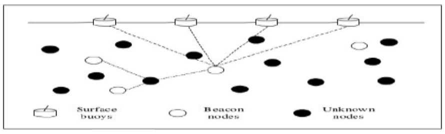

Fig. 1: UWSN Network Model

1.2 Motivation

Similar to many Wireless networks, security threats are also present in UWSN; especially in the node localization process; false localization information provided by the intruder nodes can be a major security threat. For example, a group of malicious beacon nodes might provide their corresponding locations which are much farther than the actual location coordinates; the estimated distances by these malicious nodes to the unknown node can be aligned with actual locations or some random values. Since, the unknown node estimates its corresponding location information which best fits the available data; due to false localization information, the estimated location coordinates might be far away from the actual position. This scenario can lead to network disconnection, because the unknown nodes might deem themselves as isolated; since, they have limited communication range. In the literature, effective solutions to counter this security threat are still elusive. The initial approach to address this security threat was presented in [10]; however, there is still significant scope to improve upon the presented solution; in-order to achieve better accuracy in isolating malicious nodes.

1.3 Paper Contributions

In this work, the following contributions are made:

1. To address the security threat in UWSN node localization process, a new technique to perform secure node localization is presented. This new technique, considers the node mobility due to tidal waves or other geographical factors for node localization; probabilistic framework is adopted to perform isolation of malicious nodes; the parameters of the probabilistic framework are estimated by generating the required training set.

2. The presented UWSN secure node isolation technique is implemented in MATLAB, and empirically compared against the contemporary technique [10]. The proposed security technique substantially outperforms the contemporary technique w.r.t. isolation accuracy of malicious nodes.

This paper is organized as follows: Section 2 describes the related work in this area. Section 3 presents the proposed UWSN secure node isolation technique. The empirical results and corresponding discussions are presented in Section 4. Finally, the work is concluded with future directions in the area in Section 5.

2. Related Work

The two main classifications of localization techniques for UWSN are—range-free and range-based techniques. The range-based technique [9] utilizes hardware components to estimate node distances. Metric such as—Time Difference of Arrival (TDOA), Received Signal Strength Indicator (RSSI) and Time of Arrival (TOA) are used in estimating the node distances. Even though, range-based techniques achieve better accuracy, the communication cost might be expensive. The range-free techniques [11] utilize multitude of optimization methods such as—Convex Pro¬gramming, DV-HOPS and Centroid localization algorithm to perform node localization. Even though, the cost of hardware is reduced, effectiveness suffers in-terms of localization accuracy. Range-based techniques have wider appeal; since, many UWSN applications perform critical functions. In this work, the presented UWSN secure node localization technique falls into range- based localization class.

There are myriad of localization techniques for UWSN presented in the literature. In [12], Monte Carlo based localization scheme, which was range free and took node mobility into consid¬eration was proposed. In [13], improvement over the scheme presented in [12] w.r.t. localization accuracy was presented.

In the literature, node localization technique for small size UWSN has been extensively ad-dressed. In [14], localization based on GPS enabled intelligent buoys, which are located on the surface, and having one hop communication scheme was presented. Even though, this technique achieves appreciable accuracy, the excessive cost of hardware prohibits wider appeal. The local-ization scheme presented in [15] does not depend on time synchronization; it can also be applied to one hop networks. Node mobility based localization scheme was proposed in [16], which has two stages; the first stage involves estimation of beacon node velocity, which is achieved through Durbin technique; the second stage performs localization based on the mobility statistics ob¬tained in the first stage.

In [17], the localization for UWSN was performed through dimensionality reduction on the location search space. The three dimensional search space was reduced to two dimensional space; this design was feasible due to the assumption that, pressure sensors are present in UWSN.

In [10], the initial work on secure node localization in UWSN was presented. The security scheme addressed false localization information threat. The location estimation was performed through Gradient Descent technique. Malicious nodes are identified during the Gradient Descent process using suitable thresholds. The usage of threshold without any prior analysis on the UWSN environment can lead to ineffectiveness in the localization process. It is important to design malicious node filtering mechanism based on the communication statistics between the different sensor nodes.

It is clear from the presented related work; limited attention has been provided to the problem of secure node localization in UWSN; there is still extensive scope to design an effective secure node localization technique for UWSN.

