

해사 클라우드 환경에서 MRN기반의 해사 엔터티 식별체계 설계 및 아이디기반의 메시지 전달 성능 분석

안 개 일[°], 정 도 영^{*}, 정 병 호^{*}

Design of MRN-Based Maritime Entity Identification System and Analysis of Identity-Based Message Delivery Performance in Maritime Cloud Environment

Gaeil An[°], Doyoung Chung^{*}, Byungho Chung^{*}

요 약

국제해사기구인 IMO에서는 인적과실에 의한 해양사고를 예방할 목적으로 e-내비게이션(e-Navigation) 도입을 결정하였다. 현재 e-내비게이션 서비스를 위한 통신 인프라로서 해사 클라우드가 개발되고 있다. 본 논문에서는 사용자와 선박 등 해사 엔터티를 한국에서 독립적으로 등록하고 관리하고자 할 때 요구되는 해사 엔터티의 식별 체계를 제안한다. 또한 본 논문에서는 시뮬레이션을 통하여 해사 클라우드에서 정의된 MMS 서버 기반의 통신방식과 기존 해양 통신방식을 메시지 전달 성능 관점에서 평가한다.

Key Words : e-Navigation, Maritime cloud, Maritime entity, Identity, Message delivery

ABSTRACT

IMO, an international maritime organization, decided to introduce e-Navigation to prevent marine accidents caused by human error. The maritime cloud is being developed as a communication infrastructure for e-navigation services. In this paper, we propose an identification system of maritime entities required to independently register and manage maritime entities using the maritime cloud in Korea. In addition, we evaluate the MMS server-based communication method and the existing marine communication method defined in the maritime cloud from the viewpoint of message transmission performance through simulation.

1. 서 론

매년 인명과 재산손실을 초래하는 해난 사고는 끊임없이 발생하고 있으며, 이러한 사고 원인의 대부분은 항해자의 실수 또는 주의 부족 등 인적인 요인에서 발생한 것으로 조사되고 있다^[1]. 국제해사기구인

IMO(International Maritime Organization)에서는 인적과실에 의한 해양사고를 예방할 목적으로 2006년에 e-내비게이션(e-Navigation) 도입을 결정하였다^[2]. e-내비게이션이란 첨단 ICT 기술을 활용하여 선박의 입항부터 출항까지 안전 운행에 필요한 모든 해양 정보를 통일하고 종합하여 선박들에게 제공하는 수행 체

* 본 논문은 2017년 해양수산부 재원으로 한국해양과학기술진흥원의 지원을 받아 수행된 연구임(IMO 차세대 해양안전 종합관리체계 기술개발)

[°] First and Corresponding Author : (ORCID:0000-0002-1392-6545)Electronics and Telecommunications Research Institute, Information Security Research Division, fogone@etri.re.kr, 정희원

* Electronics and Telecommunications Research Institute, Information Security Research Division, {thisisdoyoung, cbh}@etri.re.kr
논문번호 : KICS2017-10-325, Received October 30, 2018; Revised January 12, 2018; Accepted January 23, 2018

계를 말한다.

e-내비게이션 서비스를 안전하고 효율적으로 제공하기 위해서는 해양이라는 특수한 환경에서 효과적으로 운용될 수 있는 통신 인프라가 필요하다. 국제항로 표지협회인 IALA(international association of lighthouse authorities)에서는 e-내비게이션 서비스를 위한 통신 인프라로서 해사 클라우드를 개발하고 있다. 해사 클라우드의 개념도는 그림 1에 도시되어 있다. 해사 클라우드의 핵심 구성요소는 해사 엔터티(entity) 관리와 인증 기능을 제공하는 MIR(Maritime Identity Server) 서버, e-내비게이션 서비스를 관리하는 MSR(Maritime Service Registry) 서버, 그리고 끊임없는 로밍 서비스의 통신을 제공하는 MMS(Maritime Messaging Server) 서버이다³⁻⁶⁾. 여기서, 해사 엔터티는 해사 클라우드 참여자로서, 서비스 요청자에 해당하는 선박, 디바이스, 사용자와, 서비스 제공자에 해당하는 서비스, 그리고 해사 클라우드 참여자를 관리하는 조직을 말한다. 끊임없는 로밍 서비스는 해사 클라우드의 가장 큰 특징 중 하나이며, 이종 통신 네트워크상에서 특정 네트워크 링크에 장애가 발생하더라도 다른 가용 네트워크 자원을 이용하여 데이터를 끊임없이 목적지로 전달해 주는 기능이다. 끊임없는 로밍 서비스는 다양한 이종 통신 네트워크를 지원해야하기 때문에 해사 클라우드는 네트워크 주소가 아닌 아이디를 사용하여 통신 엔터티를 식별한다.

현재 국내에서는 IMO의 e-내비게이션에 어선 및 연안 소형선을 대상 서비스에 추가하여 한국해양환경에 특화된 한국형 e-내비게이션 시스템을 개발하려는 연구가 활발히 진행되고 있다⁷⁻¹²⁾. 한국형 e-내비게이션을 개발하기 위해서는 한국의 실정에 맞게 해양 선박을 위한 서비스 개발과 통신망 구축, 보안 분석 그

리고 해사 클라우드의 확장에 대한 연구가 선행되어야 한다.

