UW-ASNs: DESIGN CHALLENGES IN TRANSPORT LAYER

Reeta Mishra

Assistant Professor, Department of Computer Science & Engineering, K .J. I.T, Gujarat, India

Abstract

Underwater Acoustic Sensor Networks (UW-ASN) consist of a variable number of sensors and vehicles that are deployed to perform collaborative monitoring tasks over a given area. This paper included a suggestion of using SCTP protocol in place of TCP to minimize many of the problem in transport layer of the sensor network designing part..As well as I have also suggest like an idea to improve the traffic shaping so problem like packet/data loss etc solved and regulate traffic rate is possible so temporary loss of connectivity can be solved. In this paper as possible even I have mention the challenges in various layer of UW-ASN design.

Keywords: *underwater ASNs, design, transport layer, challenges.*

----------***----------

1. INTRODUCTION

In our earth 25% covered by human being and remaining space is covered by water that could be river and oceans also. In underwater wireless sensor network much small water living thing like fish, crocodile and many more. Suppose a scientist work on particular a thing so some special devices should be in underwater wireless sensor network that can work in underwater wireless sensor network system which should be able to interact within underwater. Group of sensors and vehicles deployed underwater and networked via acoustic links, performing collaborative tasks. Equipment that are used can be named as Autonomous Underwater Vehicles (AUVs) and Underwater sensors (UW-ASN).

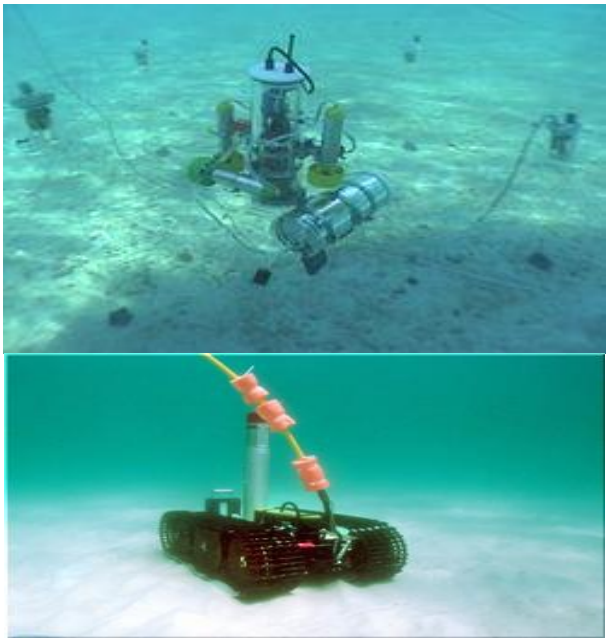

Fig: 1- Underwater Vehicles, Underwater sensor

1.1 Objectives

UW-ASNs-

-To search multi hop paths
-Signaling overhead to be reduce for building underwater paths

AUVs-

-Rely on local intelligence
-Dependence is less from online shores communications
-Control methods (autonomous coordination obstacle avoidance

1.2 Application of UWASN:-

i). Monitoring of Environment
ii). Effect of human activities on the marine ecosystem
iii). Explorations of Undersea/underwater
iv). Underwater oilfields Detection
v). Disaster handling and prevention
vi). Ocean currents and winds (Tsunamis) Monitoring
vii) Navigation of Assisted
viii) In shallow waters monitoring and Locate dangerous rocks
ix) Distributed tactical surveillance
x) Intrusion detection (Navy)

2. UWASNs ARCHITECTURE-

Two-dimensional Underwater Sensor Networks: for monitoring of ocean bottom

Three-dimensional Underwater Sensor Networks: for monitoring of ocean-column

Autonomous Underwater vehicles in Sensor Networks: for explorations of underwater

Design Challenges in various layer of UW Sensor networks-

2.1 MAC Layer

a) [9] Design access codes for CDMA taking into account minimum interference among nodes
b) To solve the stability problem in the coupling between the phase locked loop (PLL) and the decision feedback equalizer (DFE).[4]
c) Maximize the channel utilization
d) Distributed protocols to save battery consumption.
e) It needs to develop cheap transmitter/receiver modems for underwater communications [4]