3. Secure Mobility Based Localization Technique for UWSN

3.1 Localization Model

Consider a node u, which can be surface buoy, beacon node or unknown node. Based on the kinematical model, the velocity of u in x direction and y direction are represented in Equations 1 and 2 respectively. Here, VV (u) and Vy (u) indicates the velocity of u in the x and y direction respectively, k1, k2, k3, A and v indicate associated values of different factors such as temperature, salinity and tides, and k5 and k4 are random variables. Since, the kinematical model is based on two dimensional representation of node position, projection of three dimensional location coordinates on two dimensional surface is performed; also, working with reduced dimensions aids in reducing computational effort, and energy conservation in unknown nodes.

$$V_x(u) = k_1\lambda v sin(k_2x)cos(k_3y) + k_1\lambda cos(2k_1t) + k_4 \tag{1}$$

$$V_y(u) = -\lambda v cos(k_2x)sin(k_3y) + k_5 \tag{2}$$

Consider the n^th unknown node indicated by u_n, which does not know its location coordinates, which needs to be identified through localization process. Let, there be m beacon nodes in the neighborhood of u_n, which are indicated by *(*$b_{n,}$, b_{n2}, ...$b_{n,n}$). Let, the most recent estimated location coordinates of b_{na} *(1 < j <* m) be indicated by the two dimensional coordinates (77,,, 9n,); this location coordinate estimation is performed through the aid of surface buoys. The current position of b_{na} is estimated as represented in Equation 3. Here, (x_{na} , y_{na}) indicates the current position of b_{na}, T_{na} indicates the time interval after the location coordinate of b_{na} was estimated through surface buoys and the current time, and Ti indicates the approximate lag-time for the unknown node to finish its localization process.

$$x_{n_j} = V_x(b_{n_j})(T_{n_j} + T_l) + \hat{x}_{n_j};\; y_{n_j} = V_y(b_{n_j})(T_{n_j} + T_l) + \hat{y}_{n_j} \tag{3}$$

Each b_{na} communicates its current position indicated by (x_{na} , y_{na}) and corresponding distance to u_n indicated by d_{na} *to un;* u_n estimates its corresponding location coordinates by minimizing the error function represented in Equation 4. Here, *error(*u_n*)* indicates the error function, *(x, y)* are the parameters which need to be estimated by minimizing the error function. This case is represented in Equation 5. Here, (Y_n, y_n) indicates the parameter values of *(x, y),* which satisfy the optimization condition represented in Equation 5. Finally, the estimated coordinates of u_n indicated by ($_n$*)* are obtained as represented in Equation 6.

$$error(u_n) = \sum_{j=1}^{m} |(\sqrt{(x - x_{n_j})^2 + (y - y_{n_j})^2} - d_{n_j})| \tag{4}$$

$$\text{optimization condition} = \arg\min_{(x,y)} error(u_n) \tag{5}$$

$$\hat{x}_n = V_x(u_n)T_l + \overline{x}_n;\; \hat{y}_n = V_y(u_n)T_l + \overline{y}_n \tag{6}$$

To achieve the optimization goal represented in Equation 5, PSO based optimization tech¬nique outlined in Algorithm 1 is utilized.

The required solution search space is created through Intialize_search_space(un); the search particles (ri, r2, ...rb) are initialized to arbitrary posi¬tions in the solution search space through Initialize_particles(SP, (ri, r2, ...rb)). Each particle is assigned an

$$I_n = \begin{cases} 1, & (b_{n_1}, b_{n_2}, \ldots b_{n_m}) \text{contains malicious node/nodes} \\ 0, & \textit{otherwise} \end{cases} \quad (8)$$

$$I_n = \begin{cases} 1, & \text{if } \Phi(\overrightarrow{b}_n | \mu, \sigma^2) < p_t \\ 0, & \text{if } \Phi(\overrightarrow{b}_n | \mu, \sigma^2) \geq p_t \end{cases} \quad (9)$$

exclusive zone in the solution search space; the union of all assigned particle zones will be equal to the search space.

