Security Challenges of DTN Mechanism for IoUT

Khamdamboy Urunov, Jung-Il Namgung, and Soo-Hyun Park

***Abstract*—Our purpose is to analyze how to benefit from the IoUT and explore, exploit and preserve the natural underwater resources. Delay/Disruption Tolerant Network (DTN) is essential part of the network heterogeneity communication network. Our expectation security area in DTN mechanism is to create adequate mechanism for Internet of Underwater Things. In this paper, an in-depth view of the IoUT and security challenges is provided. Internet of Underwater Things (IoUT) is defined as a world-wide network of smart interconnected underwater objects that enables to monitor vast unexplored water areas.**

***Index Terms*—Underwater Internet of things, delay/disruption tolerant network, bundle layer, security challenges, custody transfer.**

I. Introduction

The earth's surface 3/4 is covered by oceans, a continuous body of water that is customarily divided into several principal oceans and smaller seas. Those natural facts always confirm 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 [1]. Destruction of wildlife due to global warming, changes in agricultural yields, extinction of species, and an increasing number of disease-carrying insects are also effects. The most important part of things used on the internet, are continuously connected to end-to-end, low-delay paths between sources and destinations [2]. It is obviously known that people are endeavoring and making a great attempt in evolving communication networks for the better all over the world and even in the galaxy as possible as they can . In the future, high quality network and reliable communication get everywhere, every time online things (communication devices) for instance: Internet of Things, Internet of Underwater Things and Interplanetary communications. 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. Likewise, the Internet of Things is 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. Underwater acoustic communication is a technique of sending and receiving message below water [3]. There are several ways of employing such communication but the most common is using hydrophones.

This paper is organized as follows: Introduction, Section II explains propose of the Custody transfer for internet of underwater things (IoUT). Section III gives the concept of analysis of security challenges Underwater Internet of Things. We conclude our paper and outline with future works.

Manuscript received December 6, 2014; revised January 25, 2015.

The authors are with Kookmin University, South Korea (e-mail: hamdamboy.urunov@gmail.com, greenji@naver.com, shpark21@kookmin.ac.kr).

II. Custody Transfer for Internet of Underwater Things

DTN custody transfer is a service that may be optionally provided to a bundle as it is delivered through a DTN. When used, custody transfer keeps track of a current "responsible entity" or "custodian" for each bundle, and the custodian is required to keep the bundle safe in persistent memory until another custodian has received it successfully. The DTN architecture is targeted at network where an end-to-end routing path cannot be assumed to exist. Rather, routers are comprised of a cascade of time-dependent contacts communication opportunities used to move messages from their destinations. Contacts are parameterized to be their start and end times (relative to the source), capacity, latency, endpoints, and direction. In addition, each underwater physical object that contains both current and historical information on that object's physical properties, origin and sensory context. This information is ubiquitous, available in real-time using different ways of communication Human to Thing (H2T) and Ting to Ting (T2T)) [4] and streamlines dramatically how to maintain and manage underwater habitats and resources. In this case, supplementary M2M mechanism and Smart house communication also provide DTN in the near the future our life.

A. Overview Bundle Layer and Concept of Underwater Communication

Literally, the capacity of the communication network will improve and encourage each public and private costumer (which request communication network things), which can be provided with quality and enhancement. Delay/Disruption tolerant network (DTN) is characterized to be intermittent connectivity, asymmetric link, high propagation delays or disruption of communication line and then high packet error rate; end-to-end functionality can and should be integrated into Bundle layer. Currently DTN has been proposed as global overlay architecture to provide network connectivity in challenged environments such as a deep-space communication field. According to the custody transfer mechanism, bundles are transmitted in a "store-and-forward" technique while the responsibility of reliable transfer is delegate to the next node in a route towards the final destination. DTN mechanism provides two fundamental things:

- Heterogeneous Network (HN)
- Interplanetary Network (IPN)

DOI: 10.7763/IJIEE.2015.V5.553

A heterogeneous Network is a network connecting computers and other devices with different operating systems and/or protocols [5].

