JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 25, No. 5: 701~708, May. 2021

보안 DDS(Data Distribution Service)의 디스커버리 및 메시지 전송 성능 분석

임진용*

Performance Evaluation of Discovery and Message Transmission of DDS (Data Distribution Service) Security

Jinyong Im*

*Engineer, Infra SW Team, Hanwha Systems, 188, Pangyoyeok-Ro, Bundang-Gu, Seongnam-Si, Gyeonggi-Do, 13524 Korea

요 약

본 논문에서는 보안 기능이 추가된 DDS(Data Distribution Service)의 디스커버리 및 메시지 전송 성능에 대해 분석한다. DDS는 분산 환경에서 실시간 통신을 위한 발간-구독 방식의 통신 프로토콜을 제공한다. 발간-구독 방식은 성능, 확장성 그리고 가용성 측면에서 강점을 가지며 국방, 교통, 의료 등 다양한 분야에서 사용되고 있다. 최근 급증하는 보안 위협에 대비하기 위해 많은 통신 표준에서 보안 기능을 추가 및 재정의 하였으며, DDS 또한 보안 기능이 추가된 표준이 발표되었다. 하지만 보안 DDS의 기능 사용을 위해 증가한 오버헤드가 기존 시스템에 미칠 영향성에 대한 연구는 이루어 지지 않았다. 실험 결과는 기존 DDS와 보안 DDS의 디스커버리 및 메시지 전송 성능을 비교하여 보여준다.

ABSTRACT

In this paper, I investigate the performances of the discovery and the message transmission of the DDS (Data Distribution Service) included the security function. The DDS serves the communication protocol, a publication- subscription method, for the real-time communication in the distributed system. The publication-subscription method is used in the various area in terms of defence, traffic and medical due to the strength such as a performance, scailability and availability. Nowadays, many communication standard has included and re-defined the security function to prepare from dramatically increased a threat of the security, the DDS also publishes the standard included the security function. But it had been not researched that the effect of increased a overhead for legacy systems due to the using of the security DDS function. The experimental results show that the comparative performance of legacy DDS and security DDS in terms of the discovery and the message transmission.

키워드 : DDS 통신, 보안, 디스커버리, 메시지 전송, 암호화

Keywords : DDS (Data Distribution Service) communication, Security, Discovery, Message transmission, Cryptographic

Received 23 October 2020, **Revised** 16 December 2020, **Accepted** 23 December 2020

*** Corresponding Author** Jinyong Im(E-mail: jinyong.im@hanwha.com, Tel:+82-31-8091-3782)
Engineer, Hanwha Systems, 188, Pangyoyeok-Ro, Bundang-Gu, Seongnam-Si, Gyeonggi-Do, 13524 Korea

Open Access http://doi.org/10.6109/jkiice.2021.25.5.701 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

DDS(Data Distribution Service)는 OMG(Object Management Group)에서 표준화한 통신 미들웨어이다. DDS는 분산 환경에서 실시간 통신을 위한 발간/구독 방식을 지원하며, 성능, 확장성 그리고 가용성 측면에서 강점을 가진다. 이러한 강점 때문에 국방, 교통, 의료 분야 등 다양한 산업시스템에서 사용되고 있다[1-2].

하지만 최근 국방 혹은 사회 기간사업에 대한 보안 위협이 지속적으로 증가하는 상황에서 기존 DDS는 자체 보안기능이 없어 보안 위험이 항상 존재한다. DDS는 발간/구독 방식의 통신이기 때문에 동일 네트워크 Domain에 존재하는 Participant에 대해 통신 메시지의 감청, 위조 및 변조 등이 가능한 취약점이 있다.

OMG는 위의 보안 위협에 대한 문제점 해결을 위해 DDS Security(이하 보안 DDS)표준을 발표하였다[3]. 보안 DDS는 인증(Authentication), 접근제어(Access Control), 암호화(Cryptographic)그리고 로깅(Logging) 기능으로 구성되며 보안을 위한 기능 별 역할은 아래와 같다[4].

1) 인증 및 접근제어 : DDS 통신 시작 전 Participant 상호 인증과 접근권한 확인
2) 암호화 : DDS 통신 메시지 암/복호화를 통해 기밀성 및 무결성 보증

이러한 보안 DDS의 기능은 통신 중 주고받는 메시지에 대한 암/복호화 연산을 통해 기밀성을 유지한다. 이때 암/복호화 연산으로 인해 필연적으로 처리지연시간이 발생하며, 해당 지연은 실시간성을 저해하는 요소로 작용한다.