현재 해사 클라우드에서는 e-내비게이션 사용할 해사 엔터티에 대한 아이디는 관리자가 직접 수동으로 할당하는 방식을 채택하고 있다¹³⁾. 한국형 해사 클라우드에서는 외국에 없는 선박 아이디 유형(예, 선박번호, 어선번호)도 고려되어야 하며 등록할 사용자 및 선박의 수가 많은 상황이다. 따라서 관리자가 아이디를 직접 할당하는 기존 방식은 대량의 해사 엔터티를 해사 클라우드에 등록하는 경우에는 매우 비효율적인 문제가 있다. 본 논문에서는 해사 클라우드 환경에서 한국에서 정의한 선박 아이디 유형을 수용하고 해사 엔터티의 아이디를 자동으로 할당할 수 있는 MRN(Maritime Resource Name) 기반의 해사 엔터티 식별 체계를 제안한다.

또한 본 논문에서는 시뮬레이션을 통하여 해사 클라우드에서 정의하고 있는 두 가지 통신 방식, 즉 끊임없는 로밍 서비스를 지원하는 MMS 서버 기반의 통신방식과 이종 통신 네트워크간 핸드오버를 지원하지 않는 기존 해양 통신방식을 메시지 전달 성능 관점에서 평가한다.

본 논문의 구성은 다음과 같다. 2장에서는 해사 클라우드에 대해서 간단히 살펴보고, 3장에서는 본 논문에서 제안하는 한국형 해사 클라우드 해사 엔터티의 식별 체계를 설계한다. 4장에서는 해사 클라우드의 메시지 전달 성능을 시뮬레이션을 통하여 분석하고, 마지막으로 5장에서 결론을 맺는다.

II. 해사 클라우드 개요

국제해사기구인 IMO에서는 안전하고 효율적인 해양 정보통신 서비스를 제공하는 것을 목적으로 e-내비게이션을 정의하였다. IALA에서는 e-내비게이션 서비스를 위한 안전하고 효율적인 통신 인프라로서 해사 클라우드를 제안하고 있으며, 실제적인 개발은 덴마크, 스웨덴, 한국이 중심이 되어 구성된 MCDF(Maritime Cloud Development Forum)라는 개발자 포럼에서 진행되고 있다¹³⁾.

해사 클라우드는 핵심 서비스로서, 해사 아이디 관리, 인증 및 데이터 보안, e-내비게이션 서비스 관리, 위치기반의 멀티캐스트인 지오캐스트(Geocast) 그리고 끊임없는 로밍 서비스를 제공한다. 해사 아이디 관리 서비스는 해사 클라우드에서 존재하는 객체를 식별하고 관리하는 기능이며, 인증 서비스는 해사 클라우드의 불법 접근을 방어하기 위한 OIDC(Open ID

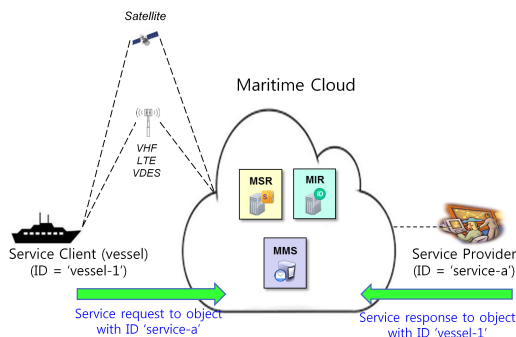


그림 1. 해사 클라우드 개념도
Fig. 1. Concept of maritime cloud

Connectivity) 및 디지털 인증서 기반의 인증 기능을 말하며, 데이터 보안 서비스는 해사 클라우드를 통해 전달되는 데이터에 대해 기밀성과 무결성을 보장하는 기능이다. e-내비게이션 서비스 관리 서비스는 관리자가 e-내비게이션 서비스를 용이하게 사용하고 등록할 수 있도록 제공하는 것을 목적으로 한다. 마지막으로 끊임없는 로밍 서비스는 AIS(Automatic Identification System), VDES(VHF Data Exchange System), LTE, 위성 등 이종 통신 네트워크상에서 특정 네트워크 링크에 장애가 발생하더라도 다른 가용 네트워크 자원을 이용하여 데이터를 끊임없이 전달해 줄 수 있는 기능을 말한다. 끊임없는 로밍 서비스는 다양한 통신 네트워크상에서 동작해야하기 때문에 네트워크 주소가 아닌 아이디를 사용하여 통신 엔터티를 식별한다.

해사 클라우드에서는 상기의 서비스를 제공하기 위해서 MIR, MSR 그리고 MMS 등 세 개의 서버를 정의하고 있다. 먼저, MIR 서버는 해사 클라우드상의 모든 해사 엔터티에 대한 아이디 정보를 관리하는 서버로서 아이디, 연락 정보, 디지털 서명 등의 정보를 관리한다. MSR 서버는 e-내비게이션 서비스를 접근하는데 필요한 정보를 관리하는 서버로서, 서비스 내용, 서비스 인터페이스, 그리고 서비스 접근 방법 등이 명세된 서비스 스펙을 관리한다. 마지막으로 MMS 서버는 끊임없는 정보 전달 서비스와 지오캐스트 서비스를 제공하기 위하여 통신 메시지 관리 기능, 프로토콜 수준의 수신 확인 기능, 그리고 통신 객체의 위치 정보 수집 기능을 제공한다. MMS 서버는 접속한 서비스 요청자의 아이디와 네트워크 주소를 관리하고 서비스 요청자와 서비스 제공자간의 메시지 전달 중계자 역할을 수행한다.