The Interplanetary Network (IPN) is a group of spacecraft equipped with gamma ray burst (GRB) detectors. By timing the arrival of a burst at several spacecraft, its precise location can be found [6].

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 the Fig. 1 heterogeneous network via DNT Getaway.

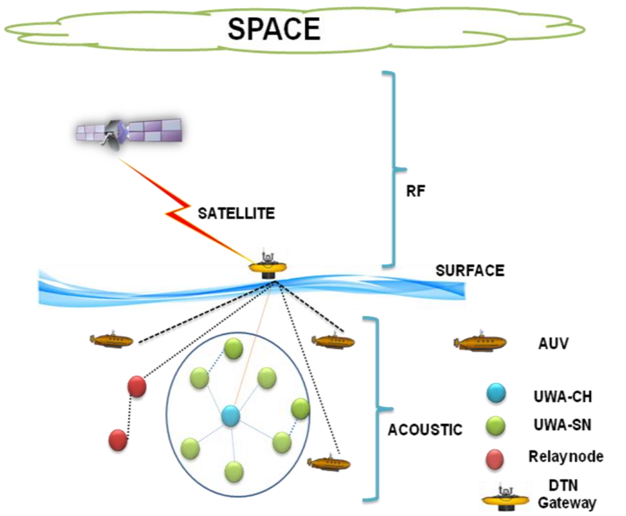

Fig. 1. Heterogeneous network via DNT getaway.

Indeed, DTN Getaway involves a wide verity of the communications. This communication surface is on Space, Earth and Underwater. It has shown three part of around the world. The first communication side's Space and second is Space to Surface part. Last one is underwater communication skill include relay nodes, DTN Getaway and underwater acoustic sensor node (UWA-SN), underwater acoustic cluster header (UWA-CH), underwater vehicles (AUV) than in this case remote environment space high bandwidth and opposite case is underwater low bandwidth more propagation delay and disruption. At the present next step represent layering process. It means heterogeneous network different layering model. 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.

In addition, key point is things/underwater things. We know that things are composed of networking area technical instrument or appliances, which layering model and differences Internet of things and Underwater Internet of Things can bundle uses with getaway and approach to Fig. 2 communication via Bundle layer, heterogeneous network uses DTN getaway. So, in Fig. 2 (left) side has Internet of Things (IoT) and communication layer model joined Bundle layer. Bundle custody transfer enforces heterogeneous internet. 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 underwater communication system.

The network [7] architecture for delay tolerant network consists of three major entities:

Host-The host is used to send or receive data in forms of the bundle.

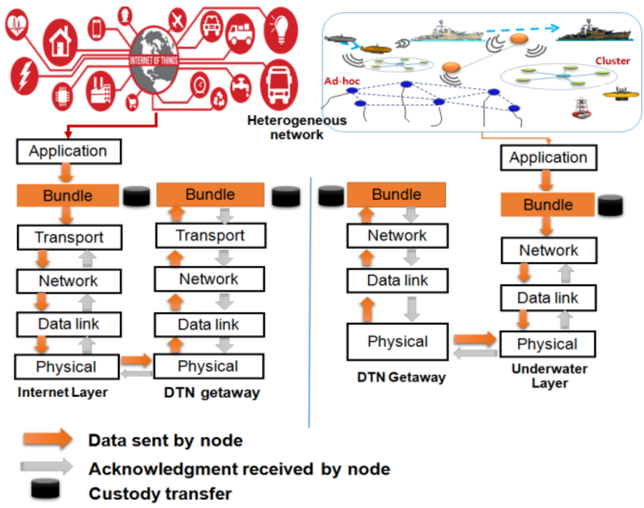

Fig. 2. Heterogeneous communication layering diagram.

Router-The router is used to forward bundles to another node in a single region. It needs some buffer space because of uncertainty regarding future communication opportunity, for this it needs to store data for retransmission.

Gateway-The gateway is used for forwards bundles to nodes in different regions. It must supports interoperability, and is also used for performing authentication.