2.2 Network Layer

a) Develop algorithms that reduces the latency
b) Handle loss of connectivity using mechanisms without generating retransmission
c) Algorithms and protocols needs to improve the way to deal with disconnections because of failures of battery depletion
d) How to integrate AUV with UW-ASNs and able communication among them
e) Geographical routing protocols [2], it is necessary to device good and efficient underwater location discovery techniques.
f) The delay variance in vertical links is generally smaller than in horizontal acoustic links due to multi-paths.

2.3 Data Link Layer

a) In order to maximize the network efficiency research on optimal data packet length need to done.
b) In order to maximize the network efficiency research on optimal data packet length need to done.
c) It necessity to devised Distributed protocols to reduce the activity of a device when its battery is depleting without compromising on network availability

2.4 Transport Layer

a) Flow control strategies to reduce high delay as well as delay variance of the control messages
b) Efficient mechanisms to find the cause of packet loss [12] and reliable network.
c) To create solutions for handling the effect of connectivity losses caused by shadow zones
d) Flow control- In Data transmissions to avoid that network devices with limited memory are overpower.
e) Congestion control-To prevent the network being congested
f) TCP implementations are not suited-The long Round Trip Time (RTT) in underwater environment affects the throughput.

2.5 Application Layer

It include understanding of the application areas and the communication problems in underwater sensor networks is difficult to outline some design principles on how to explain or reshape existing application layer protocols [1] for terrestrial sensor networks.

3. SUGGESTION

Instead of using TCP protocol because its implementations are not suited, the long Round Trip Time (RTT) in underwater environment affect the throughput. We can use Stream Control Transmission Protocol (SCTP),it is a new reliable ,message – oriented transport layer protocol. It is mostly designed for internet application. SCTP provides enhanced performance and reliability. Actually it has the best features of UDP and TCP. SCTP preserves the messages boundaries band and also detects data loss, duplication of data and out-of-order data. It also has congestion control and flow control mechanisms.

SCTP services *utilized in* Application layer processes—
i) Process -to-process communication-SCTP uses well known ports for communication.

Table 1:- ports for communication

Protocol	Port number	Description
IUA	9990	ISDN over IP
M2UA	2904	SS7 telephony
M3UA	2905	SS7 telephony
H.248	2945	Media gateway
H.323	1718-1720	IP telephony
SIP	5060	IP telephony

ii) Multiple Streams-SCTP allows multistream service in each connection which is called association in SCTP terminology. Idea is of each lane can be used for a different type of traffic.
iii) Multihoming- An SCTP association supports multihoming services. The sending and receiving host can define multiple IP address in each end .In this fault-tolerant approach , without interruption ,when one path fails, another interface can be used for data delivery .
iv) Full Duplex Communication- SCTP offers full-duplex service in which flow of data can be in two direction at the same time. Each SCTP then has a sending and receiving buffer, and packets are sent in both direction.
v) Reliable service- SCTP is a reliable transport protocol ,it uses an acknowledgment mechanism to check data safe arrival in transmission .
vi) Connection-oriented service-SCTP is a connection-oriented service. When a process a site A wants to send and receive data from another process at site B.

SCTP Feature:
1) Transmission Sequence Number (TNS)- The unit of data in SCTP is a DATA CHUNK which may or may not have a one to one relationship with the message coming from the process because of fragmentation. Data transfer in this is controlled by numbering the data chunks. To number the data chunks SCTP uses a transmission sequence number.
2) *Stream Identifiers*-In SCTP may be several streams and each has it identified by using a stream identified (SI). Stream identified is present in data chunk header so when it reach to destination, placed correctly in its stream.
3) *Stream Sequence Number (SSN)*- SCTP uses SSN, When a data chunk arrives at the destination to distinguish between different data chunks belonging to the same stream.
4) *Packets*-SCTP is different, here data chunks carried data only and control chunks carried control information. Several control chunks and data chunks can be together in a packet.