III. 해사 클라우드를 위한 해사 엔터티 식별 체계

3.1 MRN 표기 방식

해사 클라우드의 참여자인 해사 엔터티를 전역적으로 유일하게 식별하기 위해서는 해사 자원에 영구적인 고유한 객체식별 기호를 부여하는 수단이 필요하다. 해양 정보통신 분야에서는 해사자원 식별체계로서 MRN을 국제표준으로 제안하고 있다^[14]. MRN은 기본적으로 URN(Unique Resource Name)의 형식을 따르며, 해사 자원을 관리하는 조직이 자신만의 자체적인 세부 식별 구조를 정의하는 것을 허용한다.

MRN의 기본적인 구조는 그림 2에 도시되어 있다. MRN의 구조는 URN에서 정의된 형식에 따라서 두

부분, 즉 URN 기반의 MRN이라는 것을 알려주는 아이디인 “urn:mrn”과 NSS(Namespace Specific String) 필드로 구성된다. MRN 표준에서는 그 NSS 필드를 다시 해사 자원의 관리기관을 의미하는 OID(Organizational ID), 해사 자원의 유형이 명시되는 OSNID(Organizational specific namespace ID) 그리고 해사 자원의 값을 가리키는 OSNS(Organizational specific namespace string) 로 나눈다. 여기서 각 필드는 콜론(:)으로 구분되며, OID 필드에 명시된 기관은 OSNID 필드와 OSNS 필드를 어떻게 사용할지 직접 정의할 수 있다.

예를 들어, imo-number가 9743368 인 선박의 경우에, imo-number 관리 기관인 IMO에서 “imo-number”를 정의한다면, 그때 OID는 “imo”, OSNID는 “imo-number”, 그리고 OSNS는 “9743368”이 된다. 따라서 그 선박의 MRN은 “urn:mrn:imo:imo-number:9743368” 로 표기된다.

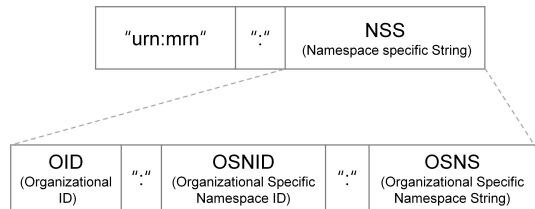


그림 2. 해사 자원 식별을 위한 MRN 체계
Fig. 2. MRN system for identification of marine resources

3.2 해사 엔터티 식별 체계의 설계

본 논문에서는 MRN을 기반으로 하여 한국 해사 클라우드를 위한 해사 엔터티의 식별 체계를 제안한다. 본 문서에서 제안하는 해사 클라우드 엔터티 식별 체계는 그림 3에 도시되어 있다. 3.1절에서 언급한 바와 같이, MRN 표기 방식에서는 OID에 명시된 기관이 하위 필드를 어떻게 구성할 지에 대한 권한을 갖는다. 해사 클라우드중에서 MIR을 개발하고 있는 덴마크에서는 OID 필드에 “mcl”라는 문자열^[13], MSR을 개발하고 있는 스웨덴에서는 OID 필드에 “stm”라는 문자열^[15]을 할당하였다. 본 논문에서는 한국 해사 클라우드 엔터티 식별 체계를 다른 식별체계와 구분하기 위하여 OID 필드에 “smart”라는 문자열을 할당하였다.

해사 클라우드에서 관리해야 할 해사 엔터티는 조직, 사용자, 디바이스, 선박, 서비스 등 총 다섯 종류이다. 조직은 사용자, 디바이스, 선박, 서비스를 관리하는 기관을 말한다. 본 논문에서는 OSNID 필드에 해

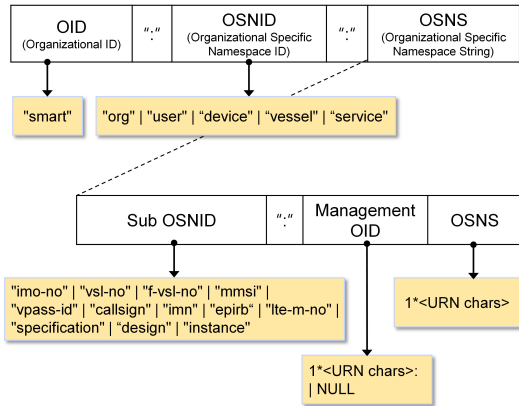


그림 3. 해사 클라우드 엔터티 식별 체계
Fig. 3. Identification system for maritime cloud entities

사 엔터티의 유형을 할당하였다. 즉, OSNID 필드는 사용자 유형이 조직이면 “org”, 사용자이면 “user”, 디바이스이면 “device”, 선박이면 “vessel”, 서비스이면 “service”가 된다. OSNS 필드는 Sub OSNID, Management OID, 그리고 OSNS 등 총 세 개의 필드로 구성된다. OSNID 필드의 값이 만약 선박 (“vessel”)이면, Sub OSNID 필드는 선박의 종류를 나타내기 위해 사용된다. 본 논문에서는 외국에서 사용하지 않는 선박 아이디 유형인 선박번호와 어선번호도 Sub OSNID 필드의 값에 포함될 수 있도록 설계하였다. Sub OSNID 필드의 가능한 값은 “imo-no”(IMO 번호), “vsl-no”(선박번호, vessel-number), “f-vsl-no”(어선번호, fishing vessel-number), “mmsi”(MMSI 번호), “vpass-id”(V-Pass 아이디), “callsign”(콜사인), “imn-no”(위성모바일번호, Inmarsat mobile number), “epirb”(EPIRB, Emergency Positioning-indicating Radio Beacon), 그리고 “lte-m”(LTE-M 번호)이다.

