www.ioirp.com

International Journal of Innovative Research in Technology, Science & Engineering (IJIRTSE)
ISSN: 2395-5619, Volume – 1, Issue – 2. April 2015

AN EFFICENT TIME SYNCHRONIZATION AND SECURE DATA FORWARDING SCHEME IN UNDERWATER NETWORK

[1]PADMA PRIIYAA S R M, [2]SARANYA P
[1]PG Student (M.E-Communication and Networking), Department of Electronics and Communication Engineering,
Pavendar Bharathidasan College of Engineering and Technology, Tiruchirappalli, India
[2]Assistant professor, Department of Electronics and Communication Engineering,
Pavendar Bharathidasan College of Engineering and Technology, Tiruchirappalli, India
[1]priyahasini07@gmail.com, [2]psaranya_08@yahoo.co.in

***Abstract*— Underwater Wireless Sensor Networks (UWSNs) offer new Underwater MAC protocols have been proposed to improve limitations caused by severely limited bandwidth and long propagation latency of acoustic waves. Unfortunately, acoustic breakers incur extended propagation delays that classically lead to low throughput particularly in protocols that require receiver feedback such as Flow data delivery.. To satisfy these needs, innovative time synchronization and Security solutions are demanded. We propose novel time synchronization and Secure Data forwarding scheme, called "TSSR".It utilizes the spatial correlation of UWSN nodes to estimate the long dynamic propagation delays. TSSR includes Sequential algorithm for time-synchronization, multi-pack transmission and also support reliable data transmission using end to end Authentication in underwater acoustic channel. Simulation results demonstrate that our algorithm compensates for time synchronization and signal propagation speed uncertainties, and achieves good result by comparing existing Mac protocols.**

I. INTRODUCTION

Sensor networks are becoming common-place for real-time information since they have ability to gather the information from their deployed area during the monitoring task. New achievements in wireless communications brought forth the recent generation of sensors with low cost, low power and multi-functional properties. Whereas the sensors enable to communicate in short distances and deployed in large numbers, networking them through wireless links promise a wide range of applications for monitoring homes or controlling cities. Moreover, the wireless networked sensors have enabled opportunities in the defense areas and surveillance as well as other tactical applications.

A Wireless Sensor Network (WSN) is normally designed based on its special application's objectives and operational environments. It can be classified into five main categories: Terrestrial WSN, Mobile WSN, Underground WSN, Underwater WSN, and Multimedia WSN. During the last decades, a growing interest in Underwater Wireless Sensor Network (UWSN) has been observed, while it is integrated with some different challenges. The major challenge in UWSN comes from its propagation medium.

There is only one choice for underwater communications which is acoustic link. In fact, radio waves suffer from high attenuation at long distances. On the other hand, optical waves are seriously affected by scattering. Hence, underwater acoustic networking is the enabling technology for the UWSN applications, and it successfully provides some opportunities of ocean environment monitoring such as the life of the ocean animals and target tracking as well as mine recognition. Additionally, the underwater warfare capabilities of the naval forces can benefit from the UASNs. As one of the humanism applications of UASN technology, the Earthquake and tsunami forewarning systems can also be addressed. The focus of this paper is to reduce latency and improving a secure communication in underwater wireless sensor network (UWSN) by introduces a TSSR scheme.

II. RELATED WORKS

In this paper proposes anew underwater MAC protocol called Time –synchronization and Secure Data forwarding scheme (TSSR),is a new solution to degrade the delay propagation and also upgrade the performance, network life time and also establishing a secure communication.

A. DOTS Protocol:

A Delay aware opportunistic Transmission Scheduling (DOTS)is used to observe the neighboring nodes information. It includes the propagation delay map and their transmission schedule. This protocol constructs a delay map management during the session which is estimate by two technique 1) temporal reuse 2) spatial reuse. However it has a long delay transmission and limitation of bandwidth in acoustic channel. To alleviate this issues introduce a sequential time synchronization and localization

B. Route discovery:

The whole route discovery process has three steps.

Step 1: node 1 detect its depth d I by its depth perception; after that, it broadcasts both d1 and its' lDl to its neighbors, Then waiting to receive feedback messages in time. Delay time t = R / V; R is the maximal transmission range (communications radius). V is the underwater sound propagation speed, 1500m/s. T=2t.
Therefore, if it receives feedback messages on time T, it has next hop node.

