DOI: 10.21917/ijct.2018.0252

SECURE LOCALIZATION USING COORDINATED GRADIENT DESCENT TECHNIQUE FOR UNDERWATER WIRELESS SENSOR NETWORKS

Baranidharan. V[1] and Kiruthiga Varadharajan[2]

[1]*Department of Electronics and Communication Engineering, Bannari Amman Institute of Technology, India*

[2]*Department of Computer Applications, Annamalai University, India*

Abstract

In the Underwater Wireless Sensor Networks (UWSN) provide a solution for several aquatic and oceanographic applications. All these UWSN applications are need to be aware of the nodes positioning. In some insecure environment, the misleading data can be transmitted to the sonobuoys or monitoring systems in the network. This may disrupt the functions of the nodes. Thus, the secured localization algorithms are designed to resistant against attack and try to achieve the localization correctly. This paper shows that modified secure localization algorithm based Gradient Descent Algorithm (GDA) to remove the misleading information in the networks. This modified algorithms the normal nodes are cooperate with each other to reduce the localization error and to improve the pruning percentage.

Keywords:

Underwater Wireless Sensor Networks, Secure Localization Algorithms, Gradient Descent Approach, Pruning Percentage

1. INTRODUCTION

Over the past few years, there is a rapid development in underwater wireless sensor networks. This UWSN are having a wide range of applications including collection of data in oceanographic regions, assisted navigation, and disaster prevention and so on. In all the above UWSN applications, the secure communication among the sensor nodes is very important challenging task [1].

For an example, reporting an event, tracking a tactile (moving object) or monitoring the oceanographic environmental physical conditions are some of the types of UWSN applications that all the position and coordinates of the referred architecture phenomena is more important. To identifying the nodes position, the localization schemes [4] are developed (i.e. they are relying on a set of anchor nodes) the anchor nodes are called as reference nodes to known the location information. The nodes locations could be calculated by the position of the reference nodes and the distance between the reference and normal nodes are also calculated. In some scenarios, some reference node may be compromised by the adversary. These nodes are transmitted false the information's to prevent accurate localization of the remaining normal nodes. Thus, the localization problem affects the entire networks proper function.

To overcome these problems, some efficient resistant methods (node deployment schemes) have been introduced. Gradient Descent Secure Localization (GDSL) [2], Least Mean Square (LMS) [4], and Voting Based Scheme (VBS) [5] are the some of the important secured localization methods from location accuracy point of view. The localization error of these methods is almost same but the complexity of GDSL is comparatively less than the other methods. So its results are very less consumption of energy [8] [9]. In [11], the authors proposed an enhanced range free localization algorithm for wireless sensor networks. This algorithm uses two important methods such as hop size and weighted correction and Localization estimation method. In this hop size and weighted correction, is used in each anchor computes its hop size and calculate the distance between itself with other anchor nodes. The secured algorithm is as localization estimation method is used to calculate the position of the unknown nodes. In [12], the author surveyed on software fault localization. This algorithm is classified into four important groups namely, slice band localization, spectral based localization, statistic based localization and model based localization. This algorithm is mainly focus on the improvements of algorithm using SFL techniques.

This paper gives a novel secure localization algorithm based GDA of UWSN. So that it improves the network lifetime. The nodes consume very low energy. The network lifetime of the nodes will be increased.

This paper organized as follows, in section 2 UWSN architecture is discussed. GDS Localization techniques are explained in section 3. The section 4 gives simulated results and its discussion. The paper is concluded in section 5.

2. UWSN ARCHITECTURE

These acoustic communications are very low frequency signals (30-300Hz). These radio frequency waves are not propagating over a long distance. The acoustic channel impairments are very limited channel bandwidth, high propagation delay, very high attenuation loss and fading. The main difference between the terrestrial and underwater sensor networks are,

- *Cost*: The terrestrial sensor nodes are expected to become expensive increasingly. But, the underwater sensor nodes are very expensive devices.
- *Deployment*: The terrestrial sensor networks are densely deployed but the deployment in underwater scenario is sparser.
- *Power*: Due to very low frequency signal, long distance data transmission having complex signal processing techniques. The power needed by the acoustic underwater communication is always higher than the terrestrial WSN.
- *Memory*: The terrestrial sensors are having very limited storage capacity but the underwater sensors are having able to catching some data as underwater channel is intermittent.
- *Spatial Correlation*: The underwater sensors are not often correlated like terrestrial networks.

There are some communication architectures of underwater sensor networks. This shows the various challenges associated in underwater scenarios.