OSNID 필드의 값이 만약 서비스(“service”)이면, Sub OSNID 필드는 서비스 문서의 종류를 나타내기 위해 사용된다. 이때 Sub OSNID 필드의 가능한 값은 “specification”(서비스 스펙 문서), “design”(서비스 기술 디자인 문서), 그리고 “instance”(서비스 인스턴스 문서)중 하나가 된다. 여기서 서비스 스펙 문서에는 서비스 데이터 모델링을 기술하며, 서비스 기술 디자인 문서에는 서비스를 제공하기 위한 프로토콜을 그리고 서비스 인스턴스 문서에는 서비스를 접근하기 위한 정보를 명시한다⁶⁾. Management OID 필드에는 OSNS를 직접 할당하는 기관을 나타내며, 만약 OID의 값과 동일하면 생략된다.

본 논문에서 제안하는 해사 엔터티 식별 체계의 MRN 표기 예는 다음과 같다. 만약 “alice@daejeon.re.kr”로 식별되는 사용자가 해사 클라우드에 등록되면, MRN은 urn:mrn:smart:user:alice@daejeon.re.kr 로 표기되며, 이름이 “router260”인 디바이스의 MRN은 urn:mrn:smart:device:router260 로 표기되고, 서비스 인스턴스가 “route-exchange”인 서비스의 MRN은 urn:mrn:smart:service:instance:route-exchange로 표기되며, “daejeon”라는 조직의 MRN은 urn:mrn:smart:org:daejeon 로 표기된다.

본 논문에서 제안하는 해사클라우드 식별체계는 기존의 덴마크와 스웨덴 식별체계들과 비교했을 크게 두 가지 차별성이 있다. 첫 번째는 본 논문에서 제안하는 식별체계는 한국에만 사용하는 선박번호, 어선번호, VPASS ID, LTE-M 등의 선박 아이디가 해사 엔터티 아이디에 포함될 수 있도록 Sub OSNID 필드 값을 확장하여 설계했다는 것이다.

두 번째 차별성은 해사 엔터티의 아이디 등록 방법이다. 기존 해사 클라우드에서의 해사 엔터티 등록 방법을 살펴보면 먼저 조직을 등록한 후에 조직 관리자가 그 조직에 속하는 선박, 디바이스, 사용자, 그리고 서비스를 직접 등록하는 방식을 사용하고 있다¹³⁾. 이 방식의 가장 큰 문제점은 등록할 해사 엔터티의 유일한 아이디 값을 조직 관리자 직접 할당해야하기 때문에, 대량의 해사 엔터티를 해사 클라우드에 등록하는 경우에는 매우 비효율적이라는 것이다. 본 논문에서는 선박에 대한 해사 엔터티의 아이디는 선박 아이디를 사용하여 자동으로 유일한 값이 할당될 수 있도록 Sub OSNID 필드의 선박 아이디 유형에 우선순위 (“imo-no”, “vsl-no”, “mmsi” 순서로 낮아짐)를 부여하고, 이를 기반으로 하여 MRN을 할당한다. 예를 들어, IMO number가 “1234567”이고 MMSI가 “987654321”인 선박을 해사 클라우드에 등록하면, IMO number가 MMIS보다 우선순위가 높기 때문에 그 선박의 MRN은 urn:mrn:smart:vessel:imo-no:1234567이 할당된다.

IV. 해사 클라우드의 통신 메시지 전달 성능 분석

4.1 메시지 전달 시나리오

해사 클라우드에서는 서비스 요청자와 서비스 제공자간 통신 방법으로서 기존 통신과 MMS 통신 등 두 가지 방식을 정의하고 있다⁴⁾. 기존 통신 방식은 MMS 서버 없이 서비스 요청자와 서비스 제공자가

직접 통신하는 방법이다. MMS 통신 방식은 서비스 요청자가 서비스 제공자와 통신할 때 MMS 서버를 경유하는 방법으로서 끊임없는 통신 서비스를 제공하는 방식이다.

기존 통신 방식은 그림 4에 도시되어 있다. 먼저, 서비스 요청자는 사용자가 원하는 서비스(예, 기상 서비스)에 대한 메타정보를 MSR 서버에게 요청한다. MSR 서버는 그 서비스 요청자가 해사 클라우드에 등록된 합법적인 엔터티인지를 확인하기 위하여 MIR 서버에게 서비스 요청자에 대한 인증을 요청한다. 만약, 인증이 성공하면, MSR 서버는 서비스 요청자에게 서비스 메타 정보(예, 서비스 제공자의 접속 인터페이스 및 주소)를 회신한다. 서비스 요청자는 MSR 서버로부터 수신한 서비스 메타정보를 사용하여 서비스 제공자에게 서비스 요청 메시지를 전송한다. 서비스 제공자는 서비스 요청자를 인증하기 위해서 MIR 서버를 접속한다. 만약, 서비스 요청자에 대한 인증이 성공하면, 서비스 제공자는 서비스 요청자에게 해당하는 서비스 응답 메시지를 회신한다.

