ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

AN ENHANCED COLLABORATIVE SECURE LOCALIZATION ALGORITHM BASED ON TRUST MODEL IN UNDERWATER WIRELESS SENSOR NETWORKS

NAZIA PARVIN NAZAR ALI
No 8, Mariyaprakasam Street,
Jothi Nagar, Attur, Salem Dt, 636102
Tamil Nadu, India
nazpar22@gmail.com

Priyanka(AP/CSE)
Maha Bharathi Engineering
College

D.Amudha Pandian
Maha Bharathi Engineering
college

Abstract **- Localization is one of the hottest research topics in Underwater Wireless Sensor Networks (UWSNs), since many important applications of UWSNs, e.g., event sensing, target tracking and monitoring, require location information of sensor nodes. Nowadays, a large number of localization algorithms have been proposed for UWSNs. How to improve location accuracy are well studied. However, few of them take location reliability or security into consideration. In this paper, we propose a Collaborative Secure Localization algorithm based on Trust model (CSLT) for UWSNs to ensure location security. Based on the trust model, the secure localization process can be divided into the following five sub-processes: trust evaluation of anchor nodes, initial localization of unknown nodes, trust evaluation of reference nodes, selection of reference node, and secondary localization of unknown node. Simulation results demonstrate that the proposed CSLT algorithm performs better than the compared related works in terms of location security, average localization accuracy and localization ratio.**

Keywords**–Underwater Wireless Sensor Network (UWSN), Trust evaluation, Collaborative localization.**

I. INTRODUCTION

Underwater Wireless Sensor Networks (UWSNs) have gained researchers' much attention in the past few years due to their great potential utility in many applications, such as ocean resource exploration, marine environment monitoring, ocean target surveillance, submarine tracking and disaster prevention. In these applications, sensor node's accurate and reliable locations are required. In addition, some network system functions, e.g., network topology management and design of network communication protocols, also need sensor nodes' location information to achieve. Thus, the secure localization problem becomes one of the most important and fundamental issues in UWSNs. Many localization algorithms have been proposed for UWSNs. However, few of them take location reliability or security into consideration, while UWSNs are always deployed in unattended and even hostile environment. Ensuring node safety is a basic and essential knowledge to improve node location accuracy and reliability. Therefore, in this paper, we study both node security and localization accuracy in the proposed secure localization algorithm. Generally, there are three kinds of sensor nodes in UWSNs: anchor nodes, unknown nodes and reference nodes. Positioning Systems (GPS) or artificial arrangement. Reference nodes consist of localized unknown nodes and initial anchor nodes. Localization process of an unknown node can be described as how the node determines its position by limited communication with several anchor nodes or reference nodes using some specific localization technologies. [5] discussed about a Secure system to Anonymous Blacklisting. The secure system adds a layer of accountability to any publicly known anonymizing network is proposed. Servers can blacklist misbehaving users while maintaining their privacy and this system shows that how these properties can be attained in a way that is practical, efficient, and sensitive to the needs of both users and services.

Unknown nodes are responsible for sensing environment data. Anchor nodes are responsible for localizing unknown nodes. They can acquire their position in advance using Global A large number of security mechanisms have been proposed to ensure safety of sensor nodes. Traditional mechanisms, e.g., cryptography and authentication, can well resist external attacks, but cannot eliminate insider attacks effectively. Although various localization algorithms have been proposed for terrestrial WSNs, they are not suitable for UWSNs. The major difference between UWSNs and terrestrial WSNs is the different communication signals. Radio signal propagates at long distances through sea water only at extra low frequencies between 30 Hz and 300 Hz. Low-frequency radio signal requires long antennae and high transmission power. Relatively, acoustic signal attenuates less and travels further. Thus, acoustic signal is more suitable for UWSNs. Acoustic communication channel has its unique characteristics. Hence, the existing localization algorithms for terrestrial WSNs cannot be applied to UWSNs.

II. PURPOSE OF CSLT

Underwater Sensor Networks are typically distributed in nature and the nodes communicate using acoustic waves over a wireless medium. Such networks are characterized by long and variable propagation delays, intermittent connectivity, limited Bandwidth and low bit rates. Due to the wireless mode of communication between the sensor nodes, a Medium Access Control (MAC) protocol is required to coordinate access to the shared channel and enable efficient data communication. However, conventional terrestrial wireless network protocols that are based on RF technologies cannot be used underwater. More than 70% of the earth's surface is covered with water. As more research is being done on underwater systems, data collection and environment monitoring become major components. These raise the need for an effective way to collect data and monitor the environment.

