International Journal of Research
Available at
https://www.internationaljournalofresearch.org/

ISSN: 2236-6124
Volume 09 Issue 01
Jan-June 2019

Encrypted security using K- Query for Two-Tiered sensor network

SHAIK MAHABOOB BASHA [1] KASUKURTHI AVIL PRADEEP [2]

[2]PG Scholar,Dept of CSE, QIS college of engineering and technology ,Ongole ,Prakasam Dist,Andhra Pradesh

[1]Assistant Professor,Dept of CSE, QIS College of Engineering and technology ,Ongole ,Prakasam Dist,Andhra Pradesh

Abstract- In two-tier wireless sensor networks, resource-rich storage nodes at the upper tier collect sensing data from resource-poor sensor nodes at the low tier, and then answer queries from the user. Sensor nodes perform sensing task and submit sensing data in one time-slot to the nearest storage node while storage nodes answer and process the query from the network owner. However the storage nodes confront serious security concerns. Storage nodes may be compromised and leak the sensitive data as well as returning fake query result. Therefore, it is important to protect the privacy and verify the query results. In this paper, we define and solve the practical and challenging problem of privacy-preserving and verifiable top-k query processing performed on the time-slot sensing data set in two-tier sensor network, and establish a set of privacy and correctness requirements for such a secure top-k query scheme to become a reality. We propose the basic PriSecTopk scheme by using order-preserving encryption, and then improve it step by step to achieve various privacy requirements as well as the correctness requirements in three levels of threat models. Theoretical analysis and experiment on the real-world data set successfully validate the efficacy and efficiency of the proposed schemes.

I. Introduction

Numerous characteristics precise to communications of underwater acoustic and networking commence added design complication into almost each layer of the stack of network protocol. All applications of Underwater Sensor depend on service of time synchronization [4]. There are a variety of algorithms of time synchronization which are by now projected for Underwater Sensors and these algorithms efficiently address the delays of long propagation together with TSHL D-Sync and MU-Sync. TSHL is intended for the networks of static hence, it does not regard as mobility of sensor node. MU-Sync confronts the issue of mobility; however it is not energy proficient [8]. The distinctive attribute of Mobi-Sync is how it makes use of information with reference to the spatial connection of nodes of mobile sensor to approximate the extensive propagation of dynamic delays between nodes [1]. To prevail over the limitations of approaches of existing, Mobi-Sync, a scheme of high energy efficient time synchronization which is exclusively designed for mobile Underwater Sensor networks was implemented. Mobi-Sync achieves enhanced accurateness when additional messages are substituted during the process of time synchronization. It is the algorithm of first time synchronization to make use of the underwater objects spatial correlation features, recovering the accuracy of synchronization in addition to the energy effectiveness [11]. Due to the potential profits and outstanding challenges posed by the water environment, the networks of Underwater Sensor have expanded important concentration. The results of simulation illustrate that this novel approach achieves superior accuracy with a lower message transparency. The procedure of time synchronization consists of three phases such as delay assessment, linear regression and phase of calibration [3]. UWSNs are often deployed in an environment, with many unattended sensor nodes. These sensor nodes are likely to undergo many critical security attacks [5], such as replay attack, message manipulation attack, and delay attack [6] [7].Therefore, time synchronization must prevent the modification attempts made by these attackers especially in applications such as military surveillance and oceanographic data collection. These attackers manipulate time stamp information of the neighbouring nodes and provide the nodes with incorrect information. In replay attack, a valid data transmission is repeated maliciously and the attacker can take part in distributing timing messages among its neighbour nodes because of which the old timing messages will be sent to its neighbouring nodes as the new time stamp information for disrupting the timing synchronization process. In message manipulation attack, an attacker can drop, modify the exchanged timing messages to interrupt the process of time synchronization. Similarly in a delay attack, an attacker delays the time messages in order to disrupt the time synchronization process and cause it to fail. There are many time synchronization algorithms that have been proposed in UWSNs .These algorithms include Mobi-Sync [8] etc. Each algorithms have their own strength and short comings. Such as the TSHL is mainly used for static networks. Therefore it does not consider the mobility of the sensor nodes .But in case of MU-Sync it considers the node mobility, but it is not energy efficient. Whereas in Mobi-Sync, high energy efficient time synchronization algorithms has been designed for mobile UWSNs [15] but Mobi-Sync is considered only for dense networks. So other methods such as DA-Sync [10] methods have been introduced .The recently introduced technique is the cluster based secure synchronization approach where the nodes have been grouped into clusters and the cluster head manages the time synchronization of these nodes. A Similar process has been done in MU-Sync but it applies half of the round trip time in order to calculate the propagation delay, which can contain many significant errors when sensor nodes move rapidly, whereas in cluster based approach (CLUSS) [5] reduces synchronization errors as well as energy consumption compared to that of other methods In this paper, we discuss a number of techniques along with their benefits and issues in underwater sensor networks. A comparative study of these techniques used in UWSNs has been elaborated. A thorough understanding and differentiation of each of these techniques have been tabulated in Table I and an easy overview is been provided regarding the time synchronization in UWSN.

