Journal of Korea Multimedia Society Vol. 18, No. 4, April 2015(pp. 506-523)
http://dx.doi.org/10.9717/kmms.2015.18.4.506

Custody Transfer of Bundle layer in Security Mechanism for Underwater Internet of Things (UIoT)

Khamdamboy Urunov[†], Jung-Il Namgung[††], Soo-Hyun Park[†††]

ABSTRACT

The intent is to determine whether or not the custody transfer is helpful for data transmission in challenging underwater communications when running Bundle protocol or underwater protocols. From the point of view defending side, Underwater Acoustic Network (UAN) will be a serious threat for its strong functionality long rang and high precision of surveillance and detection. Therefore, countermeasures must be taken to weaken its effect. Our purpose is analyzed that how to benefit from the UIoT to learn from, exploit and preserve the natural underwater resources. Delay/Disruption Tolerant Network (DTN) is essential part of the network heterogeneity communication network. The vulnerability and potential security factors of UIoT are studied thereafter. Security mechanisms for an underwater environment are difficult to apply owing to the limited bandwidth. Therefore, for underwater security, appropriate security mechanisms and security requirements must be defined simultaneously. The paper consists of mathematical and security model. Most important point of view in the security challenges of effective Buffer and Storage management in DTN.

Key words: Internet of Things (IoT), Underwater Internet of Things (UIoT), Delay/Disruption Tolerant Network (DTN), Bundle layer, Security challenges, Custody transfers, Underwater Acoustic Network (UAN)

1. INTRODUCTION

Those natural facts are always confirmed by humanity. The oceans regulate and determine climate on a global scale, and it is a fact that major disasters happen when climate is deregulated: cyclones, storms, and coastal flooding. Indeed, modern technology and high quality internet have turned into an optional feature of the people. At the moment, great deal of people know and accurate use internet [1-3]. The Internet is being the most well-known example of the network. In the case, connectivity on the Internet relies primarily on wired links, underwater communication, including wired telephone networks, although wireless technologies such as satellite and short range mobile links are also as essential part of the network. The most important part of things used on the internet, are continuously connected to end-to-end, low-delay paths between sources and destinations. Internet was born in a domain of mutual trust, being the initial network based on a closed world of trusted parties protecting themselves against the outside world [4,5]. It's known that people strives communication network to all over the world and even in the galaxy. In the future mean point of the

※ Corresponding Author : Soo-Hyun Park, Address: Kookmin University, 77 JeongungRo, Sungbukgu, Seoul Korea, TEL : +82-2-910-4559, FAX : +82-2-910-4519 , E-mail : shpark21@kookmin.ac.kr
Receipt date : Mar. 7, 2015, Revision date : Apr. 2, 2015
Approval date : Apr. 19, 2015
[†] Department of Financial Information Security, Kookmin University, Seoul, South Korea
(E-mail : hamdamboy.urunov@gmail.com)
[††] Department of Financial Information Security, Kookmin University, Seoul, South Korea
(E-mail : greenji@naver.com)
[†††] Department of Financial Information Security, Kookmin University, Seoul, South Korea
※ This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R1A1A2012461).

high quality network and to order reliable communication everywhere, each step. Let's attention: IoT, UIoT and Interplanetary communications. Likewise heterogeneous communication network provides DTN, and Delay-tolerant networking is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Nowadays the Internet of Things are already a global phenomenon that is going to change our everyday life as much as our life was already revolutionized with the global use of Internet itself. There are several ways of employing such communication but the most common is using hydrophones. Most of the cetacean emit high-pitched whistles or squeals who pitch varies from 1k to 10k Hz. Speed of sound in air is about 330m/s, but in water the speed is 1500m/s which is 4.5 times faster that in air. A sound wave doesn't stop when it reaches an obstacle. It has some very useful properties like reflection, diffraction and transmission through a medium. In this paper focus on underwater communication via DTN mechanism and security possibility. So, explanation more details Custody transfer, Persistent storage, security, layer model, Bundle layer possibility. Main goal in our paper calculated each nodes storage with security mechanism. If security enforced to custody transfer mechanism a data exchanging more secure than enough.

2. CUSTODY TRANSFER OF DTN MECHANISM

DTN is considered a suitable technology for challenging communications in the underwater communication operations environment. A key point of the DTN architecture is the "custody transfer" option.

A store-and-forward transmission mechanism and a custody transfer option are among the techniques offered by DTN Bundle Protocol (BP) for dealing with challenging communication [6,7]. The store-and-forward mechanism is adopted to combat link interruption: DTN can suspend data transfer during intervals of disconnection and resume transmission when connectivity is restored.

2.1 DTN mechanism of Bundle layer reliable transfer

The custody transfer option enables DTN nodes to act as "custodian", responsible for guaranteeing the reliable forwarding of data towards the destination. The combination of two mechanisms expected to ensure that no data packets are lost even if a router is temporarily out of sight due to occultation or rotation in space and underwater area. However, to date no quantitative investigation has been done to evaluate the performance enhancement provided by custody transfer in underwater communication. DTN mechanism has conceptual feature depicted in below side.

Most essential of DTN mechanism provides Heterogeneous network:

- Heterogeneous network (HN)

A heterogeneous network (HN) is a network connecting computers and other devices with different operating systems and/or protocols [8,9].

The precision for determining the direction of a GRB in the sky is improved by increasing the spacing of the detectors, and also by more accurate timing of the reception. Domination of communication area depicts over a Fig. 1 "Underwater communication via DNT Getaway". This communication sphere is on Space, Earth and Underwater. Scope of our paper oriented underwater congestion. Even though of the underwater acoustic network (UAN) or underwater environment consists of different or mix topology. As well as this topological method several type of cluster, ad hoc and mesh network and others. The above-mentioned depicted of the Fig. 1 invokes abbreviation of the paper. Several kind of underwater communication skill included relay nodes, DTN Getaway and underwater acoustic sensor node (UWA-SN), under-

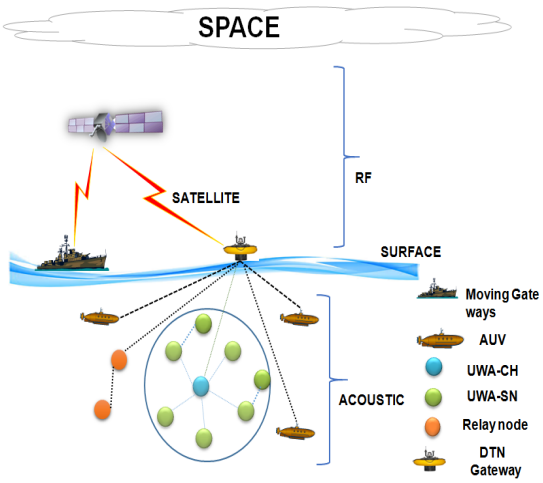

Fig. 1. Underwater communication via DNT Getaway.

water acoustic cluster header (UWA-CH), underwater vehicles (AUV). So then in this case remote environment spaces high bandwidth and opposite case is underwater low bandwidth more propagation delay and disruption.