The Bundle Protocol includes a hop-by-hop transfer of reliable delivery responsibility, called bundle custody transfer, and an optional end-to-end acknowledgement.

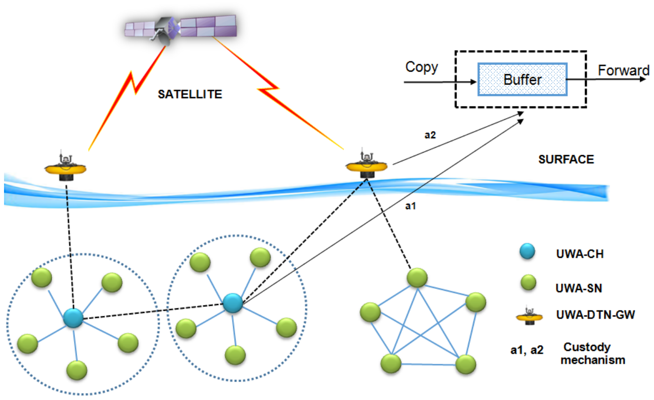

Fig. 3. Bundle layer dominate of the custody transfer.

When nodes accept custody of a bundle, they commit to retain a copy of the bundle until such responsibility is transferred to another node. Persistent storage may be used in DTN nodes to help combat network interruption, storing messages safely until a contact opportunity occurs.

We believe that the custody transfer mechanism is not necessarily less reliable than using typical end-to-end reliability although it is different. This opinion stems from the observation that in many circumstances, where end nodes cannot be assumed to remain operational for long periods of time, that the chances for data to be reliably delivered using delegation can exceed its changes of being successfully delivered end-to-end.

B. Internet of Underwater Things Communication Area

Internet of Underwater things 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 [8]. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a 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 **Internet of Underwater Things (IoUT)** 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 the IoUT to learn from, exploit and preserve the natural underwater resources. In this paper, the IoUT is introduced and its main differences with respect to the Internet of Things (IoT) are outlined.

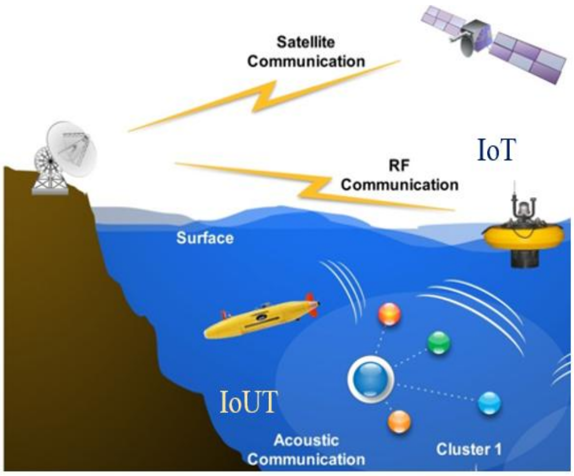

Fig. 4. Internet of underwater things.

Fig. 4 shows communication process of underwater and space station. In that case Internet of things and Underwater of things describe initial positions. 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 IoUT. Most of the routing protocols, even for terrestrial or underwater sensor networks, use separate packets for control information and data transmission.

III. Analysis Security Challenges of Underwater Internet of Things

Security challenges of Underwater of Things, challenged internetworks are characterized by latency, bandwidth limitations, error probability, node longevity, or path stability that is substantially worse than that is typical of today's Internet. We use the Internet's performance as a baseline due to its enormous scale and influence.

A. Open Issues of Underwater Bundle Layer Security

Some DTN nodes will however, be on boundaries of various sorts, whether they be network-topology related, administrative, networking technology related or simply a case where this node is the first that is capable of handling complex policy decisions. At one stage, these nodes were termed security policy routers, and were considered to be "special" nodes. 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. For example, some "bastion" node might insist on all inbound bundles being authenticated, and might add an authentication element to all outbound elements. So all the usual forms of control can and should be available for use in DTN nodes. No doubt, more will be identified as more DTN deployment experience is gained. In Underwater environment are exposed of several problems and how can tackle issues in this exploring situation. In Fig. 5(a) vividly depicted to underwater challenges and Bundle possibilities and several issue included this figure. That figure challenges for underwater communication sphere.