Step 2: assuming node 2 receives the broadcast message of node l. dz is the depth of the node 2. There are two cases. d, >= d I , node 2 is below node 1. At this point, node 2 discards the broadcast message without any response. If dz<d] ; node 1 is below node 2. At this point, node 2 is one of the candidates of node l Node 2 compute(JDl, then sends both F(JD2) and its' IDz to F(1D)EX' E node l. d is the residual energy of the current node; d, is the depth of the current node.

Step3: In the T time, node 1 receives feedback messages, and then will be recorded in a stack, Q. After time T, if Q is null, it hasn't the next hop. In order to save energy, node 1 enters into sleep state. After a random period of time, it restart the discover route, and returns to Step 1. If Q is not null, it chooses the largest (JD), and adds to the routing table. F(ID).

C. Delay map estimation:

This delay map consists of

- **Source:** the sender of the observed MAC frame
- **Destination:** the intended destination of the observed MAC frame
- **Timestamp:** the time at which the observed MAC frame was sent
- **Delay:** the estimated propagation delay between the source and the destination for the MAC frame With clock synchronization, the value of the timestamp can not only provide time information for each frame but also be an accurate indicator of the distance between the sender and the overhearing node itself.

Each node can calculate a neighbor's propagation delay to itself by subtracting the timestamp of the MAC frame from the reception Time of the MAC frame. Thus, the timestamp and delay fields provide additional distance information between the sender and overhearing node and between the sender and intended frame receiver. Given this additional information, each node can build a delay map of its one-hop neighbors and calculate the expected time a response back to the sender of the observed MAC frame will occur. Due to network dynamics, Neighboring nodes' transmissions can be backed-off or canceled. Furthermore, information of delays between each node and its one-hop neighbors can become stale. To adapt to these dynamics, an update process of the delay map is required. Whenever a new transmission is overheard, each node searches the delay map to check for the existence of existing entries based on source and destination fields. When a duplicate entry is detected, the node checks the freshness of the existing item.

D. Recovery

Neighboring non-interference. Its current transmission (RTS) and future transmission (DATA) must not interfere with neighbors' ongoing and prospective receptions (node u's prospective RTS and DATA transmissions should not interfere with node x's CTS and ACK receptions). Prospective non-interference. Its future receptions (CTS and ACK) must not be interfered with by neighbors' prospective transmissions (node u's prospective CTS and ACK receptions should not be interfered with by node x's prospective DATA transmission). In DOTS, schedule recovery happens at both sender and receiver sides. At the sender side, when an RTS or a DATA frame is sent, a timer is set to the duration by which the corresponding CTS or ACK frame is received. Once this timer expires, the sender realizes that its transmission has been

unsuccessful. In either case (i.e., no CTS or ACK reception), the sender will back off and issue a new RTS. DOTS take a conservative approach of sending a new RTS for the missing ACK to lower the potential damage; i.e., due to an incomplete delay map we cannot guarantee safe retransmission of a large packet at that moment.

III. RECENT WORKS

In this paper propose a new underwater MAC protocol, which combines the Multi-session DOTS (MDOTS) and Security named as TSSR, which redesigns Existing DOTS to enable temporal reuse. Although DOTS achieves a fair amount of channel utilization, it is unable to capitalize on temporal reuse because of its single session nature. Rather than each node keeping track of the state of a single session, in TSSR each node maintains a list of concurrent transmission sessions. Each node has a list of its current sessions, and each session independently keeps track of its own state information.

Contributions beyond TSSR: 1) it allows multiple outgoing sessions from each source and multiple (pipelined) packets on each session; 2) it applies a localized distributed algorithm and End to End Authentication to maintain Secure and collision free communication; 3) it shows significant gains with respect to existing DOTS when applied to a representative underwater monitoring and surveillance scenario.

A. MDOTS (Multi Session Transmission in DOTS):

Time Synchronization algorithm uses a sequential approach in which first nodes are time-synchronized and then location is estimated. We start with quantizing the spatial domain by representing the continuous motion of nodes as a series of discrete locations.For each received packet, the receiving node estimates the ToA(Time of Arrival) the direct path. During the localization window, two way ToA measurements for the link are obtained by piggybacking the ToA information estimated by node on packets transmitted from node to the UN, along with node 's time-varying location, ***p***These measurements are used to estimate the clock skew and offset of the UN relative to node 's internal clock and to estimate the propagation delay in the channel.

The extreme number of concurrent assemblies each node can have is a configurable value, and the routine of the protocol is heavily dependent on this value. Unless a node's current number of client session does not reach at size, a new client session is created every time the network layer has a packet for the node to send. When the client session is created, the node creates delay map entries associated with the new session. Then it checks to see if these new entries are compatible with the node's existing delay map entries.