Algorithm 1 PSO_localize(u$_n$,(b,,,,b$_{n2}$, ••••bn,n))

```
$SP = Initialize\_search\_space(u_n)$
$Initialize\_particles(SP, (r_1, r_2, \ldots r_b))$
$flag = 0$
while $flag == 0$ do
    for $i = 1$ to $b$ do
        $LS = local\_score(\overrightarrow{X}_i(t))$
        $\overrightarrow{x}_{pbest_i} = update\_local\_best\_score(LS)$
        $\overrightarrow{V}_i(t+1) = W\overrightarrow{V}_i(t) + C_1\gamma_1(\overrightarrow{x}_{pbest_i} - \overrightarrow{X}_i(t)) + C_2\gamma_2(\overrightarrow{x}_{gbest} - \overrightarrow{X}_i(t))$
        $\overrightarrow{X}_i(t+1) = \overrightarrow{X}_i(t) + \overrightarrow{V}_i(t+1)$
        $NS = local\_score(\overrightarrow{X}_i(t+1))$
        if $acceptable\_score(NS)$ then
            $flag = 1$
            break;
        end if
    end for
end while
Return $(\overline{x}_n, \overline{y}_n)$
```

The position of ri(1 < i < *b)* at time *t* in the solution search space is indicated by li(t). Each position is associated with the error function value/score represented in Equation 4. The score of the current position is calculated through *local_score(l$_i$(t)).* The overall best solution obtained until step *t* for ri is calculated through *update_local_best_score(LS)* and indicated by $_p$b$_{es}$t$_{\%}$. The next step velocity for ri is indicated by *V$_i$(t* + 1). Here, C2 and Ci indicate the degrees of particle attraction towards group and individual success respectively, W controls the impact of previous velocity on the current velocity of the particle, $_g$b$_{est}$ indicates the current global best solution discovered through all the particles, and -y1,72 E [0, 1] indicate the random factors.

The next position of ri is indicated by li(t + 1). The particle traversal continues until the error function value/score converges to the desired value; this convergence is calculated through *acceptable_score(NS);* the corresponding final solution (Y$_n$, y$_n$) is returned.

3.2 Security Model

The main goal of the security model is to isolate malicious nodes; however, the localization model is utilized to achieve this goal. The first step is to calculate *master distance* metric value for u$_n$ as represented in Equation 7. Here, *b* $_n$ indicates the master distance for u$_n$, which is the average of individual distance error for each *b$_{na}$.*

$$\overrightarrow{b}_n = \frac{\sum_{j=1}^{m} |(\sqrt{(\hat{x}_n - x_{n_j})^2 + (\hat{y}_n - y_{n_j})^2} - d_{n_j})|}{m} \quad (7)$$

If any malicious nodes are present in the beacon node set indicated by (bn,, bn2, ...bn,n), such nodes are detected by utilizing b n and the indicator random variable indicated by In, and defined for uri, which is represented in Equations 8 and 9. Here, pt indicates a threshold; the setting mechanism of the threshold value will be outlined in the subsequent section, along with the estimation techniques for the distribution parameters and cr2.

3.3 Estimation of Distribution Parameters

In-order to estimate the distribution parameters and cr^2, suitable training set has to be generated. *Training set case* refers to a simulation case in which, a specific unknown node is subjected to localization procedure by using a set of non-malicious nodes. Each case is associated with the corresponding generated master distance value. In the simulation exercise carried in this work, totally m$_u$ = 50 unknown nodes were utilized; each unknown node had m$_e$ = 20 different cases associated with it. In each case for a specific unknown node, the number of beacon nodes and their corresponding positions were varied. Each case had varying number of beacon nodes between 3 to 15.

Let, the master distance value calculated for the nth(1 < n < m$_u$) unknown node belonging to the *kth* training set case be indicated as *b* $_n$j. Based on the parameter estimation principle of Gaussian distribution, and cr^2 are estimated as represented in Equations 10 and 11

3.4 Algorithm

Algorithm 2 outlines the proposed mobility based secure localization technique for UWSN; the corresponding flow diagram is illustrated in Figure 2. The unknown node *u$_n$*, estimates its location coordinates by using the neighborhood beacon node set indicated by *U* through *PS0Joca/ize(u$_n$, U).* The master distance value for *U* is calculated through the function *master_distance(U,* 9$_n$)). If the group of beacon nodes qualifies as non-malicious based on the proposed security model, all the beacon nodes are returned as non-malicious; otherwise, if some nodes in the group are malicious, then, such malicious nodes have to be isolated.

$$\mu \approx \frac{\sum_{i=1}^{m_u} \sum_{j=1}^{m_c} \overrightarrow{b}_{ij}}{m_c m_u} \quad (10)$$

$$\sigma^2 \approx \frac{\sum_{i=1}^{m_u} \sum_{j=1}^{m_c} (\overrightarrow{b}_{ij} - \mu)^2}{m_c m_u - 1} \quad (11)$$

The isolation process of malicious nodes from the set of beacon nodes indicated by *G* = *U* involves analyzing all the possible subsets of *G.* To perform this sub-set analysis, *comp_node(G, i)* which generates a unique selection of i nodes from *G* is utilized; for each call a unique node set selection which was not seen before is produced. Also, if I GI < i then, *comb_node(G, i)* returns *NULL.* The sub-sets of *G* having cardinality between 2 to m — 1 are considered for analysis. The generated sub-sets are subjected to security check by using the proposed security model. If a particular sub-set qualifies as non-malicious, the union of such qualified sets is performed to identify the final set of non-malicious nodes.