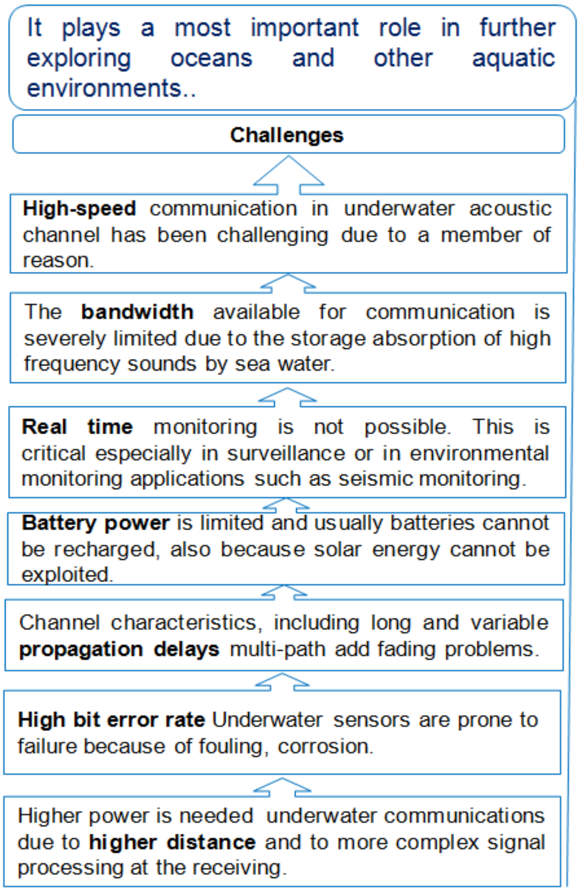

Fig. 5(a). Underwater challenges and bundle possibilities.

The Bundle Protocol suite is intended to consist of a group of well-defined protocols that, when combined, enable a well-understood method of performing store-and-forward communications.

Kind of challenges solve DTN part of the issues. Next part of the Fig. 5(b) shows DTN part of entity and possibilities.

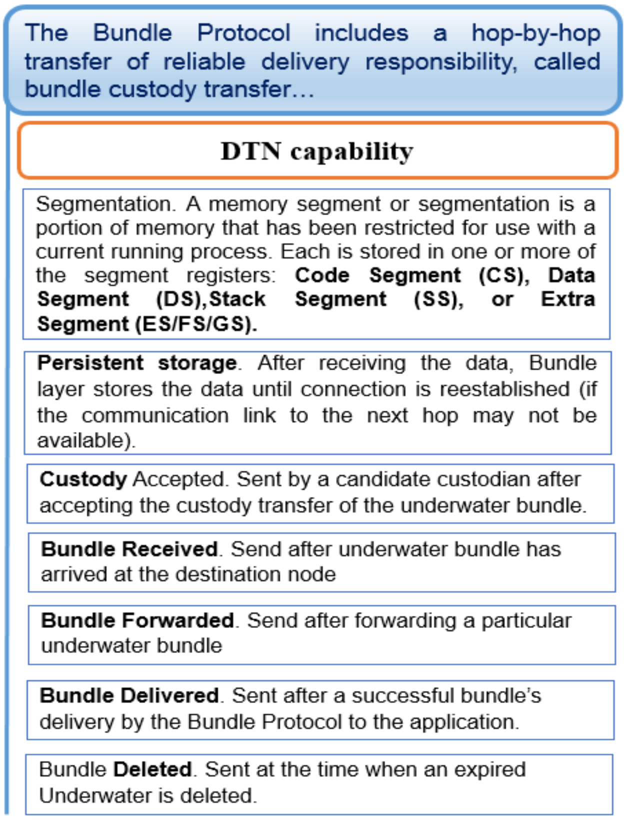

Fig. 5(b). Underwater challenges and bundle possibilities.