If a collision is detected, the state's timing information is reset, and it will reattempt the transmission session after a back-off period. Otherwise, the node will send the RTS packet for this session and wait to receive a CTS packet. When the CTS packet arrives, the node sends a DATA packet and waits for an ACK packet to arrive. When the ACK packet arrives, the session is complete and the state can be taken down. A new server session is cr,,../eated whenever a node receives a RTS. When the server session is created, the node creates delay map entries associated with the new session.

It checks to see if these new entries are compatible with the node's existing delay map entries. If a collision is detected, the state is taken down and the node waits for the client to resend its RTS in order to try again with another server state. Otherwise if no collision is detected, the node will send the CTS packet for this session and wait to receive the DATA packet from the client. When the DATA packet arrives, the node retrieves the message from the packet and sends it up to the network layer.

Then the node sends an ACK packet. After the ACK packet is sent, the session is complete the state is taken down. The cases are summarized as follows:

- When a node creates a client session, it calculates its own RTS and DATA transmission times and its own CTS and ACK reception times. It also calculates the server node's CTS and ACK transmission times and its RTS and DATA reception times.
- When a node creates a server session, it calculates its own CTS and ACK transmission times and its own DATA reception time. It also calculates the client node's DATA transmission time and CTS and ACK reception times.
- When a node overhears a RTS or CTS, it calculates the client node's CTS and ACK reception times and the server node's RTS and DATA reception times

B. Secure Transmission

In order to protect privacy, we assume that underwater communications are enciphered. At the application level, every node UN shares a secret symmetric end-to-end key, eUN with the Anchor An for one-to-one communication. Node UN uses the key eUN to encrypt unicast application message addressed to an, and to decrypt unicast messages received from An. In UWSN, Data/Ctrl Transmission and energy limitations require keeping a message size small and cipher-text expansion may introduce an overhead that is not negligible anymore.

C. Estimate best path

We introduce mechanisms for path selection when the energy of the sensors in original primary path has dropped below a certain level. This allows us to distribute energy consumption more evenly among the sensor nodes in the network. Number of hope counts is also identified by using this method. The Energy Efficiency of the individual node is increased by this path selection method.

IV. MODULES

In the proposed method our modules are classified into UWSN Deployment, Time synchronization, Localization, End to End Authorization, performance analysis

A. UWSN Deployment:

In this module 50-100 sensor nodes are randomly distributed in a 100 m X 100 m X 100 m region. We define node density as the expected number of nodes in a node's neighborhood. Hence, node density is equivalent to node degree. We control the node density by changing the communication range of every node while keeping the area of deployment the same. Range measurements between nodes are assumed to follow normal distributions with real distances as mean values and standard deviations to be two percent of real distances.The 4-sender/1-sink star topology features four sender nodes competing to send their data to the center sink node. This topology is representative of a sea swarm engaged in scouting an underwater region and reporting sensed information to a U/W command post.

B. Time synchronization with MDOTS:

The objective of the time-synchronization step of the TSSL algorithm is to estimate the propagation delay, or signals transmitted between locations ***p*** and ***j*** of anchor node *l* and the UN, respectively. Since nodes are not time-synchronized, to this end we first estimate the clock skew and offset of the UN relative to anchor node *I* and then estimate the Total Propagation Delay. DOTS protocols with high session capacities can take better advantage of temporal reuse in a 4 sinks 1 sender topology.

More sessions means the central node has more opportunities to utilize temporal reuse and schedule in new transmission sessions. Because of the central node's full knowledge of the session of the channel, any successfully scheduled transmission session is guaranteed to not have any collisions. Higher session capacities leads to more aggressive scheduling of sessions, and the aggressive scheduling leads to more throughput with no increased risk of collisions.

C. Localisation:

Anchored acoustic sensor nodes compose 3dimensional communication architecture. In this architecture, each sensor is anchored to the ocean bottom and equipped with a floating buoy that can be inflated by a pump. The buoy pushes the sensor towards the ocean surface.

The depth of the sensor can then be adjusted by the wire that connects the sensor to the anchor. The node can observe phenomena and detect events such as disaster symptoms and tactical underwater vehicles between the seabed and the surface.

A node exhaustively searches the tree for recovery by traversing sub-trees one by one. Backtracking method over a virtual coordinate system where a packet is routed towards one of the anchors (used to build the virtual coordinate system), hoping that it can switch back to the greedy mode on its way. It inherits the group motion support of Landmark Routing that dynamically elects Anchor (landmark nodes). It circumvents a void in the network using the topology knowledge of landmark nodes

D. END to END Authorization:

Packets exchanged between neighbors must be authenticated to ensure that a device accepts packets only from devices that have the same pre-shared authentication key. TSSR is configurable on a per-interface basis; this means that packets exchanged between neighbors connected through an interface are authenticated. TSSR supports the Hashed Message Authentication Code-Secure Hash Algorithm-256 (HMAC-SHA-256) authentication method.