Theorems 3.1, 3.2, 3.3 and 3.4 collectively state that, Algorithm 2 is effective in isolating malicious nodes with high probability.

```
$U = (b_{n_1}, b_{n_2} \ldots b_{n_m})$
$(\hat{x}_n, \hat{y}_n) = PSO\_localize(u_n, U)$
$\overrightarrow{b}_n = master\_distance(U, (\hat{x}_n, \hat{y}_n)$
Set $p_t \leq \mu$ and $p_t \approx \mu$
$f(\overrightarrow{b}_n) = \Phi(\overrightarrow{b_n} | \mu, \sigma^2)$
if $f(\overrightarrow{b}_n) \geq p_t$ then
    Return $U$
end if
$F = \phi$
$G = U$
for $i = m - 1$ to 2 do
    while $comb\_node(G, i) \neq \phi$ do
        $M = comb\_node(G, i)$
        $(\hat{x}_n, \hat{y}_n) = PSO\_localize(u_n, M)$
        $\overrightarrow{b}_n = master\_distance(M, (\hat{x}_n, \hat{y}_n))$
        $f(\overrightarrow{b}_n) = \Phi(\overrightarrow{b_n} | \mu, \sigma^2)$
        if $f(\overrightarrow{b}_n) \geq p_t$ then
            $F = F \cup M$
            $G = G - F$
        end if
    end while
end for
Return F
```

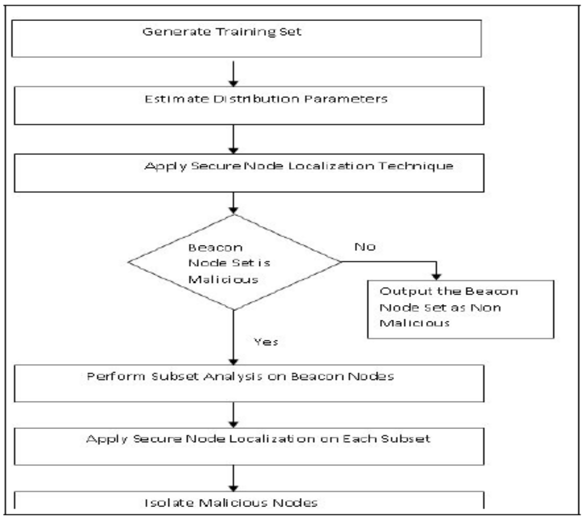
Generate Training Set
Estimate Distribution Parameters
Apply Secure Node Localization Technique
Beacon Node Set is Malicious
No
Output the Beacon Node Set as Non Malicious
Yes
Perform Subset Analysis on Beacon Nodes
Apply Secure Node Localization on Each Subset
Isolate Malicious Nodes

Fig. 2: Algorithm Flow Diagram

Algorithm 2

Secure Localization Technique(u_n)

Theorem 3.1. Let, $p_t=\Phi(\mu/\mu, \sigma^2)$ and $p_t<\Phi(\mu/\mu, \sigma^2)$; then, pt is associated with high value.

Theorem 3.2. Let, G be a group of neighbourhood non-malicious beacon nodes. If, some of the nodes in G are compromised into malicious; this new set is indicated as G. The master distance value of G will be lesser than the master distance value of G.

Theorem 3.3. *Algorithm Correctness*

Let, $p_t<\Phi(\mu/\mu, \sigma^2)$ and $p_t=\Phi(\mu/\mu, \sigma^2)$; then, the chances of isolating malicious nodes is high.

Theorem 3.4. Algorithm Correctness

Let, $p_t<\Phi(\mu/\mu, \sigma^2)$ and $p_t=\Phi(\mu/\mu, \sigma^2)$); then, the chances of isolating non-malicious nodes as malicious is low.