MMS 통신 방식은 그림 5에 도시되어 있다. 먼저, 서비스 요청자는 자신이 원하는 서비스에 대한 서비스 메타 정보를 MSR 서버에게 요청한다. MSR 서버

는 서비스 요청자에 대한 인증이 성공하면 서비스 요청자에게 서비스 메타 정보를 회신한다. 서비스 요청자는 MSR 서버로부터 수신한 메타 정보를 사용하여 서비스 요청 메시지를 생성한 후 MMS 서버에게 그 메시지 전달을 요청한다. MMS 서버는 메시지를 전송한 엔터티를 인증하고, 만약 인증에 성공하면 서비스 제공자에게 그 메시지를 전달한다. 서비스 제공자는 메시지를 보낸 서비스 요청자를 인증하기 위해서 MIR 서버를 접속한다. 만약, 서비스 요청자에 대한 인증이 성공하면, 서비스 제공자는 MMS 서버에게 서비스 응답 메시지를 회신한다. MMS 서버는 서비스 제공자로부터 수신한 메시지를 서비스 요청자에게 전달한다.

4.2 메시지 전달 성능 평가

해사 클라우드에서 정의한 MMS 서버는 선박과 통신할 때, 위성 네트워크나 무선 네트워크 등 다양한 이종 네트워크 통신을 제공하기 때문에 네트워크 장애가 발생하더라도 효과적으로 대응할 수 있다. 본 논문에서는 해사 클라우드에서 메시지 전달 방법으로 정의하고 있는 기존 통신 방식과 MMS 통신 방식의 성능을 비교 분석한다.

해사 클라우드가 MMS 통신 방식으로 동작하려면, 서비스 요청자는 이종망간의 이동시에도 통신 서비스가 끊임이 없도록 버티컬 핸드오버(vertical handover) 기능을 수행해야 하며, MMS 서버는 서비스 요청자와 육상 네트워크간의 통신이 잠시 두절되더라도 끊임없는 서비스를 지원할 수 있도록 서비스 요청자와 서비스 제공자간 통신 메시지를 관리하고 전달하는 중계자 역할을 수행해야 한다. 이를 위하여 본 논문에서는 NS3 네트워크 시뮬레이터^[6]를 사용하여 서비스 요청자, MMS 서버, 그리고 서비스 제공자를 구현하였다.

본 논문에서는 NS 네트워크 시뮬레이터상에서 끊임없는 로밍 서비스를 제공하기 위해 서비스 요청자와 서비스 제공자는 IP 네트워크 주소 대신에 3.2절에서 정의된 MRN을 사용하여 통신 객체를 식별하고, MMS 서버는 서비스 요청자와 서비스 제공자간의 통신 메시지를 저장·관리하고 중계할 수 있도록 구현하였다. 이와 관련하여 MMS 서버가 관리하는 메시지 테이블은 요청 메시지 송신 MRN, 요청 메시지 수신 MRN, 메시지 아이디, 그리고 응답 메시지로 구성된다. 서비스 요청자가 MMS 서버에게 요청 메시지를 전송하면, MMS 서버는 그 메시지를 메시지 테이블에 저장한 후 수신 MRN에 해당하는 서비스 제공자에게 전달한다. MMS 서버가 요청 메시지의 처리 결과인

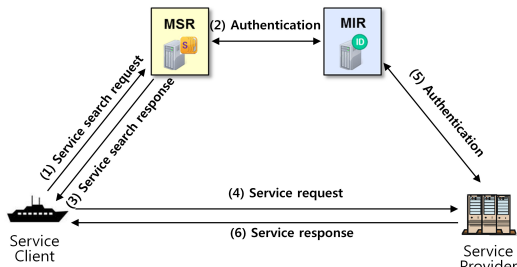


그림 4. 기존통신 방식기반의 메시지 전달 시나리오
Fig. 4. Message delivery scenario based on existing communication method

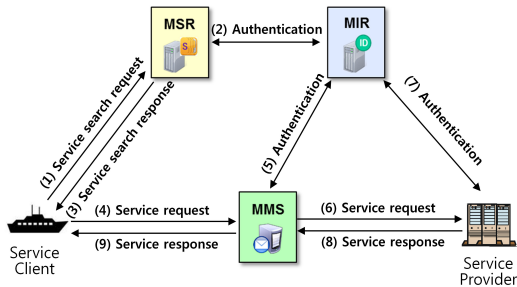


그림 5. MMS통신 방식기반의 메시지 전달 시나리오
Fig. 5. Message delivery scenario based on MMS communication method

응답 메시지를 서비스 제공자로부터 수신하면, MMS 서버는 그 응답 메시지를 메시지 테이블에 저장한다. 서비스 요청자는 이전에 전송한 서비스 요청 메시지에 대한 응답 메시지를 수신하기 위해 MMS 서버에 주기적으로 접속하여 요청하는 방법을 사용한다.