When you use the HMAC-SHA-256 authentication method, a shared secret key is configured on all devices attached to a common network.

For each packet, the key is used to generate and verify a message digest that gets added to the packet. The message digest is a one-way function of the packet and the secret key. For more information on HMAC-SHA-256 authentication, If HMAC-SHA-256 authentication is configured in an UWSN network, UWSN packets will be authenticated using HMAC-SHA-256 message authentication codes. The HMAC algorithm takes as input the data to be authenticated and a shared secret key that are known to both the sender and the receiver; the algorithm gives a 256-bit hash output that is used for authentication. If the hash value provided by the sender matches the hash value calculated by the receiver, the packet is accepted by the receiver; otherwise, the packet is discarded.

E. Performance Analysis:

We compare TSSR with well-known underwater CSMA protocols, namely Slotted FAMA (S-FAMA) and DOTS. S-FAMA is a synchronized underwater MAC protocol that eliminates the need for excessively long control packets via time slotting. It requires both the sender and receiver nodes to send warning messages when they detect possible collision, thus deferring pending data reception/transmission. DOTS is a synchronized CSMA protocol that harnesses both temporal and spatial reuse to improve throughput. Like TSSR, DOTS relies on overheard neighboring node transmissions, but it lacks the support of multiple sessions from the source.

V. SIMULATION RESULT & DISCUSSIONS

This section presents the results of our simulation. We areusingNS-2 simulator for simulation..This conclusion is TSSR was adopted as it proves to be an efficient delay aware acoustic routing protocol.

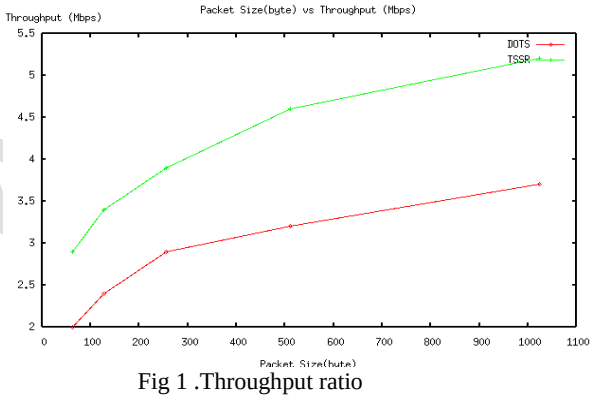

Fig 1 .Throughput ratio

Fig.1showsthe throughputs is considerably increased while comparing with DOTS and TSSR which is measure the function of offered load is multiplied the duration of transmitting data by total time duration factor Fig.2 shows the increasing the delay of links in dots comparing with TSSR. To measure the amount of time it takes a packet to travel from source to destination. Together, latency and bandwidth define the speed and capacity of a network.

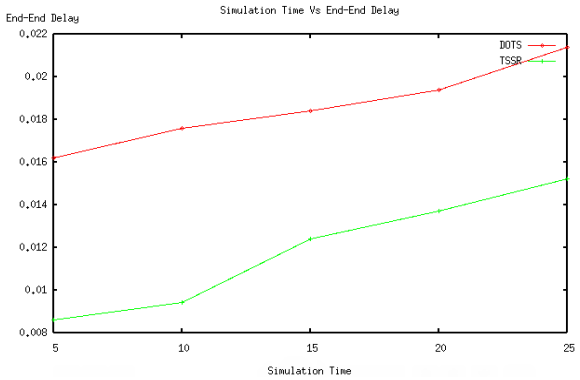

Fig.2 END to END delay

Fig.3shows the PDR is considerably increased while comparing with the DOTS and TSSR. Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources mathematically, it can be defined as: PDR=S1/S2 where, S1 is the sum of data packets generated by the each source. Graphs show the fraction of data packets that are successfully delivered during simulations time.