2.1 2D UNDERWATER WIRELESS SENSOR NETWORKS

The reference architecture of 2D networks are shown in the Fig.1. The sensor nodes are anchored at ocean bottom surface. There is an interconnection between sensor nodes by using underwater gateways. These gateways are in the charge of data relaying by the means of wireless acoustic links. This architecture is having a vertical and horizontal transceiver.

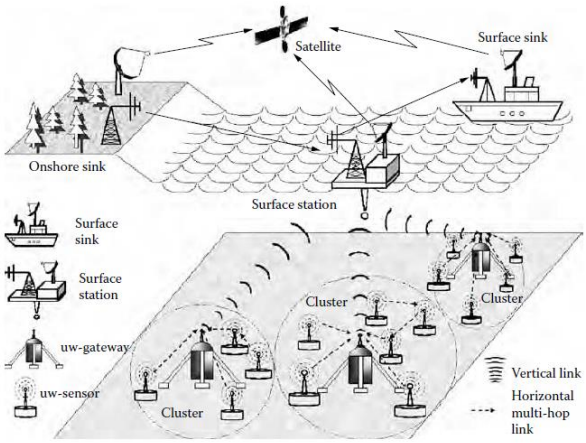

Fig.1. 2D underwater wireless sensor networks

The horizontal transceivers are responsible for the communication between sensor nodes in order to

- To sends command data and to configure the data to sensors.
- To collect the monitored data.

In a very deep water application, long range transceivers are used. The surface station is equipped with acoustic and RF transceivers to communicate with underwater nodes and to monitoring the systems through RF links.

2.2 3D UNDERWATER WIRELESS SENSOR NETWORKS

The 2D UWSN architecture is endowed with RF long ranges and satellite transmitters are used with underwater gateways. But in 3D underwater sensor networks are used to detect the phenomena in underwater rapidly. i.e., to perform a cooperative sampling of underwater environment. In a 3D underwater wireless sensor networks, the nodes are floated at different depths.

In this architecture, the each and every node are anchored at the bottom of the ocean and equipped with son buoys which are floated over the ocean surface. The sensor depth can be regulated by adjusting the wire length from the anchors. The length is to be adjusted by the electronically controlled engines. The number of sensor nodes need to be deployed to achieve optimum sensing and communication coverage is to be very less compared with 2D underwater wireless sensor networks.

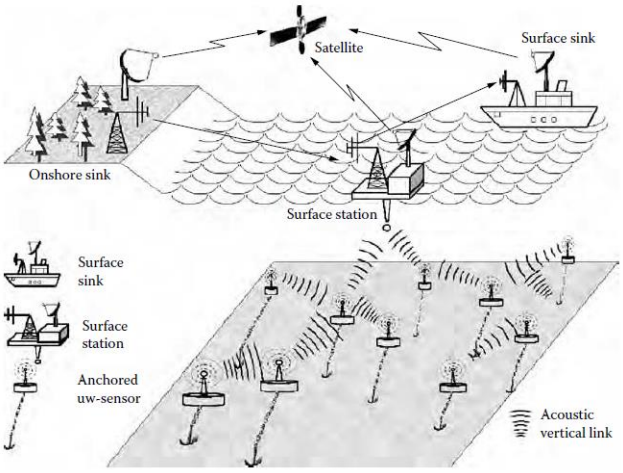

Fig.2. 3D underwater wireless sensor networks

2.3 AUTONOMOUS UNDERWATER VEHICLES

The AUV can function without use of any wires, cables, or monitor control. So, this UAV are having various applications in many areas such as ocean monitoring, environment monitoring, and to study about the underwater scenario. But the AUV are very expensive in submarines, because they are equipped with multiple underwater sensors.

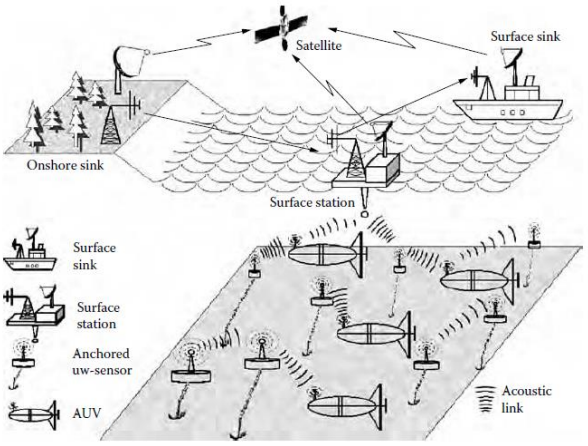

Fig.3. Autonomous underwater vehicles

The integration of AUV with Underwater wireless sensor networks needs some novel network coordination algorithms such as,

- *Self-Configuration*: This algorithm includes a control procedure to detect the connectivity between the nodes at the time of some nodes become fails.
- *Adaptive sampling*: This algorithm has control strategies to command the mobile nodes or *son buoys* to forward the data and to know its location of sensor nodes and surface son buoys.