Although various localization algorithms have been proposed for terrestrial WSNs, they are not suitable for UWSNs. The major difference between UWSNs and terrestrial WSNs is the different communication signals. Radio signal propagates at long distances through sea water only at extra low frequencies between 30 Hz and 300 Hz. Low-frequency radio signal requires long antennae and high transmission power. Relatively, acoustic signal attenuates less and travels further. Thus, acoustic signal is more suitable for UWSNs. Acoustic communication channel has its unique characteristics. Hence, the existing localization algorithms for terrestrial WSNs cannot be applied to UWSNs.

III. WORKING OF ENHANCED COLLABORATIVE SECURE LOCALIZATION

In this paper, we propose a Collaborative Secure Localization algorithm based on Trust model (CSLT) for UWSNs. CSLT first uses trust model to ensure node safety and avoid the influence from malicious nodes, which ultimately reduces unknown nodes' localization error and enhances localization accuracy. Then, based on the collaboration of sensor nodes, localization ratio and localization accuracy can be further improved. The proposed CSLT consists of the following five sub-processes: trust evaluation of anchor nodes, initial localization of unknown nodes, trust evaluation of reference nodes, selection of reference node, and secondary localization of unknown node. In the first sub-processes, each anchor node pretends to be an unknown node to ask for localization and evaluate trust for each other. Only trusty anchor nodes can be used to localize unknown nodes. Then, the unknown nodes fail to be localized in the initial localization process can ask for secondary localization. Before the secondary localization, the trust values of reference nodes are calculated based on the cloud theory. Only trusty reference nodes are chosen to further localize the rest of unknown nodes until all the nodes are successfully localized.

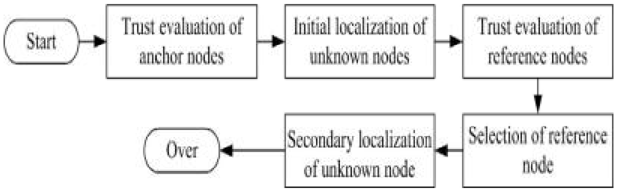
Start
Trust evaluation of anchor nodes
Initial localization of unknown nodes
Trust evaluation of reference nodes
Selection of reference node
Secondary localization of unknown node
Over

Figure 6. The five sub-processes in Collaborative Secure Localization algorithm based on Trust model (CSLT).

A. LIST OF MODULES

1. Trust evaluation of Anchor nodes
2. Initial Localization of unknown nodes
3. Trust evaluation of Reference nodes
4. Selection of Reference Node
5. Secondary Localization of Unknown Node.

1) *Trust evaluation of Anchor nodes:* In this paper, based on the sliding time window, we update sensor nodes' trust values as follows each time window T consists of several units t. During each time slot t, packets redare exchanged between two neighbor nodes, trust evidences can be collected to evaluate trust of sensor nodes. After a unit of time elapses, the window slides one time unit forward. Then, in the next time window t + 1, the historical trust values can be used to update new trust values, thereby dropping the recorded information during the last time window t.

2) *Initial Localization of Unknown Nodes:* In the first part of trust model, trust evidences are collected. As analyzed, there are many malicious attacks against localization and the main attack results can be classified into two categories: heavy packet loss and packet error. On one hand, malicious nodes can selectively forward or discard localization beacons, and they also can be selfish nodes refusing to take part in the localization process. In this case, unknown nodes may fail to localize themselves due to missing beacons, which introduces high packet loss. On the other hand, malicious nodes can monitor localization beacons from normal anchor nodes, then modify the beacons or send wrong localization information to mislead unknown nodes' localization, which introduces high packet error.

3) *Trust Evaluation of Reference Nodes:* In the process of trust calculation for one-hop neighbor nodes, there are two main types of trust evaluation: direct trust evaluation and recommendation trust evaluation If an anchor node a wants to obtain the trust value of another anchor node b, the evaluated anchor node b is named as a target node. The evaluating anchor node a which is responsible for trust evidence collection and trust evaluation is named as a sponsor node. Based on communication behaviors between anchor nodes, a sponsor anchor node can assign a target anchor node with different trust values. If there are direct communications between anchor nodes, direct trust is calculated. Otherwise, recommendation trust can be computed based on other anchor nodes' recommendations.