그림 6은 해사 클라우드 통신 성능을 분석하기 위한 시뮬레이션 네트워크이다. 네트워크 노드는 총 8개이며, 4개는 라우터이고 나머지는 기존통신기반 서비스 요청 노드, MMS통신기반 서비스 요청 노드, MMS 서버, 그리고 서비스 제공 노드이다. 시뮬레이션 네트워크에서 모든 링크는 10Mbps 대역폭과 25ms 지연을 갖는다. 두 서비스 요청 노드의 MRN은 각각 'urm:mrn:smart:vessel:imo-no:1234567', 'urm:mrn:smart:vessel:imo-no:1234568'로 할당하였고, 서비스 제공자의 MRN은 'urm:mrn:smart:service:instance:sv-01'로 할당하였다.

본 시뮬레이션에서, 기존통신기반 서비스 요청 노드는 초당 20개의 UDP로 된 서비스 요청 메시지를 생성하여 100초 동안 서비스 제공 노드에게 전송한다. MMS통신기반 서비스 요청 노드는 초당 20개의 UDP로 된 서비스 요청 메시지를 생성한 후 서비스 제공 노드가 수신할 수 있도록 100초동안 MMS 서버에게 전송한다. MMS통신기반 서비스 요청 노드는 버티컬 핸드오버 기능을 수행할 수 있도록 대체 네트워크 링크를 사용한다. 즉, 그림 6에서 MMS통신기반 서비스 요청 노드는 라우터-1과의 네트워크 링크상에 장애가 발생하면 즉시 라우터-2를 통해 끊김없이 MMS 서버와 통신할 수 있다.

그림 7은 두 서비스 요청 노드와 MMS 서버간 네트워크에 장애가 없는 안정적인 상태인 경우의 시뮬레이션 결과이다. 그림 7에서, 원형이 있는 선과 사각형이 있는 선은 각각 기존 통신 방식과 MMS 통신 방식을 가리키며, X축은 시간이고 Y축은 서비스 요청 노드가 서비스 제공 노드에게 요청하여 수신한 서비스

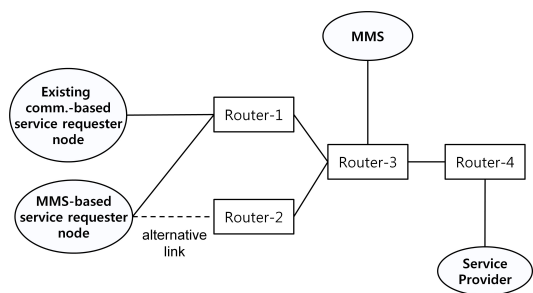
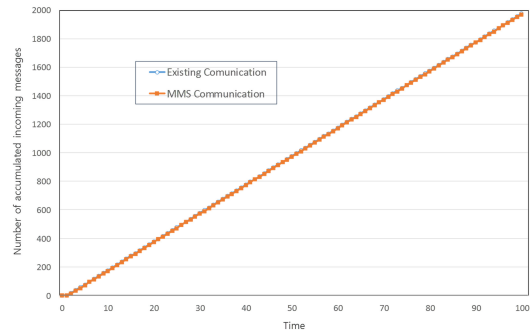
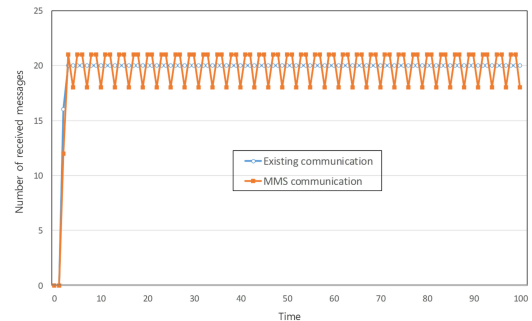


그림 6. 시뮬레이션 네트워크
Fig. 6. Simulation Network



(a) 서비스 요청자가 응답받은 메시지의 누적 합계



(b) 서비스 요청자가 응답받은 메시지의 수

그림 7. 네트워크 링크 장애가 없는 경우의 메시지 전달 성능
Fig. 7. Message delivery performance in case of no network link failure

스 응답 메시지의 수이다. 그림 7의 시뮬레이션 결과를 보면, 기존 통신 방식은 일정한 수의 서비스 응답 메시지를 일정한 시간 간격으로 안정적으로 수신하고 있지만, MMS 통신 방식은 메시지 수신 간격이 일정하지 못하는 것을 볼 수 있다. 이러한 이유는 MMS 통신 방식에서는 서비스 요청자가 MMS 서버에게 자신이 수신할 서비스 회신 메시지가 도착하였는지를 주기적으로 확인하는 과정을 수행하기 때문이다. 비록 MMS 통신 방법은 기존 통신 방법에 비해 수신한 메시지의 수에서 약간의 요동침은 있었지만, 전체적으로 볼 때 통신 성능에서 큰 차이가 없는 것을 시뮬레이션 결과를 통해 확인하였다.