Source port address	Destination port address
Verification tag	
Checksum	
Control Chunks	
Data Chunks	

Fig-2: A packet in SCTP

5) Acknowledgment Number-SCTP acknowledgment numbers are chunk-oriented. In SCTP acknowledgment number are used to acknowledgment data chunks only and the control information is carried by control chunks, which do not need a TSN.

vii) Flow Control- SCTP implements flow control to avoid overpower the receiver. In this we need to handle two units of data, the byte and the chunk. In bytes the values of rwnd and cwnd are expressed; in chunks the values of TNS and acknowledgement are expressed.

Receiver site—

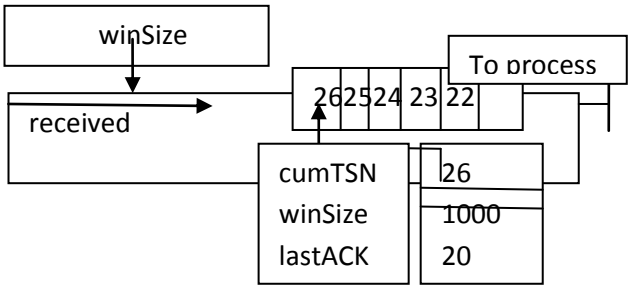

Fig 3:-Flow control on receiver site

1. When the site receives a data chunk,it stores it at the furthest part of the buffer and minus the size of the chunk from winSize . In the cumTSN variable the TNS number of the chunk is stored.
2. When the process reads a chunk,it take away it from the queue and adds the size of the removed chunk to winSize.
3. When the receiver decides to send a SACK, it checks the value of last ACK ;
   If(ACK value < cumTSN) ,it sends a SACK with a increasing by successive TSN number equal to the cumTSN.

3.2 Sender Site

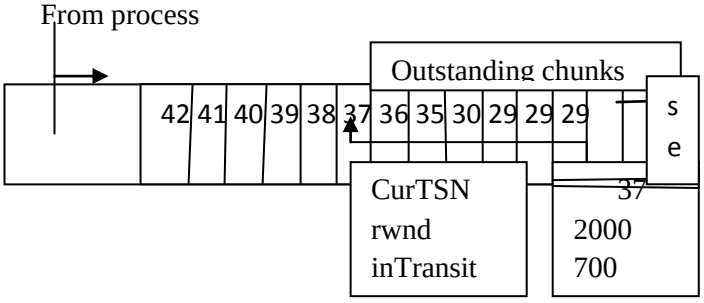

Fig- 4: Flow control on sender site

1. A chunk pointed to by curTSN can be sent **if (size of data <= quantity rwnd- inTransit).** As sending the chunk, the value of curTSN is incremented by 1 and now points to the next chunk to be next chunk to be sent. The value of inTransit is incremented by the size of the data in the transmitted chunk.
2. When a SACK is received, the chunks with a TSN <=l to the cumulative TSN in the SACK are removed from the queue and discarded. The sender does not

have to worry . The value of inTransit is reduced by the total size of the discarded chunks. The value of rwnd is updated with the value of the advertised window in the SACK.

xi)*Error Control*:-SCTP is a reliable protocol ,so for error control it uses TSN numbers and acknowledgment numbers . It uses a SACK chunk to report the state of the receiver buffer to the sender. Each implementation uses totally different set of entities and timers for the receiver and sender sites.

Receiver sites-The receiver site stores all type of chunks that have arrived in its queue as well as the out-of-order ones. It leaves spaces for missing chunks. It also remove duplicate messages, but keeps track of them for reports to the sender.