At the present next step represent layering process. Others, Moving Gateway and Horizontal multi-hop link, Underwater DTN Gateway (UWA-DTN-GW), Vertical link adhered in the Fig. 1. Underwater communication medium is, however very challenging since the usable frequency band (bandwidth) is limited and the ocean is extremely reverberant. The combination of limited bandwidth and reverberation (multi path) makes it difficult to design underwater communication systems. The type of communication system includes Internet of Things and Underwater Internet of Things. The bundle layer is ongoing enforce to heterogeneous network, and Bundle. It means one more layer of bundle is adhering in layer model. In addition, key point is things/underwater things. Indeed, things is composed of network area technical instrument or appliances, layer model includes IoT and UIoT. It can uses bundle layer in getaway on Fig. 2. communication via Bundle layer, heterogeneous network uses DTN getaway. So, in Fig. 2. (left) side has IoT and communication layer model joined Bundle layer. The Bundle custody transfer en-

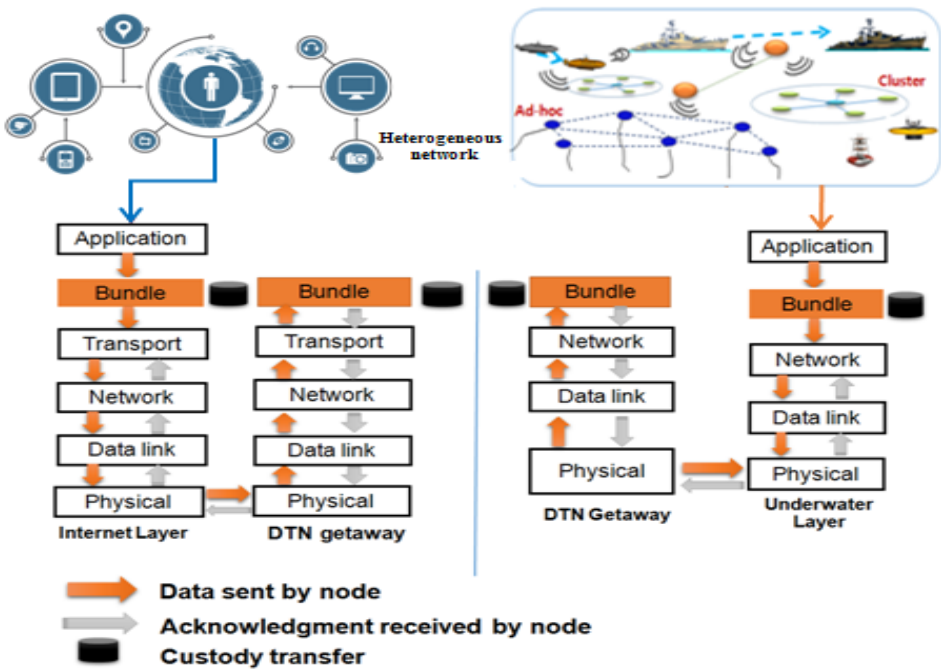

Fig. 2. DTN Bundle layer on heterogeneous network.

forces heterogeneous internet network. By the way, it depicted Fig. 2. (right) side underwater communication environment are composed type of Underwater things.

That means extra level adds layer model, it called Bundle layer. Actually, Fig. 2 gives information of the Bundle layer for layering model. The next part of the paper, we will describe DTN custody transfer and Persistent mechanism.

2.2 DTN functionality (Custody transfer and Persistent storage)

The custody transfer of the DTN architecture has specified only a coarse-grained re-transmission capability. Bundle protocol (BP) incorporates an optional feature called custody transfer, in order to offer reliable hop-by-hop transmission to the final destination. According to custody transfer mechanism, bundles are transmitted in a "store-and-forward" technique while the responsibility of reliable transfer is delegated to the next node in a route towards the final destination [10]. A node which receives custody of the Bundle is called custodian. The custodian node must forward the bundle to a neighboring node requesting custody transfer. The neighboring node will reply with a custody acceptance or custody refusal signal, according to its admission control policy. Afterwards acknowledgement (ack) receipted. So, sometimes even if a router or DTN intermediate node thinks a link is up a packet or bundle can still lost enroute. The ability to forward the bundle to the final destination before Time-to-live (TTL) expiration and resource availability, are the basic criteria each receiving node evaluates. In the Fig. 3. depicted data transmission via custody transfer, that process includes several intermediate nodes. For example: a cluster intermediate node **Node#A** and a cluster intermediate node **Node#B, Node#C,** DTN gateway or a moving gateway. In case the one of them (**Node#A** or **Node#B, Node#C**), a node does not receive a reply within a specific time interval, a timer triggers the bundle's re-transmission, possible through a new route.

The custodian is obligated to store bundle until the reception of custody acceptance signal upon which the bundle is discarded, or until expiration of bundle's lifetime. Hence, DTN mechanism means

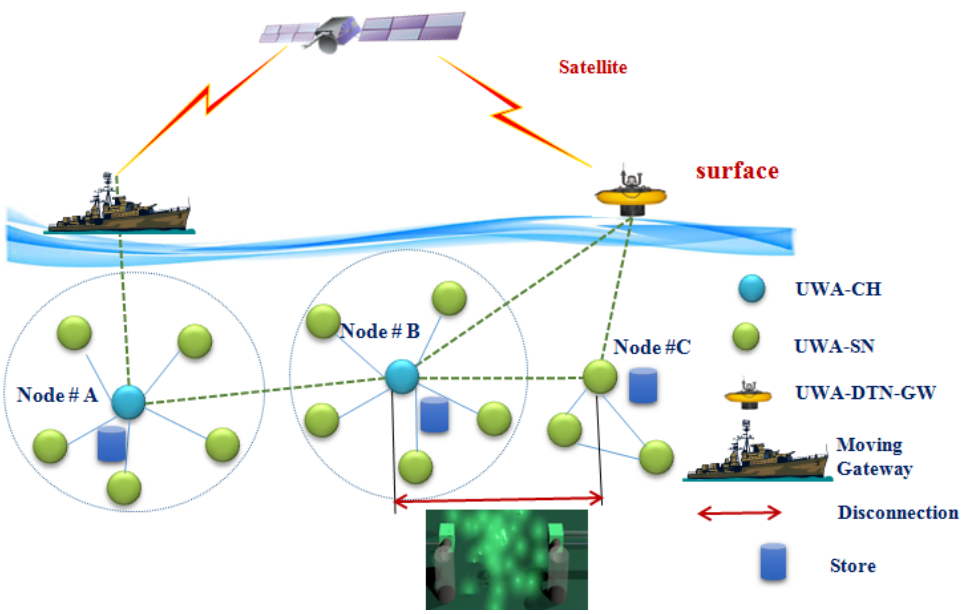

Fig. 3. Underwater communication disconnection and reduce quality possibility.

of functionality the Custody transfer. In this paper underwater cases different network communicate each other, as well as ad hoc and cluster header or mesh network when hop-by-hop transfers of reliable delivery responsibility. Above the mentioned heterogeneous network consists of several type of disconnection, disruption, lose signal or up going noise (more noisy) waves and others. In this Fig. 3 has a red disconnection arrow, is swapping through a Node#C and a Node#B intermediate cluster header optional determined when distribute DTN mechanism. If an intermediate node Node#B sends a data to an intermediate node Node#C, but the intermediate node Node#C receipt 80% data (for instance take this number), remaining data has lost. Custody mechanism helps to get a data which is remaining the data. That figure is base on storing and forwarding method. The communication area has DTN mechanism which a remaining data or a lost data can update that area. Other case, a data 80% also rejected (see Table 2). The mechanism is called DTN custody transfer mechanism.