The AUV are to be making them to rely on local intelligence and less dependent on communication. So, the control strategies are to be needed to coordinator between the AUV's, obstacle avoidance, void node avoidance etc.

3. MODIFIED GDM APPROACH

Consider the architecture of the UWSN, let N be the total number of anchor nodes. The k^{th} node sends the information to localizing node $P_k = [X_k\ Y_k]^T$ which is the correct position of the k^{th} anchor node. Consider the additive independent Gaussian noise model $N(0,\Omega^2)$ the distance can be estimated by using a received signal strength, angle of arrival and Time of arrival. In some advertise environment, some nodes leads to an incorrect localization. The type of attacks is classified into the coordinated attacks and Non-Coordinated attacks [5].

- ***Non Coordinated attacks***: The nodes are compromised independent by changing the distance to prevent localizing nodes from its accurate positioning. This scenario can be modeled by a zero mean uniform random variable to actual distance from the localization of the nodes.
- ***Coordinated attacks***: This coordinated attacks are the stronger attacks that against the launched by compromised nodes to acting together to make a localization of the normal nodes. The estimated position of all of the normal nodes as (x_{mal}, y_{mal}), where the x_{mal}, y_{mal} is an arbitrary points determined by the attackers.

The difference between the actual position of the malicious nodes are characterized via the strength of coordinated attack is given by,

$$d_x = \sqrt{\left(X_{mal} - X_t\right)^2 + \left(Y_{mal} - Y_t\right)^2} \tag{1}$$

If there is no malicious attack then the unknown position of the nodes is estimated by the ML (Maximum Likelihood estimation)

$$P_k = \frac{d_k^2}{dist_k} \tag{2}$$

The correct position of the maximized probability is,

$$P_{ml(k)} = argmax \times P_r\left(\{d_k\} P\right), \{\|P_k\|\} \tag{3}$$

where, P_r is random probability, P_k is the k^{th} probability of ML function.

An iterative GDA is to be introduced to find the estimated position. For ith iteration, the estimated position is given as,

$$P(i) = P(i\text{-}1) + \delta(i)\, X \frac{g(i)}{\|g(i)\|} \tag{4}$$

where, $\delta(i)$ is a step size, $g_k(i)$ is a force factor and $\|g(i)\|$ is get smaller than the predefined threshold. The large force vector of the malicious node is to be eliminated. This process is called as pruning stage.

The existing GDM approach the node calculates its position based on the received information. The localization error is more because it compares only the few received information from the normal node. To overcome these issues, the cooperative GDM localization method is proposed. The each node broadcast its localization information from the anchor nodes and these information are to be broadcasted it all to the other neighbours within the communication region. These broadcast information consist of a sequence id number and x, y, z position coordinates respectively.

The broadcast information is to be received by all the other neighbour nodes it calculates its distance based on the general GDM approach. So, this will provide the more information so its reduces the localization error. The noise is a zero mean additive Gaussian noise with different variance for the each transmitted and received noise level is determined by,

$$Noise = \frac{20rR}{d_{\max}} \tag{5}$$

where, d is the distance between the transmitter and receiver and d_{max} is the maximum transmission range.

To calculate the distance between the normal node and the anchored nodes, the Lambert function is to be $W(s)$ is,

$$\text{Distance} = \frac{20000W\left[\frac{\alpha \ln(10) e^{\frac{\ln 10}{20} TL}}{20000}\right]}{\alpha \ln(10)} \tag{6}$$

where, α is the absorption coefficient and T_L is the Transmission loss.

4. SIMULATED RESULTS

The underwater wireless sensor networks model was simulated using the Aquasim software tool. This software is created to simulate packet collision and the acoustic signal attenuation scenario in underwater environment. The networks included an anchor nodes and normal nodes. The nodes are scattered randomly over the entire region of 1000m × 1000m deployed region. Assumed that the nodes are placed under the depth of 500m.