그림 8은 두 서비스 요청 노드와 해사 클라우드간 대체 링크가 있는 네트워크 환경에서 네트워크 링크 장애가 발생한 경우의 시뮬레이션 결과이다. 즉, 그림 6에서 두 서비스 요청 노드와 라우터-1간 네트워크 링크상에 장애가 발생하였지만 MMS통신기반 서비스 요청 노드는 라우터-2간 네트워크 링크를 대체 링크로 사용할 수 있는 경우이다. 그림 8의 시뮬레이

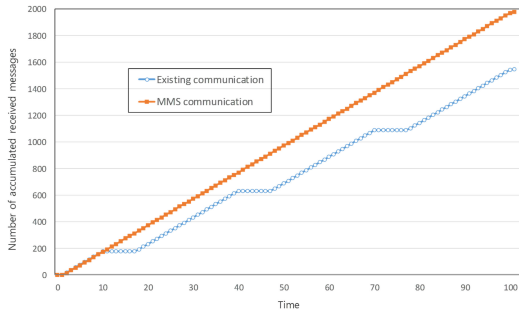


그림 8. 대체 링크가 있는 환경에서 네트워크 링크 장애가 발생한 경우의 메시지 전달 성능
 Fig. 8. Message delivery performance in case of a network link failure in an environment with alternate links

션을 위하여 두 서비스 요청 노드와 라우터-1간 링크 장애를 30초마다 발생시켰다. 기존 통신방식에서는 대체 링크를 사용자가 직접 전환해야 하는데, 그 시간은 7초라고 본 시물레이션에서는 가정하였다. 그림 8에서 Y축은 누적된 서비스 응답 메시지의 총 수이다. 시물레이션 결과, 100초 동안 두 서비스 요청 노드는 서비스 제공자에게 각각 총 1,981개의 서비스 요청 메시지를 전송하였는데, 기존 통신방식기반의 서비스 요청 노드는 총 1,549 개의 서비스 응답 메시지를 수신하였지만 MMS 통신 방식기반의 서비스 요청 노드는 모든 서비스 응답 메시지를 손실 없이 수신하였다. 그림 8의 시물레이션 결과를 종합하면, 기존 통신 방식의 메시지 전달 성능은 78.2%이었으며, MMS 통신 방식의 메시지 전달 성능은 100%로 계산된다. 따라서 본 시물레이션에서는 MMS 통신 방식이 기존 통신 방식보다 메시지 전달 성능에서 21.8% 더 우수하였다. MMS 통신 방식이 기존 통신 방식보다 더 성능이 우수한 이유는 해사 클라우드의 MMS 서버는 네트워크 대체 링크를 이용하여 끊임없는 통신 로밍 서비스를 제공하기 때문이다.

그림 9는 두 서비스 요청 노드와 해사클라우드간에 대체 링크가 없는 네트워크 환경에서 네트워크 장애가 발생한 경우의 시물레이션 결과이다. 즉, 그림 6에서 두 서비스 요청 노드와 라우터-1간 그리고 두 서비스 요청 노드와 라우터-2간 네트워크 링크에 장애가 동시에 발생한 경우이다. 본 시물레이션에서는 두 서비스 요청 노드와 라우터-1간 링크 장애를 10초마다 발생시켰다. 그림 8에서 Y축은 누적된 서비스 응답 메시지의 총 수이다. 시물레이션 결과, 100초 동안 두 서비스 요청노드는 서비스 제공자에게 각각 총 1,981개의 서비스 요청 메시지를 전송하였는데, 기존 통신 방식기반의 서비스 요청 노드는 총 1,045개의 서비스

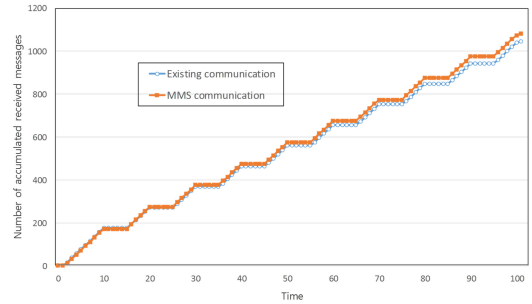


그림 9. 대체 링크가 없는 환경에서 네트워크 링크 장애가 발생한 경우의 메시지 전달 성능
 Fig. 9. Message delivery performance in case of a network link failure in an environment without alternate links

응답 메시지를 수신하였고, MMS 통신 방식기반의 서비스 요청 노드는 총 1,081개의 서비스 응답 메시지를 수신하였다. 그림 9의 시물레이션 결과를 종합하면, 기존 통신 방식의 메시지 전달 성능은 52.8%이었으며, MMS 통신 방식의 메시지 전달 성능은 54.6%로 계산된다. 따라서 1.8%로 비록 작은 차이지만 MMS 통신 방식이 기존 통신 방식보다 메시지 전달 성능에서 더 우수하였다. MMS 통신 방식이 기존 통신 방식보다 성능에서 우수한 이유는 MMS 서버는 링크 장애 때문에 서비스 요청자에게 전송하지 못한 메시지들을 메시지 테이블에 저장하고 있기 때문이다.

V. 결론

스웨덴과 덴마크 등 많은 해양국가에서는 인적과실에 의한 해난사고를 예방하기 위한 목적으로 ICT 기술을 활용하여 선박과 육상간 또는 선박과 선박간 정보공유를 제공하는 e-내비게이션을 도입하고 있다. 본 논문에서는 한국형 e-내비게이션을 개발할 때 가장 우선적으로 고려해야 할 사항 중의 하나인 해사 엔터티의 아이디 식별체계를 제안하였다. 제안하는 식별체계는 한국에서 사용하는 고유한 선박 아이디 유형을 지원하며, 선박 아이디를 자동으로 할당함으로써 대량의 선박을 e-내비게이션의 통신 인프라인 해사 클라우드에 효율적으로 등록할 수 있다.