All-inclusive a detail of custody transfer of DTN mechanism. In the Fig. 4. depicted data transmission via custody transfer that processes an intermediate node **Node#A** and an intermediate node **Node#B**. In case the custodian node does not receive a reply within a specific time interval, a timer triggers the bundle's re-transmission, possible through a new route. The custodian is obligated to store the bundle until the reception of custody acceptance signal upon which the bundle is discarded, or until the expiration of bundle's lifetime.

More essential point three parameters copy, buffer and forward. Hence, DTN mechanism means of functionality the Custody transfer. In this paper underwater case different network communication each other, ad hoc and cluster header or mesh network when hop-by-hop transfer of reliable delivery responsibility. Underwater communication case has more disconnection and disruptions. It is possible to use DTN mechanism and a node Node#B arrow (Fig. 4) uses DTN technology number of conceptual steps and consensus statements. Other part of this paper has more details buffer mechanism.

Likewise, water has a very high attenuation of radio waves, which requires extremely low frequencies. But low frequencies require long antennas, which are almost impossible to use. Usually

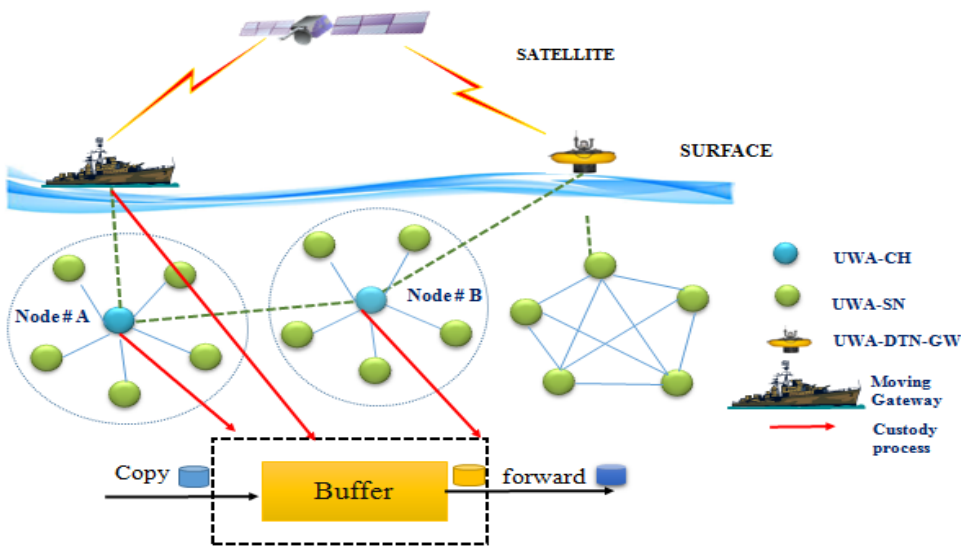

Fig. 4 DTN feature of Custody transfer mechanism.

submarines surface or get close to the water surface for radio communication.

Persistent storage may be used Underwater DTN routers need persistent storage for their queues for one or more of the following reasons. The Underwater Bundle protocol is specification different entities. Persistent storage is used in DTN nodes to accommodate data in cases of intermittent connectivity. The time space between two data transmissions may be long and usually varies during the connection. Using persistent storage [11], the Bundle protocol manages to resolve most of these issues. Instead of storing packets in a temporary buffer, a DTN node stores packets permanently to a local storage unit. A data will be transmitted when the next hop is available and may be retransmitted several times, if the transmission fails. Fig. 5. shows Persistent storage functionality. Persistent storage, however, has a significant drawback: it increases the communication overhead as it adds a processing delay which results by moving the data from buffer to persistent storage and back to buffer.

Although most of the time this delay is negligible, there are cases where two intermediate nodes may be engaged in continuous low-delay transmissions. Persistent storage has such kind of

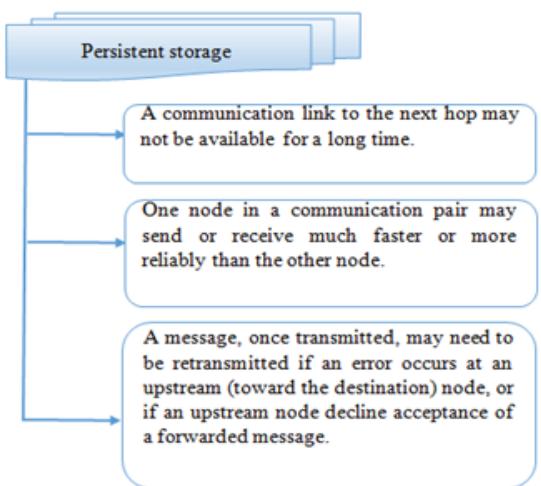

Fig. 5. Persistent storage on DTN mechanism for UIoT.

functional mechanism for Underwater Internet of Things. Next part of the paper consists of persistent storage mechanism and mathematical model, afterwards algorithmic function. In this Fig. 5. main link up advantages and disadvantages in shown. Top of the Fig. 5. gives detail about underwater link disruption an intermediate Nodes (simple example: a **Node#A** and a **Node#B; send data; data bundled-custody transfer use persistent storage; acknowledgment**). The middle part of the Fig. 5, if functional method is working well, communication pair maybe send and receives faster than enough. As well as bottom side of the last communication process, if accepted data (maybe for acceptances not 100%, it would be 68% or less, just guess) gets to receiver (here a **Node#B** asks from a **Node#A**) forwards part of the data. While the whole process of data transmission will be done.

2. 3 Characteristics of UIoT

UIoT can approach two objects: Things and IoT.

Generally, **the Internet of Things (IoT)** refers to the interconnection of uniquely identifiable embedded computing-like devices within the existing Internet infrastructure [11]. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers variety of protocols, domains, and applications.

Typically, Things is some kind of devices, appliances which communicate to Internet. In this part devices are computers, mobile devices, laptops, smart watch, and other smart devices.

Indeed, the **Underwater Internet of Things (UIoT)** is defined as a world-wide network of smart interconnected underwater objects that enables to monitor vast unexplored water areas. The purpose of this paper is to analyze how to benefit from UIoT to learn from, exploit and preserve the natural underwater resources. In this paper, UIoT

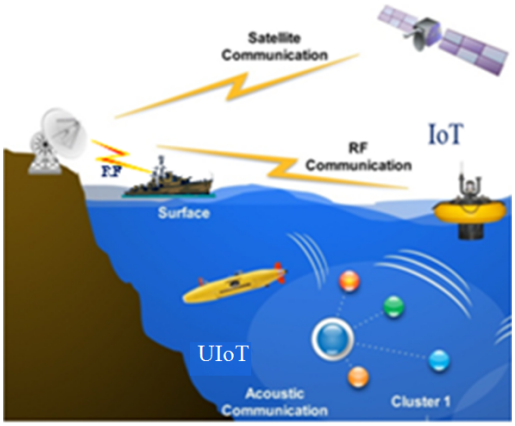

Fig. 6. Connection between IoT and UIoT.

is introduced and its main differences with respect to IoT are outlined.

This is why, IoT and UIoT have relationship for the communication area. As shown in Fig. 6, DTN Gateway connects IoT and UIoT.