4. Results and Discussions

4.1 Simulation Setup

The proposed mobility based secure node localization technique for UWSN is simulated using MATLAB. The utilized parameter values for simulation are outlined in Table 1. For the ease of reference, the proposed mobility based secure node localization technique for UWSN will be indicated as new local, which is compared against the contemporary technique [10], which will be referred as old local. The performance of new local and old local are analyzed through two metrics{LT N(un) and LF P(un); here, the first metric is related to True Negative analysis, and it is represented in Equation 12; LT N(un) represents the proportion of malicious beacon nodes which have been accurately identified as malicious by the localization technique w.r.t. unknown node un, actual malicious(un) indicates the actual malicious node set of un, and identified malicious(un) indicates the identified malicious nodes by the utilizing localization technique, which are actually malicious.

The second metric is represented in Equation 13, which is related to False Positive analysis. Here, LF P(un) indicates the proportion of non-malicious nodes which have been identified as malicious by the utilized node localization technique w.r.t. un, actual valid(un) indicates the actual non-malicious nodes, and identified_valid(un) indicates the identified non-malicious nodes by the utilized node localization technique, which are actually non-malicious.

From the definition of LF P and LT N, clearly, 0 LF P; LT N 1; higher the values of LF P and LT N, greater will be the effectiveness of the utilized node localization technique. Since, communication systems inside the water environment face signal attenuation; Gaussian attenuation, whose variance is proportional to the distance between un and the beacon node nj is added to dnj .

4.2 Empirical Results and Discussions

Two experiments are performed to analyze the performance of new local and old local. The first experiment varies the number of beacon nodes; the result of this analysis w.r.t. LT N(un), LF P(un) and execution time is presented in Figures 3, 4 and 5 respectively. The new local performs exceedingly better than old local w.r.t. effectiveness parameters LT N(un) and LF P(un)
mainly due to assiduous design presented for new local. The performance of new local decreases as the computational load increases, which is mainly due to compounded effect of signal attenuation. In-case of execution time, old local performs better than new local, because of combinatorial execution complexity of new local; however, this increase in execution time is not substantial; the large effectiveness advantage seen for new local offsets this limitation.
The minimum distance between the beacon node and un is varied in the second experiment; the number of beacon and malicious nodes are fixed. The analysis result w.r.t. LT N(un), LF P(un) and execution time is presented in Figures 6, 7 and 8 respectively. The new local outperforms old local w.r.t. LT N and LF P, and slightly underperforms w.r.t. execution time for the same reasons explained above. The performance of new local decreases with the increase in the minimum distance between beacon node and un due to the compounded effect of signal attenuation. The execution time of new local does not show large variance mainly due to the fixed computational load.

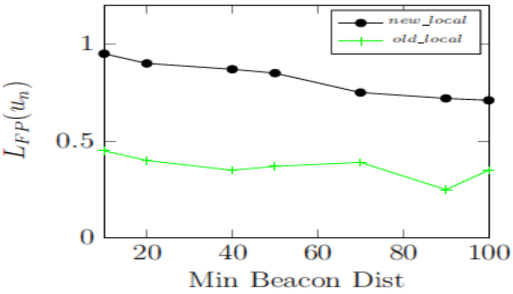

Fig. 3: No of Beacon nodes vs LT N(un)

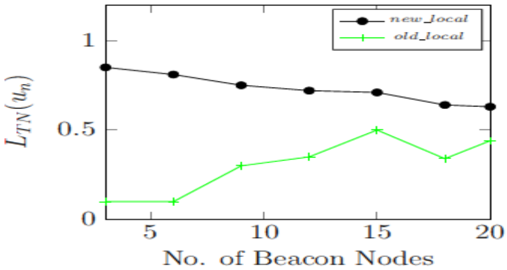

Fig. 4: No of Beacon Nodes vs LF P(un)