본 논문에서는 기존 시스템에 보안 DDS가 적용 될 경우 해당 지연이 미칠 수 있는 영향에 대해 분석하고자 한다. 이를 위해 보안 DDS의 Discovery 성능 및 기존 DDS와 보안 DDS의 메시지 전송 성능을 분석한다. 시험 결과는 기존 시스템에 보안 DDS를 적용할 경우와 신규 시스템을 설계 할 때 참고자료로 활용 될 수 있다.

2장에서는 관련 연구에 대해 다루며 3장에서는 기존 DDS와 보안 DDS의 성능차를 확인하기 위한 시험의 시나리오와 결과에 대해 설명한다. 마지막 4장에서는 결론 및 향후 연구에 대해 다룬다.

Ⅱ. 관련 연구

본 장에서는 기존 DDS와 보안 DDS에 대한 관련 연구를 다룬다.

2.1. DDS (Data Distribution Service)

DDS는 OMG에서 표준화한 발간(Publish)/구독(Subscribe) 모델 기반 실시간 데이터 통신 미들웨어이다. DDS는 분산 환경에서 데이터 중심 프로그램 모델에 대한 신뢰성을 제공하고 각 Node간의 실시간 통신을 지원한다[1-2].

이러한 DDS는 동일 네트워크에서 메시지를 송수신하는 응용 프로그램의 위치와 무관하게 상호간 데이터 교환이 가능하다. 이를 통해 사용자는 네트워크 프로그래밍을 단순화하여 분산 환경의 응용 프로그램 설계 및 구현을 단순화시킬 수 있다.

DDS 표준은 DDS API 표준을 서술한 DCPS(Data Centric Publisher/Subscriber)와 네트워크 계층 통신 프로토콜을 서술한 RTPS(Real-Time Publish-Subscribe)로 구성된다. DCPS는 발간/구독 모델 기반의 데이터 교환 기능에 대한 인터페이스 표준을 정의한다. 그림 1은 DDS 미들웨어의 통신 구조를 나타내고 있다. 발간자(Publisher)는 전송할 데이터를 생성하고 배포하는 기능을 제공하기 위해 하나 이상의 발간 개체(DataWriter)를 생성해 데이터를 송신한다. 구독자(Subscriber)는 발간 개체와 대응하는 구독 개체(DataReader)를 생성해 데이터를 수신한다.

이때, 발간자와 구독자는 동일한 DDS 네트워크 도메인(Domain)에 참여한 상태여야 하고 데이터는 DDS의 토픽(Topic)이라는 개념으로 정의된다. 또한 DDS 표준은 토픽 데이터 전달의 신뢰성과 실시간성을 위해 여러

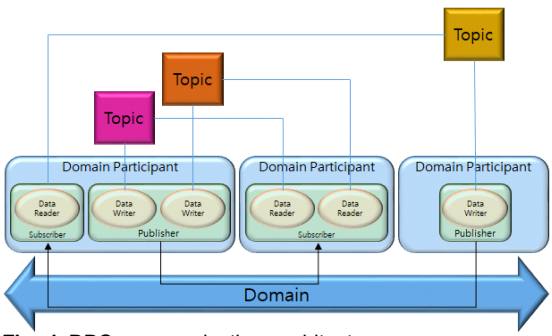

Fig. 1 DDS communication architecture.

QoS(Quality Of Service) 설정을 제공하고 있다. RTPS는 실제 메시지 전송과 수신을 담당하는 데이터 전송 프로토콜로서 UDP(User Datagram Protocol)/IP와 같은 전송계층 위에서도 동작 가능하도록 설계되어있다. RTPS에서는 DCPS에서 정의한 발간/구독 객체가 실제 통신하기 위해 필요한 디스커버리(Discovery), 데이터 코딩 방식, 메시지 포맷 및 교환방식, 전송 절차 등에 대한 사항을 정의하고 있다[2].