Internet communication network system is suggestion underwater side all nodes and buoys, ships called underwater things. For any location based routing, most of the protocols require and manage full-dimensional location information of the sensor nodes in the network, which is also a challenge to be solved for UIoT. Most of the routing protocols, even for terrestrial or underwater sensor networks, use separate packets for control information and data transmission.

3. SECURITY ANALYSIS BASED ON DTN MECHANISM OF UIOT

People concerns about privacy are indeed well justified. Public or Private users or exploiter should use to communication products (mobile, computer, laptop, drone, and other devices), everyone is interesting product quality and security privacy. Even though, modern technologies do not get abiding security channel. IoT or UIoT stables concern. In DTN mechanism case, DTNs themselves do not appear to generate many new types of policy-based controls – the usual ingress, egress and forwarding types of control can all be applied in DTNs. No doubt, more will be identified as more DTN deployment experience is gained. In Underwater environment are exposed of several problems and tackle the problems.

3.1 Security challenges of DTN mechanism

Security challenges described several steps for Underwater communication. No doubt, DTN networks can be thought of as operating across varying conditions across several different axes, depending on the design of the subnet being traversed:

1. Low or high propagation delay;
2. Dedicated or shared, congested links;
3. Links with intermittent disruption and outages or scheduled planned connectivity;
4. Bandwidth is extremely limited. The attenuation of acoustic signal increases with frequency and range. Consequently, the feasible band is extremely small. For instance, a short range system operating over several tens of a hundred kHz; a medium-range system operating over several kilometers has a bandwidth on the order of ten kHz; and a long-range system operating over several ten kilometers is limited to only a few KHz of bandwidth;
5. Probability of bit error is much higher and temporary loss of connectivity (shadow zone) sometimes occurs, due to the extreme characteristics of the channel.

The bundle security protocol is still very much a work-in-progress and there are some significant open issues remaining to be determined. The DTN bundle security protocol specification [12-16] defines basic data integrity and confidentiality mechanisms for bundles. The approach defines two different data integrity blocks: one for end-to-end integrity, and a separate one for hop-by-hop integrity (between adjacent DTN nodes). Cryptographic protection at the bundle layer may not be

necessary in these network segments. For these reasons, DTN security allows for intermediate DTN nodes (between the source and destination) to apply or check the validity of the cryptographic credentials. The relevant nodes in these cases are referred to as the security source and security destination, respectively, which can differ from the bundle source and destination. In this part Fig. 7. depicted underwater attack and challenges. Let's consider of several attacks underwater communication. Briefly explain each attack in below side.

Jamming attack: consists of interfering with the physical channel by putting up carriers on the frequencies neighbor nodes use to communicate [17]. Since underwater acoustic frequency bands are narrow (from a few to hundreds of kilohertz), Underwater communication is vulnerable to narrow band jamming. Localization is affected by the replay attack when the attacker jams the communication between a sender and a receiver, and later replays the same message with stale information (an incorrect reference) posing as the sender.

Sybil attack: an attacker with multiple identities can pretend to be in many places at once. Geographic routing protocols are also misled because an adversary with multiple identities can claim to be in multiple places at once. Authentication and position verification are methods against this attack, although position verification in Underwater Acoustic Network is problematic due to mobility.

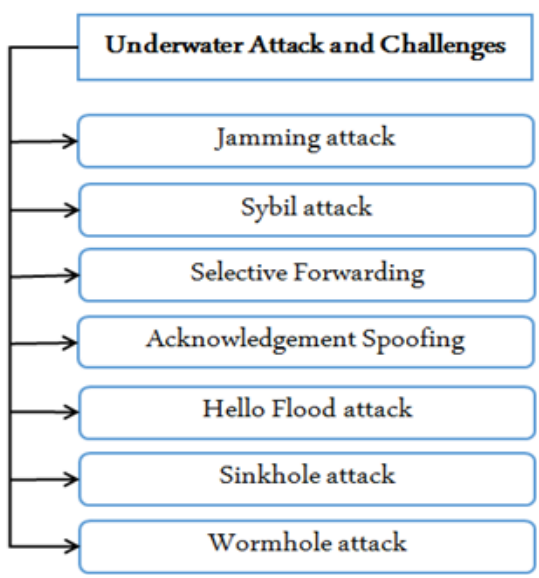

Fig. 7. Underwater attack and challenges.

Selective Forwarding: Malicious nodes drop certain messages instead of forwarding them to hinder routing. In Underwater network it should be verified that a receiver is not getting the information due to this attack and not because it is located in a shadow zone. Multipath routing and authentication can be used to counter this attack, but multipath routing increases communication overhead.

Acknowledgment spoofing: A malicious node overhearing packets sent to neighbor nodes can use this information to spoof link layer acknowledgments with the objective of reinforcing a weak link or a link located in a shadow zone. Shadow zones are formed when the acoustic rays are bent and sound waves cannot penetrate. They cause high bit error rates and loss of connectivity. This way, the routing scheme is manipulated. A solution to this attack would be encryption of all packets sent through the network.

Hello flood attack: A node receiving a HELLO packet from a malicious node may interpret that the adversary is a neighbor; this assumption is false if the adversary uses high power for transmission. Bidirectional link verification can help protect against this attack, although it is not accurate due to node mobility and the high propagation delays of underwater network. Authentication is also a possible defense.

Sinkhole attack: In a sinkhole attack, a malicious node attempts to attract traffic from a particular area toward it; for example, the malicious node can announce a high-quality route. Geographic routing and authentication of nodes exchanging routing information are possible defenses against this attack, but geographic routing is still an open

research topic in underwater network.

Wormhole attack: A wormhole is an out-of-band connection created by the adversary between two physical locations in a network with lower delay and higher bandwidth than ordinary connections. This connection uses fast radio (above the sea surface) or wired links to significantly decrease the propagation delay. In a wormhole attack the malicious node transfers some selected packets received at one end of the wormhole to the other end using the out-of-band connection, and re-injects them into the network. The effect is that false neighbor relationships are created, because two nodes out of each other's range can erroneously conclude that they are in proximity of one another due to the wormhole's presence. This attack is devastating. Routing protocols choose routes that contain wormhole links because they appear to be shorter; thus, the adversary can monitor network traffic and delay or drop packets sent through the wormhole. Localization protocols can also be affected by these attacks when malicious nodes claim wrong locations and mislead other nodes. Above the mentioned all attack and issue accusers in the Underwater communication.

3.2 Security challenges of effective Buffer and Storage management in DTN

The above-mentioned security cryptographic protection at the bundle layer may not be necessary in these network segments. Hop-by-hop or end-to-end communication network has many obstacles or problems, as understand that is not easy solving problem. Although we are exploring in the sphere (underwater network), it helps to reduce issues, thats' way not increasing weak point of the network communication. In this paper, we consider an intermediate node which acts an intermediate to several flows. Packets of several senders enter the node at various instances. The flows can be identified either by the protocol addresses (example, IP addresses) of the sender and receiver, if IP is used, or by the endpoint ID [18]. In the first case, the packets arrive back-to-back with constant inter arrival times, and in the second case, in a stochastic manner. The node then has to keep them until a connection opportunity occurs, or until its storage space is full. Each node has a buffer and a persistent storage unit, both limited. The buffer consists of two queues; a low-delay traffic (LDT) queue and a high-delay traffic (HDT) queue. Fig. 8 shows the control model. There is a **Node#A** send to data other a hop or a node, so most important point is not in this case lost or reduce data integrity. In this process storage management model which persistent mechanism each other data exchanges. Note that at this point we do not determine the sizes of the two queues. In this paper we assumed size, their sizes can be either defined at the beginning, or vary as the correlation of traffic changes. Custody transfers are also stored in persistent storage. The aggregate incoming rate is noted as λ from a **Node#A**. The Policy Unit is to accept all the bundles that enter the node (here instance a **Node#A**) and, depending on the conditions, move them to buffers or storage.