The above-mentioned conceptual steps vividly show DTN of Bundle layer. 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 [9] 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). The rationale for the separation is to provide for different types of canonicalization and key management that are likely to be used for hop-by-hop vs. end-to-end cryptographic services. Some DTNs (e.g., wireless sensor networks) may involve nodes that are extremely challenged in CPU terms, or more likely, in key management terms, and so cannot they encrypt, decrypt, sign or verify bundles. In addition, there may be some DTNs in which portions of the physical network topology are contained in physically secured facilities. 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.

B. Known Problems and Violates Underwater Communication

The current 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 [10]. Error detection is a very basic networking concept that was over looked in the Bundle Protocol design [11].

TABLE I: BUNDLE LAYER FUNCTIONAL PARAMETERS

DTN entity	Description
Segmentation	In order to message segmentation into tunable size DTN bundle
Data Forwarding	After receiving the underwater bundle from source node, forwarding these bundle to the destination node with the help of intermediate nodes.
Persistent storage	After receiving the data, Bundle layer stores the data until connection is reestablished (if the communication link to the next hop may not be available).
Convergence Layer Adapter	As each of these protocols provide somewhat different semantics, a collection of protocol-specific convergence layer adapters (CLAs) provide the functions necessary to carry DTN protocol data units (called Bundles) on each of the corresponding protocols.

Node was received error-free or not. Error detection is a very basic networking concept that was over looked in the Bundle Protocol design. The design of the bundle architecture completely ignores the well-known end-to-end principle. Without useful error detection, the 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.

IV. CONCLUSION

In this paper, our research area underwater communication network and security challenges.

Underwater communication is difficult due to factors like multi-path propagation, time variations of the channel, small available bandwidth and strong signal attenuation, especially over long ranges. In underwater communication there are low data rates compared to terrestrial communication, since underwater communication uses acoustic waves instead of electromagnetic waves. Table.1 shows DTN entity and functionality. The bundle security protocol is still very much a work-in-progress and there are some significant open issues remaining to be determined.

Thus problem to guarantee security and resilience of the network in this environment is to establish a uniform foundation for trust in nodes and terminals as well as security of communication between them. Actually, it must establish roots of trust for connected devices and network nodes that rely on hardware security to reach the necessary assurance level and make security scalable.

ACKNOWLEDGMENT

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).

REFERENCES

[1] J. Partan, J. Kurose, and B. N. Levine, "A survey of practical issues in underwater networks," in *Proc. ACM WUWNet*, 2006, pp. 11–24.
[2] A. Schmidt, A. Pasic, F. Martinelli, D. Métayer, A. Waller, and I. E. Ivanov, "NESSI TSD WG position paper on security challenges in future Internet," 2003.
[3] M. B. Kasmani, "A socio-linguistic study of vowel harmony in Persian: Different age groups use of vowel harmony perspective," *International Proceedings of Economics Development and Research*, pp. 359-366, vol. 26, 2011.
[4] I. F. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: research challenges," *Ad Hoc Networks* (Elsevier), vol. 3, no. 3, pp. 257-279, March 2005.
[5] Hetergenous network. [Online]. Available: http://en.wikipedia.org/wiki/Hetergenous network
[6] InterPlanetary network. [Online]. Available: http://en.wikipedia.org/wiki/InterPlanetary_Network
[7] L. K. Choudhary, M. P. Singh, U. Chaurasia, and M. K. Ahirwar, "Survey of delay tolerant network - An architectural prospective," pp. 4-8.
[8] 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*, Elsevier, 2014.
[9] S. Symington, S. Farrell, H. Weiss, and P. Lovell, "Bundle security protocol specification," presented at Work in Progress, Sep. 2007.
[10] E. Koutsogiannis, F. Tsapeli, and V. Tsaoussidis, "Bundle layer end-to-end retransmission mechanism," S2011 Baltic Congress on Future Internet and Co.
[11] R. Thumpi, R. B. Manjula, and S. M. Sunilkumar, "A survey on routing protocols for underwater acoustic sensor networks," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 2, no. 2, May 2013.

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.