4) *Selection Reference Node:* Then, based on the collaboration of sensor nodes, localization ratio and localization accuracy can be further improved. The proposed CSLT consists of the following five sub-processes: trust evaluation of anchor nodes, initial localization of unknown nodes, trust evaluation of reference nodes, selection of reference node, and secondary localization of unknown node. In the first sub-processes, each anchor node pretends to be an unknown node to ask for localization and evaluate trust for each other. Only trusty anchor nodes can be used to localize unknown nodes. Then, the unknown nodes fail to be localized in the initial localization process can ask for secondary localization. Before the secondary localization, the trust values of reference nodes are calculated based on the cloud theory. Only trusty reference nodes are chosen to further localize the rest of unknown nodes until all the nodes are successfully localized.

5) *Secondary Localization of Unknown Node:* All the unknown nodes that receive the coordinates can estimate their distances to the corresponding anchor nodes. If an unknown node receives four or more than four non-coplanar coordinates from different anchor nodes, the unknown node can calculate its position based on a multilateral localization method. However, in large-scale UWSNs, not all the unknown nodes can be successfully

localized in the first sub-process. For example, some unknown nodes may not receive enough at least beacons from anchor nodes, or receive beacons from coplanar anchor nodes. In this case, the unknown nodes cannot be localized. In order to localize all the unknown nodes in the UWSN, we propose use other distance estimation methods and localization algorithms to help unknown nodes with localization.

B. PROPOSED SYSTEM ADVANTAGES

The objective of the project titled "An Enhanced Collaborative Secure Localization Algorithm Based on Trust Model in Underwater Wireless Sensor Networks"

1. To ensure node safety and avoid the influence from malicious nodes, which ultimately reduces unknown nodes localization error.
2. Enhances localization accuracy.

IV. SURVEY OF UWSN

*A. Existing system based on mobile algorithm:*In real applications, an absolutely stationary network does not exist. The underwater sensor nodes always freely float with ocean current. Therefore, in many research works, ocean current and sensor mobility are taken into account in localization algorithms. For example, in [1], a Collaborative Localization Scheme (CLS) is proposed for mobile UWSNs, where unknown nodes collaborate with each other to determine their positions autonomously without using any anchor nodes. In addition, in mobile UWSNs, mobile anchor node, e.g., Dive and Rise (DNR) anchor nodes [2, 3], Autonomous Underwater Vehicles (AUVs) [4, 5], mobile detachable elevator transceiver (DET) [6], are adopted to improve localization performance. DNR anchor nodes and AUV equipments are equipped with GPS. They can first obtain their positions on the ocean surface, then sink into water and broadcast their positions to localize unknown nodes. In order to avoid position change from ocean flow, the anchor nodes periodically rise to the surface to update their position information. Mobile anchor nodes can move not only in the vertical direction, but also in the horizontal plane. For example, in [7], a Range-free scheme based on Mobile Beacons (RSMB) is proposed for UWSNs, where a mobile anchor node moves on the sea surface at a constant speed following the random way-point (RWP) model and broadcasts localization beacons for unknown nodes. The unknown nodes localize themselves based on the projection technique. In [8, 9], a novel Underwater Directional Beacons (UDB) is proposed for UWSNs, where a mobile AUV moves according to a predefined route navigated by compass and sends directional beacons to localize unknown nodes. Compared with stationary localization algorithms, mobile ones are more suitable for dynamic UWSNs.

V. UWSN ARCHITECTURE

There are three different architectures for UWSNs:

A. Static Two-Dimensional Underwater Sensor Networks

All the nodes anchored to the ocean floor. An uw-sink collects the data from the sensor nodes by the horizontal transceiver. Then, it relays the information to surface station by the vertical transceiver.