Buffer and Storage control (management) is initially differentiated based on whether there is connectivity between the DTN node and the next-hop. During periods of connectivity, packets that enter a node may be immediately routed to the output without being stored first. The total sending rate is calculated by the sum of sending rates of the Low-delay traffic queue or High-delay traffic queue.

Low-delay traffic (LDT) queue The Policy unit moves bundles to the Low-delay traffic queue only when there is connectivity and therefore the corresponding bundles can be forwarded to the next node. After a time-period which is determined by some threshold, when no connectivity exists, bundles that are stored temporarily in the LDT queue move to Persistent storage.

Persistent storage The Policy unit moves bundles to Persistent storage in three cases:

a) When there is no connectivity;

b) When there is connectivity but no LDT space available;

c) When there is both connectivity and LDT space available, however the contact graph, which is known a priori, instructs that time does not suffice to forward bundles to the next hop.

High-delay traffic (HDT) queue Bundles are moved from storage to the Non Connectivity buffer in the following two cases:

a) When bundles are of high priority (are either urgent or a scheduled contact is expected) and there is no connectivity;

b) When there is connectivity but other bundles are selected to be forwarded (opportunistic contact). The algorithm that determines which bundles should be forwarded first at a given communication opportunity is described briefly in the Scheduling section.

If the packet belongs to a high delay flow, it will be moved immediately to persistent storage, unless there is a communication opportunity. In this case it will be moved to the HDT buffer. Packets that exist in persistent storage are allowed to move to the HDT buffer, only when the next hop for the corresponding flow becomes available. The total service rate μ results by multiplying the output of the two queues with a Weighted Fair Queuing [19-20] multiplexer. Details of the WFQ mechanism are still an open issue. Summarizing, moving packets from buffer to storage and back, is allowed only in the following three cases:

1) From LDT buffer to persistent storage. Packets that can move in this direction are either new packets that belong to a high-delay flow, or old packets that belong to a low-delay flow and the LDT buffer is full.

2) From persistent storage to HDT buffer. Packets that can move in this direction are packets that were previously in persistent storage and currently they have a communication opportunity.

3) From LDT buffer to HDT buffer upon packets arrival. Packets belonging to a high-delay flow, will move to HDT buffer if there is currently a communication opportunity with a next hop. There is, however, a very rare case where packets would need to move from HDT buffer to persistent storage. This would happen when there is a communication opportunity, which lasts less time than the time required to move the packets from persistent storage to HDT buffer and commence transmission. Packets which were transferred to HDT buffer would have nowhere to go and should be moved back to storage. Nevertheless, this is a special case that is unlikely to happen, given the high processing capabilities of current computers. Clearly, special case this is not security property of the Fig. 8. The buffer and Storage control model. The above-mentioned Fig. 7. has several attacks. Other more challenges are masquerade attack. If we get good quality connection any problem is security part of weak like unattended.

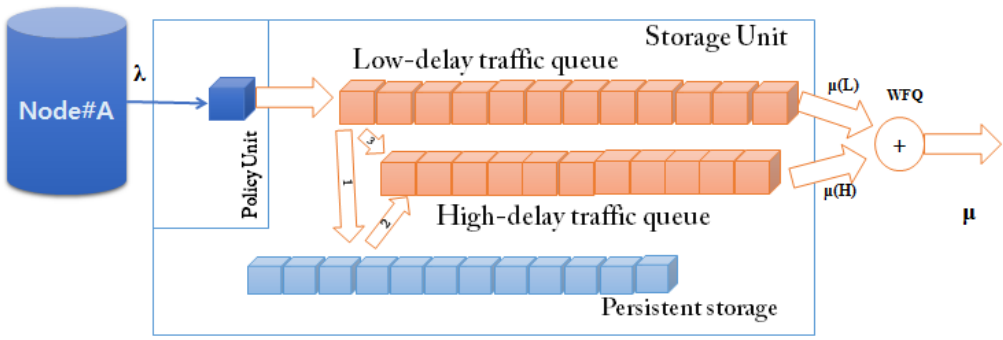

Fig. 8. The buffer and Storage control model.

3.3 Mathematic model and algorithm effective Buffer and Storage management for UIoT

No doubt, Schedule or Time synchronization is even most important for underwater acoustic communication. Time synchronization is even more important in sensor networks, where applications such as acoustic beam forming and target tracking require collaboratively processing of time-sensitive data. This part consists of mathematic model and algorithm for underwater communication. Likewise, sensor networks add the additional requirement that energy consumption of the synchronization protocol be minimized. Many time synchronization protocols for sensor networks have been proposed recently. These mechanisms provide a high degree of precision while being reasonably energy efficient. The protocols adopt increasingly sophisticated approaches to reduce noise and account for latency in communications, but all assume that propagation latency is negligible and thus can be effectively factored out of design consideration.

Scheduling: Scheduling unit reassign the priorities for each bundles should be outputted from the DTN node when a communication opportunity occurs. A priority-oriented model should be inevitable considered; this model should incorporate application requirement, data requirements, Time-to-Live (TTL) for bundles etc. In our mathematical abbreviation includes Table 1.

In this case, table-1 and mathematical analysis belong to Fig. 8. Indeed, flows that have less average storage delay than the total average are characterized as low-delay flows, whereas the rest are characterized as high-delay flows. Assuming N flows passing through the node, we have:

$$\Delta T_{InOut} = t_{out} - t_{in} \quad (1)$$

$$\Delta T_{average} = \frac{N-1}{N} * \Delta T_{average} + \frac{1}{N} * \Delta T_{InOut} \quad (2)$$

$$\Delta T_{Diff} = \frac{\sum_{i=1}^{N} \Delta T_{average}}{N} \quad (3)$$

So, (2) N= 12, in persistent storage and low-delay transfer value the same.

$$\Delta T_{average} = \frac{N-1}{N} * \Delta T_{average} + \frac{1}{N} * \Delta T_{InOut}$$
$$= \frac{11}{12} * \Delta T_{average} + \frac{1}{12} * \Delta T_{InOut} \quad (4)$$

Summarizing moving packets and data flow from buffer to storage and back is allowed only three cases. (1) Every packet; (2) Every flow; (3) Result average value for delay.