Consider that among the 60 nodes, 20 nodes are anchor anodes and remaining 40 nodes are normal nodes. Under the Non – coordinated attack scenario, the anchor nodes are affected by the attack and act as malicious nodes, add a disturbance within the uniform distribution with zero mean and the variance at the noisy distance. If the attack is coordinated scenario based, then for each and every ordinary node, the hypothetical position are calculated and the malicious nodes are reported based on their position with ordinary nodes.

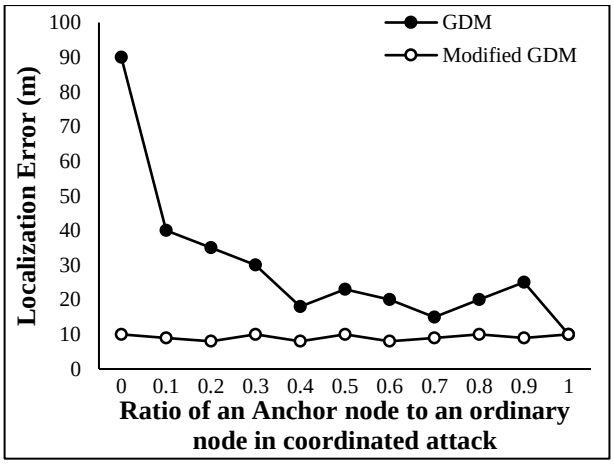

Fig.4. Localization error in terms of Ratio of anchor nodes to ordinary nodes in coordinated attacks

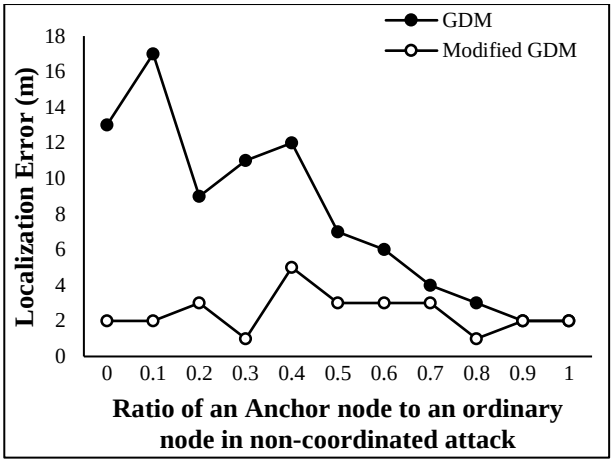

Fig.5. Localization error in terms of Ratio of anchor nodes to ordinary nodes in non-coordinated attacks

The Fig.4 and Fig.5 shows the position error decreases by increasing the number of anchor nodes. In this proposed underwater environment model, the positioning error is reduced by without adding any anchor node in the network by increasing the cooperative nodes to node localization.

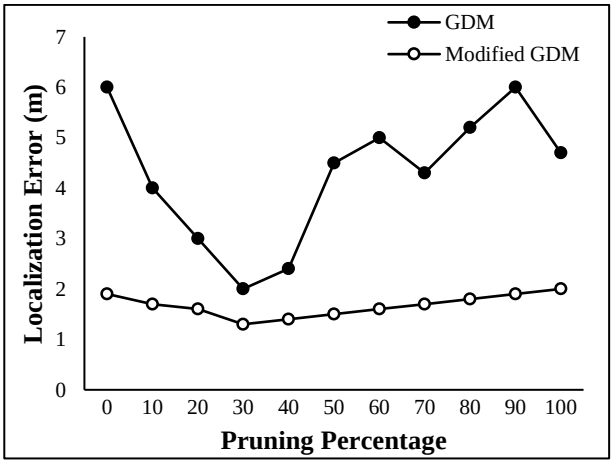

Fig.6. Localization error versus pruning percentage for Non-coordinated attack

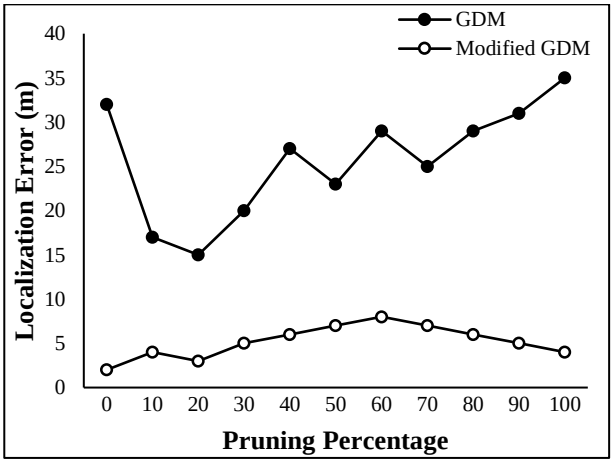

Fig.7. Localization error versus pruning percentage for coordinated attack

From the above Fig.6 and Fig.7 the error in positioning is to be calculated in terms of pruning percentage. The simulation parameters and results are listed out in the Table.1.