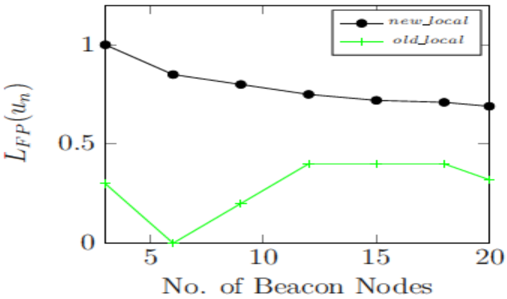

Fig. 5: No of Beacon nodes vs Exe Time

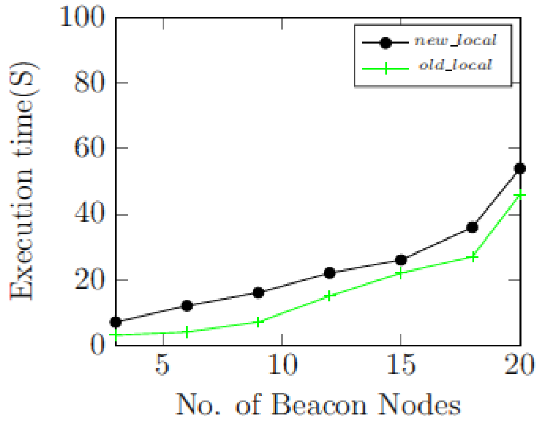

Fig. 6: Min Beacon Dist vs LT N(un)

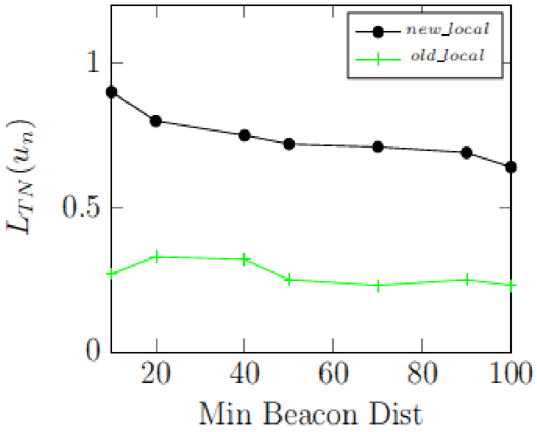

Fig. 7: Min Beacon Dist vs LF P(un)

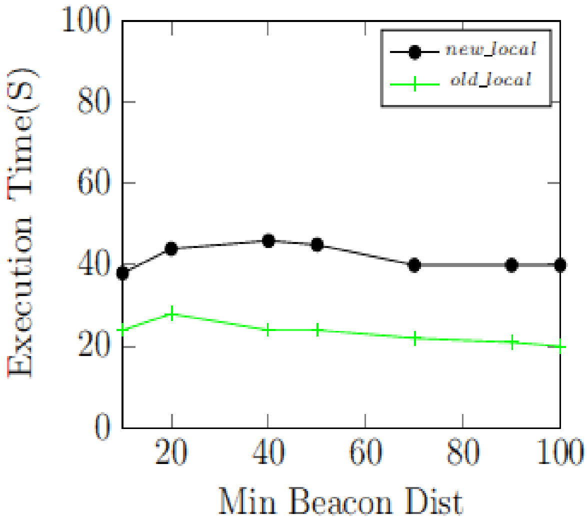

Fig 8: Min Beacon Dist vs Exe Time

5. Conclusion

In this work, mobility based secure node localization technique for UWSN was presented; this technique was designed through probabilistic scheme; its performance guarantees based on theoretical analysis was presented; empirical evaluation exhibited the considerable security effectiveness of the proposed technique over the contemporary technique. In future, the presented security design can be evaluated and suitably modified for different underwater environments; also, energy optimal and effective secure localization techniques need to be investigated, in-order to prolong the node lifetime.

References

[1] Heidemann, J.Stojanovic, M.Zorsi, M Underwater sensor networks: applications,advances and challenges Phillos. Trans. R. Soc. AMath. Phys. Eng. Sci.2012, 370,158-175.

[2] Javid, NJafri, M.R Khan, Z.A Alrajeh, N Imran, M.Vasilakos A Chain based communication in cylindrical underwater wireless sensor networks sensors 2015, 15, 3625-3649.

[3] Climent, S.Sanchez, A.Capella, J.V Meranthia, N.Serrano, Underwater acoustic wireless sensor networks: advances and future trends in phusical, MAC and routing layers. Sensors 2014, 14, 795-833.

[4] Liu, Z.Gao, H.Wang, W.Chang, S. Chen color ltering localization for three-dimensional underwater acoustic sensor networks. Sensors 2015, 15,6009-6032.

[5] Beniwal, M.Singh, localization techniques and their challenges in underwater wireless sensor networks. Int. j.Comput. Sci. inf. Technol. 2014,5,4706-4710.

[6] Ying Zhang, Jixing Liang, Shengming Jiang, Wei Chen A Localization Method for Underwater Wireless Sensor Networks Based on Mobiliity prediction and particle Swan optimization Algorithms in Sensors, 2016.