Sender sites-At this site , two buffer needed : a sending queue and a retransmission queue as well as three variables rwnd, in Transit and curTSN as explain in flow control

x) *Congestion control*—SCTP has the same methods for congestion control as in TCP. Basically there are two main algorithm that used to control over congestion in case of various networks.

a) Leaky Bucket algorithm

b) Token Bucket algorithm

Let have a detail studies about theses above mention algorithm .After that I have try to combine in one place and used it for solving congestion problem in UW-ASNs.

S.No	Features	Leaky bucket	Token bucket
1	Data holding	The buckets holds the data in packets form	The buckets holds the data in token form
2	Handling	When the bucket is full ,excessive packets are discarded	When the bucket is full ,excessive packets are not discarded but keep away to be treated in idle time.
3	Output pattern	It has rigid o/p pattern	It has burstiness o/p pattern
4	Output rate	In this o/p rate remains constant	In this o/p rate not remains constant
5	Credit	It does not credit an idle host although the bucket becomes empty	It do credit an idle host for the future in form of token
6	Speed	Impossible to speed up the output at the time of necessary	Its possible to speed up the output at the time of necessary(burst y data arrives)
7	Time period	It need long time to work	It need less time as one token may contain many packet to send
8	Transmission	In this at every clock tick one packet is transmitted	In this tokens generated by a clock at the rate of one token every DT sec.
9	Depend on	It never depends on type of bursty data traffic	It depends on type of bursty data traffic
10	Applicability	Not applicable for large, and high speed o/p needed applications	Applicable to almost all types of application
11	Traffic shaping rate	It shapes by averaging the data rate by converting the bursty into fixed .	It shapes bursty traffic at a regulated maximum rate

1. Initialize a token to t = 0,each time
   t = t + 1, And
   a counter n, n = n + 1.
2. As unit data sent and decremented the counter by 1.
3. As n = 0 (the host cannot send data), the counter need to be reset and go to step 1.

Algorithm for Leaky bucket—

1. Initialize a counter to *n* at the tick of the clock.
2. If (*n* > size of the packet), send the packet and decrement the counter by the packet size. Repeat the step until *n* < the packet size.
3. Now the counter need to reset and go to

Proposed Suggestion

By combing Leaky bucket and Token bucket algorithm into one we can form a new algorithm which help to solve many of the problem related to underwater sensor networks like, congestion control as the above mention algorithm are basically used as congestion control algorithm.

Here we can combine to get credit an idle host and regulate the traffic .so none of the packets will be discarded, packet or data loss can be prevented as well as regulates the traffic so accurate, reliable and complete data can reach to their destination.

For this we need to do two important things:-
a) The rate of Leaky bucket must be greater than rate of token added in the token bucket.
b) While combining the two algorithm, first apply the token bucket (so all packet can collected , non will discarded)secondly

Leaky bucket algorithm (although burstiness o/p patterns are coming from first applied can be regulated by average output rate).