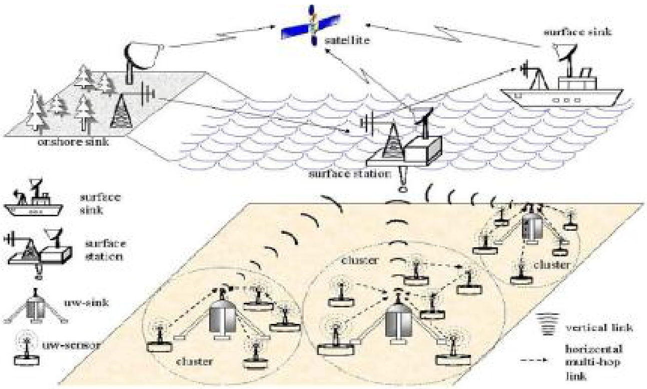

Figure 2: Static two-dimensional UWSN

1) In the direct link: each sensor directly sends data to the selected sink. This may not be the most energy efficient.
2) In multi-hop path: the source sensor relayed the data to intermediate sensors until reaches the sink. This saves the energy and increases the network

capacity, but also increases the difficulty of the routing.

B. Static Three-Dimensional Underwater Sensor Networks

Each node attached to a buoy by a cable. The sensed data transmitted to the central station by the buoy using RF signal. However, floating buoys may block ships navigating, or can be noticed and turned off by opponents in military applications. The scheme whose sensor nodes anchored to the bottom can overcome this. The sensors anchored to the seabed and fitted out with floating buoys. The buoy pays the sensor towards the water surface. The lengths of the cables are different for the required depth.

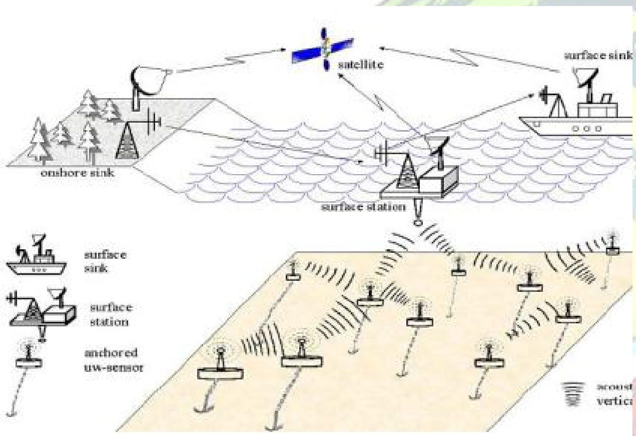

Figure 3: Static three-dimensional UWSN (Node anchored to the bottom)

C. Three-Dimensional with Autonomous Underwater Vehicles

It consists of lots of static sensors together with some autonomous underwater vehicles (AUVs). AUVs play a key role for additional support in data harvesting. AUVs could considered as super nodes, which have more energy, can move independently, and it could be a router between fixed sensors, or a manager for network reconfiguration, or even a normal sensor. Proposes a specialized architecture for UWSNs to provide Energy Efficient and Robust Architecture.

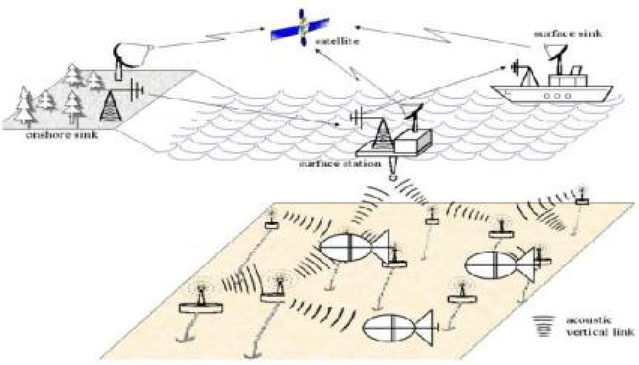

Figure 4: Static three-dimensional with AUV

VI. Working of Algorithm

The algorithms covered in our survey are grouped according to their objective, to make it easier for the reader to understand the point of each algorithm. We survey algorithms used by a group of sensor nodes to verify the location of another node. We survey algorithms used by a sensor node to estimate its location correctly.

The protocols described under this category aim to verify location claims of nodes. This is particularly important because, usually, nodes are granted more services, privileges, trust or credibility when they are closer to other nodes. So, an adversary node would probably try to claim a closer location to an authority node.

By introducing this protocol, Brands and do not solve the problem of verifying location claims. Rather, they solve the closely related problem of a verifier that wants to assure that a prover is within a certain distance. The distance-bounding protocol has been extended in so many ways in wireless localization schemes. A verifier sends out a single-bit challenge. A prover, immediately after receiving the challenge, sends out a single-bit response. The verifier logs the round-trip time (the time it took the response to reach the verifier after sending out the challenge). This process repeats K times (K being a security parameter). After that, the verifier determines the upper-bound on the distance by multiplying the maximum delay (i.e. the maximum round-trip time) by the known signal propagation speed.