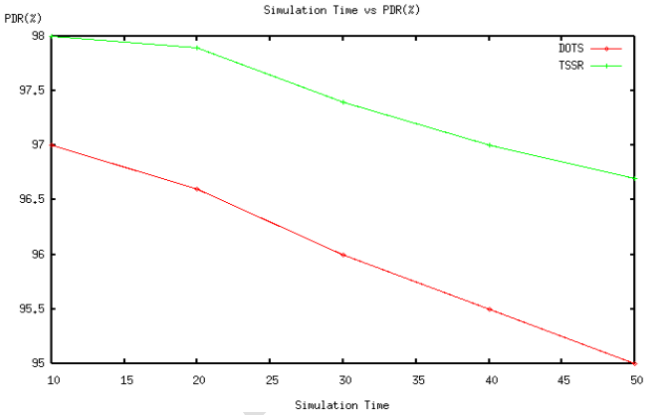

Fig 3.Packet delivery ratio

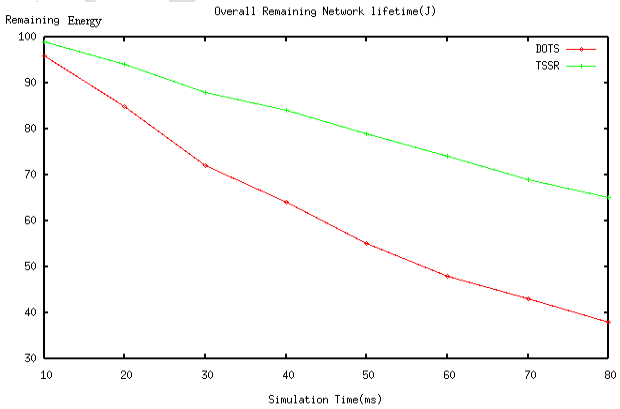

Fig 4.Networklife time

Network lifetime ratio is shown in fig.4while comparing the DOTS and TSSR. TSSR increases the network lifetime then residual energy is calculated by the number of energy packets sent to the monitoring node for various thresholds.

VI. CONCLUSION

In all wireless networks, the major problem for synchronization protocols is the variance in the send time, access time, propagation time, and the receive time. Also our proposed system supports multi-packet transmission which improved throughput and reduce the overall transmission delay Elimination or the ability to accurately predict any of these greatly increases the effectiveness of the synchronization protocol. Comparison on DOTS and TSSR was provided with each protocol's advantages. TSSR protocol was designed with performance in mind and take into account for security.

References

[1] M.Chitre, S.Shahabodeen, and M.Stojanovic, "Underwater acousticcommunications and networking: Recent advances and future challenges," in *Marine Technology Society Journal*, vol. 42, no. 1, Garmish- Partenkirchen, Germany, Apr. 2008, pp. 103–116.

[2] J. Weber and C. Lanzl, "Desigining a positioning system for finding things and people indoors," in *IEEE Spectrum*, vol. 35, no. 9, Sep. 1998, pp. 71–78.

[3] C. Lee, P. Lee, S. Hong, and S. Kim, "Underwater navigation system based on inertial sensor and doppler velocity log using indirect feedback kalman filter," in *Journal of Offshore and Polar Engineering*, vol. 15, no. 2, jun 2005, pp. 88–95.

[4] R. Hartman, W. Hawkinson, and K. Sweeney, "Tactical underwater navigation system (TUNS)," in *IEEE/ION Position, Location and NavigationSymposium*, Fairfax, Virginia, USA, May 2008, pp. 898–911.

[5] V. Chandrasekhar, W. K. Seah, Y. S. Choo, and H. V. Ee, "Localization in underwater sensor networks - survey and challenges," in *Proc. OfACM International Conference on Mobile Computing and Networking(MobiCom)*, New York, NY, USA, Sep. 2006, pp. 33–40

[6] J. Partan, J. Kurose, and B. Levine, "A Survey of Practical Issues in Underwater Networks," in *International Conference on Mobile Computingand Networking (MobiCom)*, Los Angeles, CA, USA, Sep. 2006.

[7] W. Burdic, *Underwater Acoustic System Analysis*. Los Altos, CA, USA: Peninsula Publishing, 2002.

[8] M. Erol, H. Mouftah, and S. Oktug, "Localization techniques for underwater acoustic sensor networks," in *IEEE Commun. Mag.*, vol. 48, no. 12, 2010, pp. 152–158.

[9] H. Tan, R. Diamant, W. Seah, and M. Waldmeyer, "A survey of techniques and challenges in underwater localization," Accepted for Publication in the ACMJournal of Ocean Engineering [Onl

[10] http://ecs.victoria.ac.nz/twiki/pub/Main/TechnicalReportSeries/ECSTR11- 03.pdf].

[11] J. Garcia, "Adapted distributed localization of sensors in underwater acoustic networks," in *MTS/IEEE international Oceans conference*,Singapore, May 2006.