II.STATIC NETWORK APPROACHES

1. TSHL

TSHL is the first time synchronization technique introduced for high latency networks. TSHL is a two phase technique for time synchronization. The main idea in TSHL [14] is that it splits time synchronization process in the mobile UWSN into two phases. In the first phase, the nodes estimate clock skew. In the second phase in order to determine the offset, they swap skew compensated synchronization messages within the network. After the completion of the 2 phases we get a model that maps the local, inaccurate clock to the reference time base. We can then compute a global time for synchronization. In phase one, without receiving any knowledge about the propagation delay we are estimating the clock skew, which means the accuracy of the estimation is dependent on consistency, not the duration, of propagation delay. In this method we assume that the propagation is constant over the message exchange. The second assumption we are made in the TSHL is that clocks are short term stable, which means clock frequency and skew remains constant for a short period of time (typically 5-10 min). The factors enabling the short term instability includes environmental factors such as sudden variation in temperature, supply voltage or shock. This assumption allows us to use linear regression for modeling the clock skew.

2. WATERSync

WATERSync [21] is a correlation-based time synchronization protocol specifically for shallow underwater sensor networks. WATERSync integrates the time synchronization procedure with the tree-like network routing topology in vertical direction (the surface station is the tree root), which consists of Gradual Depth Timing (GDT) phase and Level 1 (i.e., between the surface station and first depth nodes) Skew Compensation (LSC) phase. To make the time synchronization dependable, WATERSync adopts a correlation based security model to detect outlier timestamp data and identify malicious nodes. However, horizontal direction is neglected during the process of time synchronization, which
results in high offset errors.

III.DYNAMIC NETWORK APPROACHES

1. MU-Sync

MU-Sync is a cluster-based synchronization algorithm for mobile underwater sensor networks. By estimating both the clock skew and offset, MU-sync avoids the frequent re-synchronization. MU-sync uses the message exchange for gathering the local time information, by using these information we can estimate the clock skew by performing the linear regression twice over a set of local time information. The first linear regression helps the cluster head to calculate the effect of long and varying propagation delay; the second regression obtains the estimated skew and offset. The MU SYNC mainly consists of 2 phases, namely, the skew and offset acquisition phase, and the synchronization phase. In the first phase, the clock skew and offset is estimated. The estimation of the clock skew and offset are done by applying linear regression twice over a set of n reference beacons. Comparing MU-sync with other existing technologies, it performs the linear regression twice. The first regression enables the cluster head to gather the amount of propagation delay using message exchange technique from each reference packet (REF). After receiving the REF, it adjusts the REF beacons' timings with their respective propagation delays [18]. To estimate the skew and offset a second linear regression is applied to this new set of points. In case of MU-Sync since it is cluster-based, it can be directly applied to mobile multi-hop UWSN.

2. MC-Sync

MC-Sync is a time synchronization technique for mobile underwater sensor networks which uses two mobile reference nodes for node mobility. It consists of a network with a number of sensor nodes in which a node has to be synchronized(N).MC-sync approach has two reference nodes along with time and will be located at opposite sides of the node N. Node N sends its synchronization information to both these reference nodes and due to the mobility of the node N, changes will occur in the sending position information. By using this information, the clock skew and offset have been calculated. To implement Mc-Sync algorithm [13], we need to consider two requirements that is to assume that the two reference nodes that are formed along the direction of ocean current and the node is placed in the connection link of the two reference nodes. The first requirement has been fulfilled designing equipment which consists of a two reference nodes, in which one node remains mobile and the other is a static reference node. The static reference node is connected to the mobile reference node through a light cable. After forming it we assume that the mobile reference node is in a still stage and the static reference node moves with the ocean current. The main factors affecting the movement of the static reference node is ocean current. Which in turn causes the light cable connecting the two reference nodes to move in a direction parallel to the direction of ocean current? And the second requirement is fulfilled by considering the two reference nodes should be deployed at the opposite sides of the area. Reference nodes should move a little distance and should be in the still state to perform the time synchronization. Until all the nodes have been synchronized the reference nodes keep repeating this process. The MC-sync is not energy efficient when compared to mc-sync as it does not allow the reference nodes to broadcast the synchronization messages. Thus the packet number of Mc-Sync is smaller when compared to MU-Sync.