Showed how this can prevent a mafia fraud attack described in Recall that the main players in a mafia fraud attack are: a legitimate prover p, a legitimate verifier v, a malicious prover pm, and a malicious verifier vm. The K challenges and the K responses are chosen at random, and the rapid bit transfer is performed (i.e. sending the K challenges and receiving the K responses). p signs, using its secret key, the concatenation of all the 2k bits and sends the signature to v, which accepts it if and only if the received signature is correct, and finds the upper bound on the distance using the rapid bit transfer. There is a possibility that pm guesses the random responses of p. However, the possibility decreases exponentially with increasing the value of K.

VII. CONCLUSION

In this paper, we proposed CSLT for UWSN. CSLT is a cost effective and energy efficient strategy. Here, based on trust model we calculate anchor nodes trust values. Only trust model and reference nodes helps to localize unknown nodes to avoid impact from malicious nodes. CSLT provides better sensor node safety and localization accuracy which plays an important role in UWSN. CSLT has helped to achieve a high detect ratio of malicious nodes. Malicious nodes cause packet error or loss in their own communication. We are using trust model to avoid the attacks from malicious nodes. However, real malicious nodes cannot be detected efficiently. We use MATLAB to evaluate the performance of the proposed algorithm. In order to easily compare our new algorithm with previous work.

Our future work includes to develop enhanced trust model which offers strong defense not only against distance reduction attacks but also distance enlargement attacks and to overcome the communication behavior which are impacted by surrounding malicious node. Last but not least we will further study the new platforms and underwater localization algorithms which may provide accurate position of the nodes and their safety measures.

REFERENCES

[1]. Mirza, D.; Schurgers, C. *Collaborative localization for a fleets of underwater drifters.* In Proceedings of the oceans, Vancouver, BC, Canada, 29 September–4 October 2007; pp. 1–6.

[2]. Erol, M.; Vieira, L.F.M.; Gerla, M. *Localization with Dive'N'Rise (DNR) Beacons for Underwater Acoustic Sensor Networks.* In Proceedings of the 2ndWorkshop on Underwater Networks, Montreal, QC, Canada, 9–14 September 2007; pp. 97–100.

[3]. Erol, M.; Vieira, L.F.M.; Caruso, A.; Paparella, F.; Gerla, M.; Oktug, S. Multi Stage Underwater Sensor Localization using Mobile Beacons. In Proceedings of the 2nd International Conference on Sensor Technologies and Applications, Cap Esterel, France, 25–31 August 2008; pp. 25–31.

[4]. Erol, M.; Vieira, L.F.M.; Gerla, M. AUV-Aided Localization for Underwater Sensor Networks. In Proceedings of the International Conference on Wireless Algorithms, Systems and Applications (WASA), Chicago, IL, USA, 1–3 August 2007; pp. 44–54.

[5]. Christo Ananth, A.Regina Mary, V.Poornima, M.Mariammal, N.Persis Saro Bell, “Secure system to Anonymous Blacklisting”, International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Issue 4,July 2015,pp:6-9

[6]. Waldmeyer, M.; Tan, H.P.; Seah, W.K.G. A Hierarchical Localization Scheme for Large Scale Underwater Wireless Sensor Networks. In Proceedings of the 11th IEEE International Conference on High Performance Computing and Communications, Seoul, Korea, 25–27 June 2009; pp. 470–475.

[7]. Lee, S.; Kim, K. Localization with a Mobile Beacon in Underwater Sensor Networks. In Proceedings of the IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC), Hong Kong, China, 11–13 December 2010; pp. 316–319.

[8]. Luo, H.; Zhao, Y.; Guo, Z.; Liu, S.; Chen, P.; Li, L.M. UDB: Using Directional Beacons for Localization in Underwater Sensor Networks. In Proceedings of the 14th IEEE International

Conference on Parallel and Distributed Systems (ICPADS), Melbourne, Australia, 8–10 December 2008; pp. 551–558.

[9]. Luo, H.; Guo, Z.; Dong, W.; Hong, F.; Zhao, Y. LDB: Localization with directional beacons for sparse 3D underwater acoustic sensor networks. J. Netw. 2010, 5, 28–38.