Mathematical formula (1) is called every packet. That means a Node#A is sending or receipting data from other a Node#B or others. As well as data is forwarding and receipting period totally different, as we are expecting. Time synchronization also includes here. So time is difference if a data receipt (here buffered and persistent) and forwarding. Next formula (2) has counted how many packet flows and maximum size of a data storage in an intermediate node (**Node#A**). (3) one is differences. And than average of delay packet. Last one is time average (4) of whole packet which is receipting and forwarding. Achieve less processing delays in a

Table 1. Distinguishing Low- and High-Delay Traffic

Title	Entity
t_{in}	Packet enters the node
t_{out}	The time it leaves
ΔT_{InOut}	The difference of these two times
i	The time period where the packet remains in the node, either in buffer or persistent storage. For each flow.
$\Delta T_{average}$	Weighted moving average of storage delay
ΔT_{Diff}	The average value of all flows' storage delays gives the average storage delay of the system.
N	Flows passing through the node

DTN network. It has several open issues. Determine the size of LDT and HDT queues. Should they be statically defined, or it is preferable to obtain values depending on the network load. Review the WFQ scheme used to multiplex the outputs of the two queues. This will also define the bandwidth that each type of traffic will possess. Failure to do so and we will end up in under-utilization.

4. Security opportunity of Mathematic model and algorithm effective Buffer and Storage management for UIoT

The current Underwater Bundle Protocol specification does not address reliability, in that it has no checksum support for error detection and rejection of corrupted bundles. That means that one cannot determine if the bundle information received at each node was received error-free or not. Error detection is a very basic networking concept that was overlooked in the Underwater Bundle Protocol design. The design of the bundle architecture completely ignores the well-known end-to-end principle. Without useful error detection, the Underwater Bundle Protocol's custody transfer mechanism cannot guarantee that a node taking responsibility for final delivery of a bundle has actually received an uncorrupted copy of that bundle to send on. Leaving error recovery up to the applications is only possible when the applications are tightly coupled across the network, with a tight control loop for resends of eroded data. DTN networks, by their ad-hoc nature, are loosely coupled, and there may not be any direct communication or control loop between applications at end nodes, requiring increased assistance from the network to improve performance - in line with the end-to-end principle.

4.1 Security requirements to Buffer and Storage management involves Encryption algorithm

Security mechanisms for an underwater environment are difficult to apply owing to the limited bandwidth. Therefore, for underwater security, appropriate security mechanisms and security requirements must be defined simultaneously [22-26]. The following are the three requirements to be fulfilled for basic underwater environment security.

Confidentiality: Underwater sensor nodes communicate acoustically. If another entity collects the transmitted data, it can be easy to retrieve the original data. Therefore, the system must be protected from eavesdropping.

Authentication and Integrity: If an underwater sensor node does not require identification or message authentication, an attacker node can easily participate in communication inside the network. If an attack node collects packet information and ID information from wiretapping, communication data can be compromised by data falsification.

Availability: The system should continue to provide robust service even when the network is being threatened by a malicious node.

Indeed, the protocol stack of a UWASN (Underwater acoustic sensor network) or underwater environment is composed of an application layer, bundle layer, transport layer, network layer, MAC layer, and physical layer. If data is sent from an upper layer to a lower layer, the data needs a header added to the payload in each layer. Fig. 9 shows the process of data encryption. The aggregate incoming rate is noted as λ from a **Node#A** (see Fig. 8). In our case λ = DATA, header and new header consist of each layer possibility. The lower layer adds its header, in front of which another new security header may be added. The new security header contains several security parameters for the receiver that needs to retrieve data securely. After adding the headers, the entire message, New_Security_Header - Header - Bundle - Data, is entered into a message-authenticated code algorithm such as AES-CBC-MAC with a shared secret key,

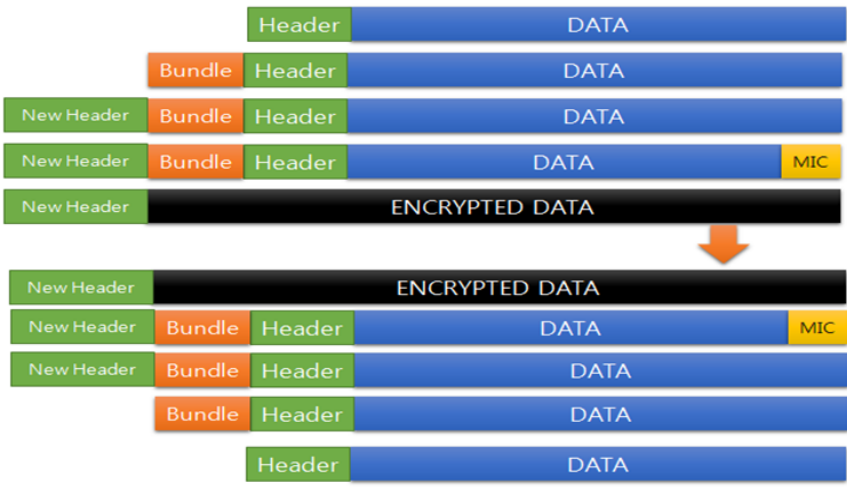

Fig. 9. The process of data encryption.

and the output value message integrity code (MIC) is added at the end of the entire message. The value of the MIC ensures that the every single bit in the entire message including the shared key involved in this calculation is authentic. Then, the receiver having the same shared key recalculates its own MIC value and compares it with that received. If the two MIC values are different, the receiver can discard the entire received message. After adding the MIC value (8-bit, 16-bit, 32-bit, 64-bit, etc.) at the end of the entire message, the encryption algorithm encrypts the data and the MIC. Obviously, the encryption uses both the security header and the new header, but the new header is not encrypted. The receiver follows the process inversely to ensure that all the data is authentic and the entire message is originated from a known device. The data could arrive as a justifiable object that the receiver cannot identify. In this case, the data can be guaranteed safely through the MIC. Additional MIC data can be generated and added to the message. However, in order to ensure stability, it is essential that at least the length of the MIC is used. The next most important issue is applying an encryption algorithm. In this paper, we suggest that a transmitter and receiver use the same key for data encryption and decryption. Symmetric keys are divided into stream and block ciphers. However, for device or user authentication, control data authentication, sensing data authentication, confidentiality, and data availability for UAN, a symmetric key encryption algorithm is the only possible solution. Because the key size of a symmetric key algorithm is relatively smaller than an asymmetric key, a symmetric key-based encryption algorithm such as AES or ARIA is suitable for a lower-powered UAN.

$$M = N * \lambda;$$

However, a symmetric key encryption algorithm used for encrypting plaintext from a cipher key that is also used for decryption has the advantage of speed and is suitable for an underwater communication environment. A UWASN that uses a hash algorithm regardless of the size of the input produces a result of the same size. A hash algorithm is used to encrypt input message of arbitrary length, and other compression functions use a fixed length. However, a cryptographic hash function algorithm features existing one-way functions. We strive to enforce this algorithm above the mentioned is part 3.3. So most important is delay and data integrity. Formula (1) has variable Data, M and others.

Here M-data size. How many data comes a minute to intermediate node.

$$\Delta T_{Diff} = \frac{\sum_{i=1}^{N} \Delta T_{average}}{N} + \sum_{i=1}^{M} \lambda \quad (5)$$

Summarizing moving packets and data flow from buffer to storage and back is allowed only three cases. (5) Every packet difference; **Node#A** forward or receipt data from other **Node#B** or others. As we suggested data forwarding and receipt period totally difference, time synchronization. Delay and disruption time. So time is difference if a data receipt (here buffered and persistent) and forwarding.

Achieve less processing delays in a DTN network. It has several open issues. This algorithm should not be used when the data size is reduced because it does not have the capability of decoding the data and is difficult to use while is sending and receiving.