본 논문에서는 또한 끊임없는 서비스를 제공하는 MMS 통신방식과 기존 해양 통신방식중에서 어떤 방식이 해사 클라우드에서 더 우수한지를 확인하기 위하여 시물레이션을 하였다. 시물레이션 결과, MMS 통신방식이 대체 링크가 있는 환경에서 뿐만 아니라 대체 링크가 없는 통신 환경에서도 기존 통신방식보

다 메시지 전달 성능에서 더 우수하였다.

본 논문에서 제안하는 해사 엔터티의 아이디 식별 체계가 실제의 e-내비게이션 환경에 적용되었을 때 문제는 없는지 그리고 선박 아이디를 할당함에 있어서 얼마나 효율적인지에 대한 실험 및 검증 과정이 필요하다. 이에 대한 연구는 향후연구과제로 남긴다.

References

- [1] H. K. Cho, B.S. Park, D.H. Kang, and S. S. Kim, "The main factor and counterplan for marine accidents in Korea," *J. Korean Soc. for Fisheries and Marine Sci. Edu. (JFMSE)*, vol. 29, no. 3, pp. 746-756, Aug. 2017.
- [2] IMO, e-navigation, Retrieved April 2017, from <http://www.imo.org/en/OurWork/Safety/Navigation/Pages/eNavigation.aspx>.
- [3] K. I. Lee, G. I. An, J. Y. Park, H. J. Lee, and B. H. Chung, "An identification and authentication scheme for maritime digital communication infrastructure," in *Proc. Int. Conf. Advanced Intell. Maritime Safety and Technol. (Ai-MAST)*, Daejeon, Korea, Nov. 2015.
- [4] The Maritime Cloud Development Forum, "Maritime cloud conceptual model," *Int. Assoc. Lighthouse Authorities (IALA)*, ENAV20-9.19, Mar. 2017.
- [5] The Maritime Cloud Development Forum, "Identity management and cyber security," *Int. Assoc. Lighthouse Authorities (IALA)*, ENAV19-9.13, Sept. 2016.
- [6] The Maritime Cloud Development Forum, "Specification guideline for Technical Services," *Int. Assoc. Lighthouse Authorities (IALA)*, ENAV19-9.14.1, Sept. 2016.
- [7] Korea Research Institute of Ships and Ocean engineering (KRISO), SMART navigation project, Retrieved Nov. 2017, from <http://www.smartnav.org/html/Index>.
- [8] G. I. An, G. I. Lee, and B. H. Chung, "Analysis of cyber-security threat on maritime cloud proposed as maritime communication framework," in *Proc. KIISE Winter Conf. 2015*, pp. 892-893, Pyeongchang, Korea, Dec. 2015.
- [9] G. I. An and B. H. Chung, "Design of maritime user management system for safe e-Navigation service," in *Proc. KICS Summer Conf. 2017*, pp. 1082-1083, Jeju, Korea, Jun. 2017.
- [10] G. I. Lee and P. R. Kim, "A study on the development of SMART navigation service Management technology using maritime messaging service communication," in *Proc. KINPR Fall Conf. 2017*, pp. 132-133, Busan, Korea, Nov. 2017.
- [11] W. S. Jang, B. J. Kim, and M. S. Kang, "Analysis of the AMQP for data message queuing of Korean e-Navigation operation system," in *Proc. KINPR Fall Conf. 2017*, pp. 132-133, Busan, Korea, Nov. 2017.
- [12] G. I. An, D. Y. Chung, and B. H. Chung, "Architecture of vessel ID importation system for efficient registration of maritime ID in maritime cloud environment," in *Proc. KINPR Fall Conf. 2017*, pp. 132-133, Busan, Korea, Nov. 2017.
- [13] The Maritime Cloud Development Forum, Maritime Cloud, Retrieved Nov. 2017, from <https://github.com/MaritimeCloud>.
- [14] K. Nielsen, "Maritime resource names (MRN)," *IETF*, draft-knielsen-mrn-urn-00, Feb. 2017.
- [15] Putzis, P. Stjernström, Skillzore, and J. Almén, Software engineering project spring 2017, Retrieved Oct. 2017, from <https://github.com/pontusstjerna/SEProject/blob/master/README.md>
- [16] NS3 project, NS3 network simulator, Retrieved Jan. 2016, from <https://www.nsnam.org>

안 개 일 (Gaeil An)



1992년 2월 : 충남대학교 컴퓨터 공학과 졸업
1995년 2월 : 충남대학교 컴퓨터 공학과 석사
2001년 8월 : 충남대학교 컴퓨터 공학과 박사
2006년 7월~2007년 6월 : 시라큐스대학교 포닥연구원

2001년 8월~현재 : 한국전자통신연구원 책임연구원
<관심분야> 정보보호, 네트워크 시뮬레이션, 해양 선박 보안, 사이버보안 정보공유

정 병 호 (Byungho Chung)



2005년 7월 : 충남대학교 컴퓨터 과학과 박사
1988년 2월~2000년 6월 : 국방과학연구소 선임연구원
2000년 6월~현재 : 한국전자통신연구원 책임연구원
<관심분야> 정보보호, 무선네트워크 프로토콜, 기계학습

정 도 영 (Doyoung Chung)



2010년 2월 : KAIST 전산학과 졸업
2012년 2월 : KAIST 전산학과 석사
<관심분야> 해양·선박 보안, e-navigation 보안