3. Mobi-Sync

Mobi-sync is used for mobile under water sensor networks. Mobi-Sync differs from other approach as it considers spatial correlation among the moving patterns of the neighboring nodes which allow to accurately estimating the long dynamic propagation delay. There is no specific movement for the underwater objects that is it moves in random motion. So spatial correlation is required in such movement. This is used for an ordinary node to calculate its own moving velocity. The time synchronization in Mobi-Sync [8] has mainly three phases that is delay estimation, linear regression and calibration. The delay estimation is done in order to accurately estimate the propagation delay the information regarding spatial correlation is acquired. This phase mainly consist of two phases that is message exchange and delay calculation. During the message exchange an ordinary node starts the time synchronization by sending a request message to its neighboring super nodes. These super nodes on receiving the request schedules a response message back to these nodes. These response messages consist of the velocity of the super nodes along with its time stamp. illustrates message exchange among sensor nodes for the case where there are three super nodes available to assist the ordinary node perform time synchronization. The second step during the first phase is delay calculation where the ordinary node computes its own velocity by using the spatial correlation information contained in the velocity vectors of the super nodes. The ordinary nodes continue to send the response message until they get enough points to perform linear regression. During the second phase the first round of linear regression is performed with the propagation delay and the time stamp obtained in the first phase and estimates the clock skew and the offset. Here weighted lest square estimation procedure is used in order to reduce the assumptions made during the 1st phase. In the last phase that is the calibration phase to improve the accuracy during the synchronization the ordinary node updates the initial skew and distance and then recalculates the propagation delay and performs the linear regression again. The second round of linear regression provides the final clock skew and offset.

4. DA-Sync

DA-Sync that is Doppler assisted time synchronization scheme uses a pair wise cross layer time synchronization approach for under water sensor networks. Compared to the other synchronization approaches DA-Sync works in physical MAC cross layer. In DA-Sync the Doppler shift [6] [18] that is the relative changes in velocity has been estimated and then the accuracy in synchronization is maintained by employing a kalman filter. In order to measure the relative velocity of the sensor nodes they use Doppler scaling factor estimation algorithm which are further refined by a kalman filter in order to improve accuracy. Advantages of this approach is that accuracy of the propagation delay estimation is tremendously improved when compared to the other approaches as it incorporates the relative moving velocities between these nodes. Whereas the previous approaches used half of the round trip time to estimate the propagation delay. Also it uses the MAC layer time stamp information's to reduce the non-deterministic errors in the time synchronization.

5. CLUSS

The CLUster-based Secure Synchronization approach (CLUSS) [5] considers both security and accuracy in synchronization. CLUSS ensures the security of synchronization against various attacks like Sybil attack, replay attack, message manipulation attack, and delay attack. This system mainly consists of three types of nodes such as beacons, cluster head and ordinary nodes as shown. Beacons are nodes that have unlimited energy resources and two beacons communicate with each other through radio frequencies. Whereas beacons communicate to the ordinary nodes and cluster heads using links. These nodes are classified or divided into different clusters and each of these clusters has one cluster head. All the ordinary nodes are connected to these cluster heads through a hop. The beacons are present in the water surface along with the GPS in order to obtain time information. CLUSS protocols mainly consist of three phases which include the authentication phase, inter-cluster synchronization phase as well as the intra-cluster phase. In the authentication phase all the sensor nodes are authenticated to each other and they identify and remove the malicious nodes from the networks. Then in the inter cluster phase the cluster nodes synchronize with the beacons in the sender to receiver mode and the intra-cluster phase the ordinary nodes synchronize with the cluster head in the receiver to receiver mode. In order to reduce the message overhead a part of the inter-cluster synchronization phase and the intra-cluster synchronization phase can be executed concurrently. The advantage of the cluster based secure synchronization protocol is that it improves the time synchronization accuracy by detecting abnormal end to end delay and also identifies the malicious nodes in the network. It also finds the difference in the propagation delay of the downlink from that of uplink caused during the node movement. CLUSS can reduce the errors during time synchronization as well as the energy Consumption when compared to other protocols.