4.2 Result of Buffer and Storage management consist of DTN mechanism for UIoT

The applications mentioned in the previous sections looks very different at first glance, but when the requirements which enable such applications are analyzed the following characteristics can be derived. Just Table 2. example of process of DTN custody transfer and IP. Acoustic communication has been proven to work much better under water. This technique is used for diver conversation and in scientific applications for underwater sensor communication.

In addition to the aspects of the terrestrial sensor networks, underwater networks suffer a reasonable propagation delay, limited bandwidth and reasonable disturbances. Fig. 10. these problems are

Table 2. Compares protocol

Item	Node#B (send)	Node#C (receiver)	Result
DTN bundle	Data=A 100%	Data=A 80%	80% alive
IP	Data=A 100%	Data=A 80%	0% alive
DTN bundle	Data=A 100%	Data=A 25%	25% alive
IP	Data=A 100%	Data=A 25%	0% alive

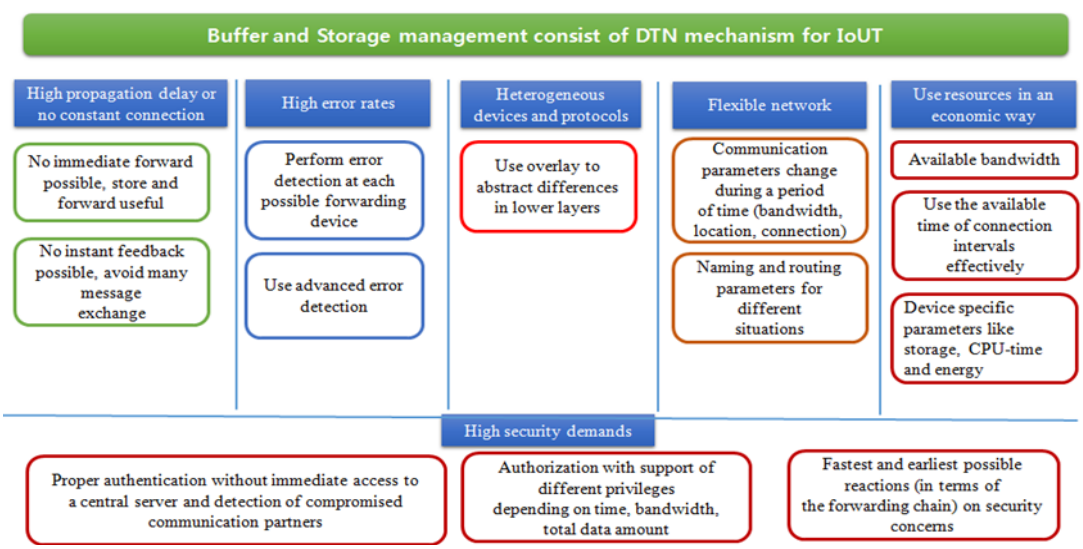

Fig. 10. Buffer and Storage management consist of DTN mechanism for UIoT decryption.

caused by different noise sources, by a self eliminating effect of the sound wave due to its reflection and phase shift at the water surface and by different propagation speeds at different temperatures.

This makes well adapted network architecture much more necessary than in common sensor networks. In addition to the aspects of the terrestrial sensor networks, underwater networks suffer a reasonable propagation delay, limited bandwidth and reasonable disturbances. Fig. 10. these problems are caused by different noise sources, by a self eliminating effect of the sound wave due to its reflection and phase shift at the water surface and by different propagation speeds at different temperatures. This makes well adapted network architecture much more necessary than in common sensor networks. Interest in UWASNs is increasing, and related research studies are also in progress.

However, as mentioned before, underwater environment is a special environment that has many restrictions. Mathematical analysis is approach of custody transfer process and data forward and store functionality. Ad-hock topology or other type of physical combination to need storage to get perfectly result of underwater network. Actually, in our suggestion mathematical formula (1) in part of 4.1. In this formula analysis and assume a **Node#A** forward to data other a **Node#B**. As you know data forwarding and receipt period totally difference, time synchronization, security process. Afterwards we would get security part (encryption and decoding) of the data exchanging each other intermediate Nodes. Advantage of this formula (1) has security and conceal from any kind of attacks. One more is quality of the data always kept and adjusted. Disadvantage of the formula more got more space in the memory. Correctly, Intermediate nodes storage space's limited. Achieve less processing delays in a DTN network. It has several open issues. Determine the size of LDT and HDT queues. So many packet flows and encrypt-decrypt process has improve maximum number of data possibility.

5. CONCLUSION

In this paper, we explored several terminologies and mathematical result. Afterwards buffer and storage management has solution in the diagram.

Most essential of the paper invoked custody transfer of the DTN architecture has specified only a coarse-grained re-transmission capability. Bundle protocol (BP) incorporates an optional feature called custody transfer, in order to offer reliable hop-by-hop transmission to the final destination. According to custody transfer mechanism, bundles are transmitted in a "store-and-forward" technique while the responsibility of reliable transfer is delegated to the next node in a route towards the final destination.

Security mechanisms for an underwater environment are difficult to apply owing to the limited bandwidth. Therefore, for underwater security, appropriate security mechanisms and security requirements must be defined simultaneously. The following are the three requirements to be fulfilled for basic underwater environment security. Our suggestion mathematical formula (1) consist of persistent storage and security process. Let me show some part of the formula (1).

In 4.1 part, before formula (1) has variable Data, M and others.

$$M = N * \lambda;$$

Here M-data size. How many data comes a minute to an intermediate node. A suitable encryption algorithm for an aquatic environment was investigated. Considering an underwater protocol stack, when the application layer sends data from a sub-layer, sending an encrypted payload is simple and safe.

The protocol packets includes multiple message formats [27].

However, when we applied security mechanism to UIoT the amount of data increases. In this Table

Table 3. IoT and UIoT elements

Elements	UIoT	IoT
BER	Bit error rate of acoustic communication high because of path loss, multi path fading, Doppler spread, and noise (from man and ambient) in the underwater channel	The bit error rate of RF communication is depends on signal - to - noise ratio.
Path loss	The path loss of acoustic waves is very high due to geometrical spreading and absorption of acoustic waves.	The path loss of radio waves is low in terrestrial environment communication.
Cost	In underwater acoustic sensor network, the cost of sensor nodes is expensive due to the more complex underwater transceivers and hardware protection also needed and availability also very limited	In terrestrial sensor network the cost of sensor nodes to become inexpensive compare to underwater sensor nodes.
Power	The need of power in underwater medication is higher than compare to radio communication due to higher distance and to more complex signal processing at the receivers and replacement of batteries also difficult.	The usage of power in radio communication is limited
Deployment	In underwater communication the sensor nodes are sparsely deployed due to the cost involved and to the associated to the deployment itself in the underwater environment.	In terrestrial sensor networks the nodes are densely deployed
High propagation Delay	The signal propagation speed of acoustic channel is about 1.5x103 m/s which are five orders of magnitude lower than the radio propagation speed (3×108 m/s).	The signal propagation speed of RF signal about 3×108 m/s.
Memory	Underwater sensor nodes need to more buffer space due to some data caching as the underwater channel may be intermittent.	Terrestrial sensor nodes have very limited capacity

3. described different point of IoT and UIoT elements. Security mechanism improves underwater communications. Therefore, we added a minimum amount of data and considered the mechanisms for underwater operation. We will constantly improve our research and works. If we are going to struggle reduce to energy consumption whole underwater network communication process. It will be UIoT quality communication for all.