Table.1. Simulated results of Modified GDM

Parameters	GDM Approach	Modified GDM
Number of Anchor nodes	20	20
Number of Ordinary nodes	40	40
Packet Sent (packets)	1246	1250
Packets Received (packets)	898	912
Packet Deleviery ratio	72.07	84.48
End to end delay (ms)	12.465ms	11.925ms

The error in the proposed GDM approach is always less than the existing algorithm because the more number of nodes are act as an anchor nodes to node localization. In this proposed model, as the pruning percentages increases the node is removed. At the same time the remaining nodes that can cooperative to positioning increases and the localization error are also reduces.

5. CONCLUSION

This paper concludes that the secured cooperative localization scheme is based on the Gradient Descent algorithm with a selective pruning approach to remove the incorrect node information from the underwater sensor networks. To reduce the localization error, the cooperative model is helps the normal nodes to improve localization. The simulated results are shows the effectiveness of the proposed method.

REFERENCES

[1] Vikash Mainanwal, Mansi Gupta and Shravan Kumar Upadhayay, "A Survey on Wireless Network: Security Technology and its Design Methodology Issues", *Proceedings of International Conference on Innovations in Information, Embedded and Communication Systems*, pp. 1-5, 2015.

[2] Movassaghi Shamaneh, Mehran Abolhasan, Justin Lipman, David Smith and Abbas Jamalipour, "Wireless Body Area Networks: A Survey", *IEEE Communication Survey*, Vol. 16, No. 3, pp. 1658-1686, 2014.

[3] M. Hosseini, H. Chizari, T. Poston, M.B. Salleh and A.H. Abdullah, "Efficient Underwater RSS Value to Distance Inversion using the Lambert Function", *Mathematical Problems in Engineering*, Vol. 2014, pp. 1-8, 2014.

[4] S. Misra et al., "Jamming in Underwater Sensor Networks: Detection and Mitigation", *IET Communications*, Vol. 6, No. 14, pp. 2178-2188, 2012.

[5] H. Kulhandjian, T. Melodia, and D. Koutsonikolas, "Securing Underwater Acoustic Communications through Analog Network Coding", *Proceedings of Annual 7th IEEE International Conference on Sensing, Communication, and Networking*, pp. 1-9, 2014

[6] R. Garg, A.L. Varna and M. Wu, "Gradient Descent Approach for Secure Localization in Resource Constrained wireless Sensor Networks", *Proceedings of International*

Conference on Acoustics, Speech, and Signal Processing, pp. 1854-1857, 2010.

[7] M. Mofarreh-Bonab and S.A. Ghorashi, "A Low Complexity and High Speed Gradient Descent Based Secure Localization in Wireless Sensor Networks", *Proceedings of 3rd International Conference on Computer and Knowledge Engineering*, pp. 300-303, 2013.

[8] R. Garg, A.L. Varna and M. Wu, "An Efficient Gradient Descent Approach to Secure Localization in Resource Constrained Wireless Sensor Networks", *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 2, pp. 717-730, 2012.

[9] M. Mofarreh-Bonab and S.A. Ghorashi, "The Effect of Pruning Stage in Secure Localization in Wireless Sensor Networks", *Proceedings of 6th International Symposium on Telecommunications*, pp. 455-458, 2012.

[10] V. Obado, M. Hosseini, K. Djouani and G. Noel, "Underwater Wireless Sensor Network Localization for Wormhole Attack Detection", *Proceedings of International Conference on Southern Africa Telecommunications Networks and Applications*, pp. 57-63, 2011.

[11] A. El Assaf, S. Zaidi, S. Affes and N. Kandil, "Low-Cost Localization for Multi-hop Heterogeneous Wireless Sensor Networks", *IEEE Transactions on Wireless Communications*, Vol. 15, No. 1, pp. 472-484, 2016.

[12] A. El Assaf, S. Zaidi, S. Affes and N. Kandil, "Robust ANNs based WSN Localization in the Presence of Anisotropic Signal Attenuation", *IEEE Wireless Communications Letters*, Vol. 5, No. 5, pp. 504-507, 2016.