Algorithm for Token Bucket –

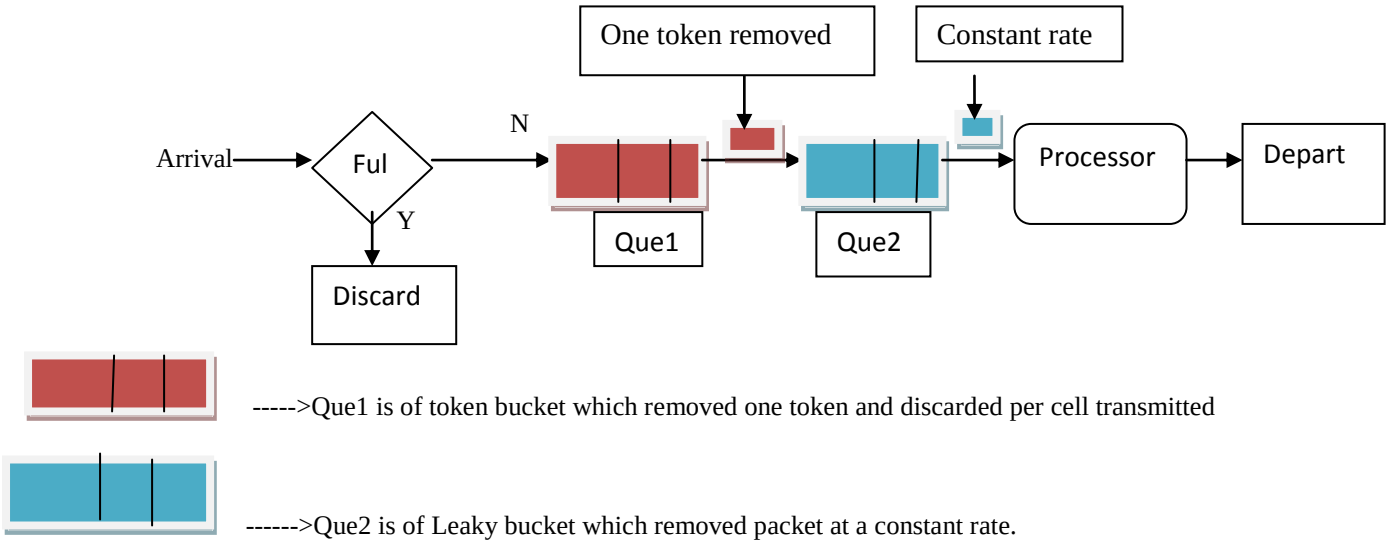

Fig- 5: TLB Traffic shaping Block Diagram

4. CONCLUSIONS /FUTURE WORK

In this paper, we overviewed the main challenges for perfect and accurate data communications in underwater acoustic sensor networks. We outlined the problem of the underwater channel with particular reference to networking solutions for monitoring applications of the ocean environment. The ultimate objective of this paper is to encourage research efforts to lay down fundamental basis for the development of new advanced communication techniques for accurate and efficient underwater communication and networking for enhanced ocean monitoring and exploration applications.

REFERENCES

[1]. I.F. Akyildiz, W. Su, Y. Sankara Subramanian, E. Cayirci , “Wireless sensor networks: A survey, Computer Networks” 38 (4) (2002) 393–422.

[2]. P. Bose, P. Morin, I. Stojmenovic, J. Urrutia,” Routing with guaranteed delivery in ad hoc wireless networks”, ACM Wireless Networks 7 (6) (2001) 609–616

[3]. T. Melodia, D. Pompili, I.F. Akyildiz, “Optimal local topology knowledge for energy efficient geographical routing in sensor networks”, in: Proceedings of IEEE INFOCOM_04, Hong Kong SAR, PRC, and March 2004.

[4]. D.N. Kalofonos, M. Stojanovic, J.G. Proakis, “Performance of adaptive MC-CDMA detectors in rapidly fading Rayleigh channels”, IEEE Transactions on Wireless Communications 2 (2) (2003) 229–239.

[5]. L. Freitag, M. Stojanovic, S. Singh, M. Johnson, “Analysis of channel effects on direct-sequence and frequency-hopped spread-spectrum acoustic communication”, IEEE Journal of Oceanic Engineering 26 (4) (2001) 586–593.

[6]. E.M. Sozer, M. Stojanovic, J.G. Proakis, “Underwater acoustic networks, IEEE Journal of Oceanic Engineering” 25 (1) (2000) 72–83.

[7]. M. Stojanovic, "Acoustic (underwater) communications", in: J.G. Proakis (Ed.), Encyclopedia of Telecommunications, Wiley , New York, 2003.
[8]. M. Stojanovic, J.G. Proakis, J. Catipovic, "Performance of high-rate adaptive equalization on a shallow water acoustic channel", Journal of the Acoustical Society of America 100 (4) (1996) 2213–2219.
[9]. F. Salva-Garau,, "Multi-cluster protocol for ad hoc mobile underwater acoustic networks", in: Proceedings of IEEE OCEANS_03, San Francisco, CA.
[10]. O.B. Akan, I.F. Akyildiz," Event-to-sink reliable transport in wireless sensor networks", IEEE/ACM Transactions on Networking, in press