REFERENCE

[1] U. Khamdamboy, J.I. Namgung, and S.H. Park, "Security Challenges of DTN Mechanism for IoUT," *Proceeding of International Conference on Advances in Electronics Engineering*, pp. 302-307, 2015.

[2] J. Partan, J. Kurose, and B.N. Levine, "A Survey of Practical Issues in Underwater Networks," *Proceedings of ACM International Conference on UnderWater Networks and Systems,* pp. 11-24, 2006.

[3] W. Ivancic. Store, Carry and Forward Problem Statement draft-ivancic-scf-probl m-statement-01. "Network Working Group". NASA GRC, Dec.13, 2013. https://tools.ietf.org/html/draft-ivancic-scf-problem-statement-01. (accessed April. 28, 2015).

[4] E. Koutsogiannis, F. Tsapeli, and V. Tsaoussidis, "Bundle Layer End-to-End Retransmission Mechanism," *Proceeding of Baltic Congress on Future Internet and Communications*, pp. 109-115, 2011.

[5] I.F. Akyildiz, D. Pompili, and T. Melodia, "Underwater Acoustic Sensor Networks: Research Challenges," *Ad Hoc Networks*, Vol. 3, No. 3, pp. 257-279, 2005.

[6] Q. Yu, X. Sun, and R. Wang, "The Effect of DTN Custody Transfer in DEEP-SPACE COMMUNICATIONS," *IEEE Wireless Communications*, pp.169-175. Oct 23, 2013.

[7] K. Scott. Bundle Protocol Specification, http://www.ietf.org/rfc/rfc5050.txt, "Network Working Group". (accessed Apr. 28, 2015).

[8] Heterogenous Network Definition, http://en.wikipedia.org/wiki/ Heterogeneous_network, (accessed Apr. 28, 2015).

[9] InterPlanetary Network, http://en.wikipedia.org/wiki/InterPlanetary_ Network, (accessed Apr. 28, 2015).

[10] C. Caini, "DTN Bundle Layer Over TCP: Retransmission Algorithms in the Presence of Channel Disruptions," *Journal of Communications,* Val.5, No 2, pp. 5(2). Feb. 2010.

[11] J. Höller, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, and D. Boyle, "From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence," Val.2, No 4, 2014.

[12] K. Scott and S. Burleigh, *Bundle Protocol Specification*, IETF RFC 5050, Experimental, 2007.

[13] J. Partan, J. Kurose, and B.N. Levine, "A Survey of Practical Issues in Underwater Networks," *Proceedings of ACM International Conference on UnderWater Networks and Systems*, pp. 11-24, 2006.

[14] Forrest Warthman, Warthman Associsatires. "Delay-and Disruption-Tolerant Networks (DTNs) A Tutorial" *Based on Technology Developed by the Interplanetary Interest Group*", Forrest Warthman, Warthman Associates, based on technology developed by the Interplanetary Internet Special Interest Group, Version 2.0. pp. 1-33, 2012.

[15] Mari Carmen Domingo. "An Overview of the Interenet of Underwater Things". *Electrial Engineering Department*, Vol. 35, No. 6, 2012

[16] I.F. Akyildiz, D. Pompili, T. Melodia, "Underwater acoustic sensor networks: research challenges" *Ad hoc networks*, Vol. 3, No. 3, pp. 257-279, 2005.

[17] M.C. Domingo, "Securing Underwater Wireless Communication Networks," *IEEE IEEE Wireless Communications*, Vol. 18, pp. 536-1284, 2011.

[18] Dimitriou S., Tsaoussidis V. "Effective buffer and storage management in DTN nodes" *Ultra Modern Telecommunications & Workshops*, pp. 1-3, 2009.

[19] Underwater Acoustics, http://www.123helpme.com/view.asp?id=149626, (accessed Apr. 28, 2015).

[20] A. Demers, S. Keshav, S. Shenker, "Analysis and simulation of a fair queueing algorithm" *ACM SIGCOMM Computer Communication* Vol 8, No. 4, pp. 1-12, 1989.

[21] Zasina, Damian, and Jarosław Zawadzki. "Statistical analysis of data set on national reporting of emission of air pollutants." Ochrona Środowiska i Zasobów Naturalnych - Environmental Protection and Natural Resources 24.3 pp. 45-51, 2013.

[22] E. Kim, N.Y. Yun, S. Muminov, S.H. Park, and O.Y. Yi, Security in Underwater Acoustic Sensor Network: Focus on Suitable Encryption Mechanisms. Springer Berlin Heidelberg, pp. 160-168, 2012.

[23] Perrig, A., Stankovic, J., Wagner, D.; "Security in Wireless Sensor Networks," *Communications of the ACM*, Vol. 6, pp. 53-57, 2004.

[24] Yi. Zhou, GU. Boa-jun, Kai.Chen, Jain-bo.Chen, Hai-bing.Guan. et al., "A Range-free Localization Scheme for Large Scale Underwater Wireless Sensor Networks," *Journal of Shanghai Jiaotong University*, Vol. 14, No. 5, 2009.

[25] C. Tian, Jiang. Hongbo, Liu.Xue, Wang. Xinbing, Liu.Wenyu, Yi.Wang et al., "Tri-Message: A Lightweight Time Synchronization Protocol for High Latency and Resource Constrained Networks" *Proceeding of IEEE ICC*, pp. 9-11, 2009.

[26] C. Tian, Liu.Wenyu, Jin.Jiang, Yi.Wang, Mo.Yijun et al., "Localization and Synchronization for 3D Underwater Acoustic Sensor Networks" *Ubiquitous Intelligence and Computing,* pp. 622-31, 2007.

[27] S. Muminov, N.Y. Yun, S. H. Park, "Software Design of Packet Analyzer based on Byte-Filtered Packet Inspection Mechanism for UW-ASN," *Journal of Korea Multimedia Society,* Vol. 14, No 12, pp. 1572-1582, 2011.

Khamdamboy Urunov

has received his B.S. degree in Information Technologies department at Tashkent University of Information Technology of Urgench branch, 2009 and he graduated master degree department in Applied Informatics at Tashkent University of Information Technologies, Tashkent, Uzbekistan, 2011. Khamdamboy has got grant ITEC program in India, 2013. He is studying PhD degree in Financial Information Technology, Kookmin University. His research area includes Security mechanism of DTN (Delay/Disruption Tolerant Network), M2M (Machine to Machine) communication and Internet of Things (IoT).

Jung-Il Namgung

has received his B.S. degree in mechanical engineering from Incheon University in 1995, M.S. and Ph. D degrees in Business IT from Kookmin University in 2005, 2011, respectively. Now, he is a BK21+ research professor in the department of Financial Information Security, Kookmin University. His current research interests include IoT (Internet of Things) / M2M (Machine to Machine communication) and Context Awareness / Service Composition / Artificial Intelligence.

Soo-Hyun Park

has received his B.S., M.S. and Ph. D degrees in computer science engineering from Korea University in 1988, 1990 and 1998, respectively. Now, he is a professor in the Department of Information System, Kookmin University, Korea. His current research interests include underwater IOT (Internet of Things) and Ubiquitous Network.