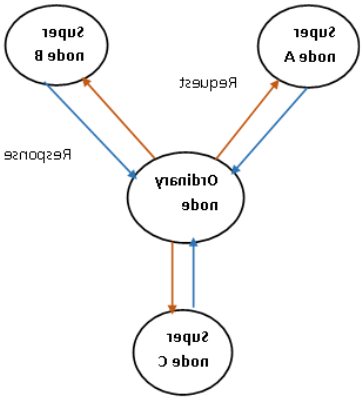

Fig1. Message exchange.

IV.CONCLUSION

This paper presents the study of various Time Synchronization Techniques used in under water sensor networks.

The approaches discussed in this paper are TSHL, MC-Sync, MU-Sync, Mobi-Sync, DA-Sync and CLUSS. A comparative study of all these methods along with their benefits and short comings have also been discussed in order to provide a clear overview of these techniques.

REFERENCES

[1] John Heidemann, Wei Ye, Jack Wills, Affan Syed, Yuan Li, "Research Challenges and Applications for Underwater Sensor Networking," *IEEE Communications Society (2006), 228-235.*

[2] Li Wang, Zhi Bin Wang, et al., "A survey of time synchronization of wireless sensor networks", Conference on Wireless, Mobile and Sensor Networks (CCWMSN07)2007.

[3] Zhengbao Li, Zhongwen Guo, Feng Hong, Lu Hon, "E2DTS: An energy efficiency distributed time synchronization algorithm for underwater acoustic mobile sensor networks," Ad Hoc Networks 11 (2013) 1372–1380

[4] Lasassmeh, S.M., Conrad, J.M., "Time Synchronization in wireless sensor networks: a survey",IEEE SoutheastCon, 2010.

[5] Ming Xu, Guangzhong Liu, Daqi Zhu, Huafeng Wu, "A Cluster-Based Secure Synchronization Protocol for Underwater Wireless Sensor Networks," Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2014, Article ID 398610, April 2014

[6] Y. Liu, J. Li, and M. Guizani, "Lightweight secure global time synchronization for wireless sensor networks," in *Proceedings ofthe IEEE Wireless Communications and Networking Conference:Mobile and Wireless Networks*, pp. 2312–2317, 2012.

[7] A. S. Uluagac, R. A. Beyah, and J. A. Copeland, "Secure sourcebased loose synchronization (SOBAS) for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 4, pp. 803–813, 2013.

[8] Jun Liu, Zhong Zhou, Zheng Peng, Jun-Hong Cui, Michael Zuba, "Mobi-Sync: Efficient Time Synchronization for Mobile Underwater Sensor Networks",IEEE Trans on parallel and Distributed Systems, Vol. 24, No. 2, Feb 2013.

[9] Jun Liu, Zhong Zhou, Zheng Peng, Jun-Hong Cui, "Mobi-Sync: Efficient Time Synchronization for Mobile Underwater Sensor Networks," *IEEE Globecom* 2010.

[10] Jun Liu, Zhaohui Wang, Michael Zuba, Zheng Peng, Jun-Hong Cui, Shengli Zhou, "DA-Sync: A Doppler-

Assisted Time-Synchronization Scheme for Mobile Underwater Sensor Networks," *IEEE Transactions on Mobile Computing*, Vol. 13, No. 3, March 2014.

[11] Nitthita Chirdchoo, Wee-Seng Soh, Kee Chaing Chua, "MU-Sync: A Time Synchronization Protocol for Underwater Mobile Networks," *WuWNet'08,* September 15, 2008, San Francisco, California, USA.

[12] Feng Lu, Diba Mirza, Curt Schurgers, "D-Sync: Doppler-Based Time Synchronization for Mobile Underwater Sensor Networks," *WUWNet'10,* Sept. 30 - Oct. 1, 2010, Woods Hole, Massachusetts, USA.

[13] Jun Liu, Zhong Zhou , Zheng peng , Jun-Hong Cui, Michael Zuba ,Lance Fiondella " Mobi-Sync : Efficient Time Synchronization for Mobile Underwater Sensor Networks " – IEEE Transactions on Parallel and Distributted System Vol 24, No . 2 FEBRUARY 2013.

Author's Profile

Sk.Mahaboob Basha

Assoc.professor,Dept of CSEQIS College of Engineering & Technology,Vengamukka Palem,Ongole.His intrested areas include Computer networks,Computer orgniation andprogramming.

\

KASUKURTHI AVIL PRADEEP

B.Tech(IT(INFORMATION TECHNOLOGY)) in SSN ENGG COLLEGE, Ongole

M. Tech(CSE) Scholar in QIS college of Engg and Tech, Ongole