[7] Krishna C.R, Yadav P.S A hybrid localization scheme for underwater wirelesssensornetworks In proceedings of the IEEE 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Ghazibad, India, 7-8 February 2014, pp.579-582.

[8] Erol-Kantarci M. Mouftah HT, Oktug S A survey of architectures and localization techniques for underwater acoustic sensor networks. IEEE Commun. Surv. Tutor.2011, 13, 487-502.

[9] A1Hajri M.I, Goian A, Darweesh M, AlMemari R, Shubair R.M, Weruga L,Kulaib A.R, Hybrid RSS-DOA technique for enhanced WSN localization in a correlated environment, In Proceedings of the 2015 IEEE International Conference on Information and Communication Technology Research(ICTRC), Abu Dhabi, United Arab Emirates, 17-19 May 2015, pp238- 241.

[10] Zahra Ansari, Reza Ghazizadeh, Zahra Shokhmzan Gradient Descent Approach to Secure Localization for Underwater wireless Sensor Networks In Iranian Conference on Electrical Engineering, 2016.

[11] E1 Assaf A, Zaidi S.A.R, A es S, Kandil N Range-free localization algorithm for heterogeneous wireless sensor networks. In proceedings of the 2014 IEEE Wireless Communications and Networking Conference(WCNC), Istanbul,Turkey, 69 April 2014,pp.2805-2810.

[12] Hu L, Evans D Localization for mobile sensor network In proceedings of the ACM 10th annual International conference on Mobile computing and networking, Philadelphia, PA, USA, 26 september-1 October 2004, pp-45-57.

[13] Soltaninasab B, Sabaei M,Amiri J,Improving Monte Carlo localization algorithm using time series forecasting method and dynamic sampling in mobile WSNs. In proceedings of the 2010 Second International Conference on Communication Systems, Networks and Applications, Hong Kong, China, 29 June-1 July2010, pp 389-396.

[14] Alcocer A, Oliveira P, Pascoal AStudy and Implementation of an EKF GIB-based underwater positioning system Control Eng. Pract 2007, 15,689-701.

[15] Cheng X, Shu H, Liang Q, Du D.H.C Silent Positioning in underwater acoustic sensor networks. IEEE Trans. Veh.Technol.2008, 57,1756-1766.

[16] Zhou Z, Peng Z, Cui J.H, Shi Z Bagtzoglou AC Scalable localization with mobility predictionfor underwater sensor networks. IEEE Trans. Mob Comput.2011, 10,335-348.

[17] Cheng W,Teymorian A.Y, Ma L, Cheng X, Lu X, Lu Z Underwater Localization in sparse 3D acoustic sensor networks. In proceedings of the 27th IEEE Conference on Computer Communications INFOCOM, Phoenix, AZ USA, 13-18 April 2008, pp 236-240.

Appendix a proofs of theorems

Proof of Theorem 3.1

Proof. Here, indicates the mean of Gaussian distribution; the values around have high probability; so, the theorem immediately follows.

Proof of Theorem 3.2

Proof. Let, G = (bn1 ; bn2 ; ::::bnm) indicate the non-malicious neighbor beacon nodes of un, x indicate the master distance value for G; suppose, r < m beacon nodes are compromised into malicious nodes to create a new group indicated byG, with y indicating the new master distance value for G.
The metric indicates the estimated distance by the unknown node un, from it to bnj (1 j m); indicate this value as ^dnj . Let, .! dnj = j^ dnj .dnj j, it is clear from Equation 7; if the variance of .! dnj is high, .! bn will have larger value; this scenario is seen in a group of beacon nodes which contain malicious nodes; for example, G. Similarly, if the variance of .! dnj is lesser, .! bn will have lesser value; this scenario is seen in a group of beacon nodes which are all non-malicious; for example, G; hence, x < y.

Proof of Theorem 3.3

Proof. It is clear from the proof of Theorem 3.3, x with high probability, because of the property of Gaussian distribution, and is estimated from the training set cases which only involve non-malicious nodes; by using Theorem 3.3, security model included in Algorithm 2 will most likely isolate the malicious nodes.

Proof of Theorem 3.4

Proof. Here, by using the proofs of Theorem 3.2 and 3.3, it can be concluded that, x with high probability; by the security model presented in Algorithm 2, and the result of Theorem 3.1, the theorem immediately follows.