2.2. DDS Discovery

DDS는 Endpoint라고 부르는 DDS Entity간의 정보 교환을 필요로 하며, 사용자가 통신을 위해 만든 미들웨어 객체로서 메시지의 발간개체/구독개체(DataWriter/DataReader)가 이에 해당한다. 이 정보를 사전에 서로 교환하는 것이 DDS Discovery 과정이다. 그림 2는 Discovery 과정을 개략적으로 보여준다. Discovery는 그림과 같이 Phase1의 SPDP(Simple Participant Discovery Protocol) 메시지와 Phase2의 SEDP(Simple Endpoint Discovery Protocol) 메시지를 이용하여 정보를 교환한다. Simple Discovery Protocol 에서 SPDP 메시지는 멀티캐스트로 송신된다. SPDP의 교환으로 미들웨어는 다른 노드의 DDS Entity, IP, port 등의 정보를 취득하게 되고 이 IP, port 를 이용하여 SEDP 정보를 유니캐스트 통신을 이용하여 교환한다[5].

Discovery 과정에서 자세한 데이터 교환에 대한 내용은 그림 3에서 보여준다. 최초 DDS Participant#1이 생성되면 자신의 정보를 동일한 네트워크에 존재하는 다른 Participant#2 혹은 다수의 Participant에게 멀티캐스트 통신을 통해 송신한다. 해당 메시지를 수신한 Participant#2는 응답으로 자신의 정보를 송신하고 Participant#1이 해당 정보를 수신함으로써 SPDP 과정이 종료된다. SPDP

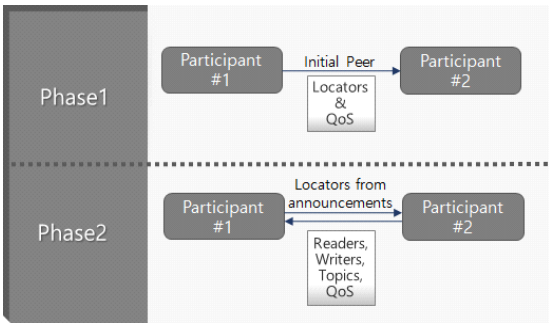

Fig. 2 Discovery process for simple.

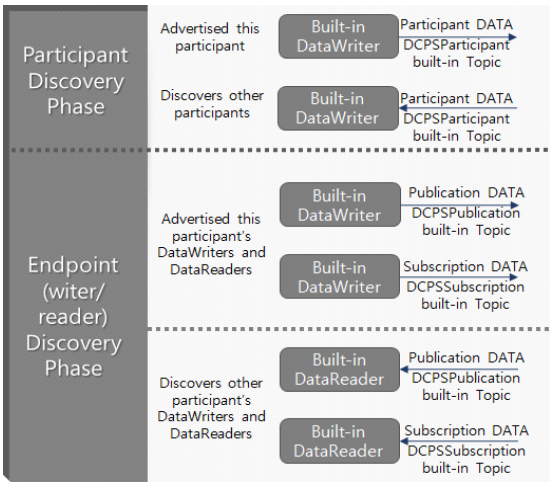

Fig. 3 Discovery process for detail.

종료 후 Participant#1은 자신이 가지는 Endpoint인 DataWriter와 DataReader에 대한 정보를 Participant#2에 유니캐스트 통신을 통해 송신한다. Participant#2는 해당 메시지 수신 후 자신의 DataWriter와 DataReader 정보를 다시 Participant#1에 송신한다. 이때 Participant#1과 Participant#2가 같은 Topic을 사용한다면 Discovery 과정은 완료되고, 이후 사용자는 해당 Topic을 자유롭게 발간/구독하여 통신을 수행할 수 있다[6-8].

2.3. DDS Security

DDS의 특징인 발간/구독 방식의 통신은 보안 측면에서 큰 단점으로 작용하며, 대표적인 이유는 아래와 같다[9].

1) 송/수신지의 Validation 단계 부재
2) 송/수신지의 권한 검토 단계 부재
3) 전송 데이터 암/복호화 단계 부재

아래의 그림 4를 통해 위의 대표적인 3가지 문제를 가진 기존 DDS의 보안 위협에 대한 예시가 설명 가능하다. 아래 그림에서 Alice와 Bob이 일반 사용자이다. 앞

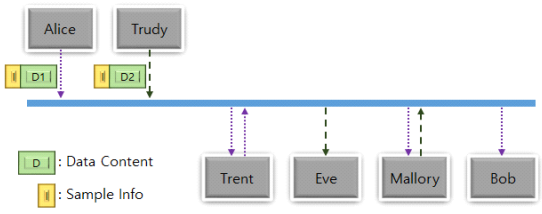

Fig. 4 Example of Security threat.

서 설명하였던 DDS Discovery 과정 후 데이터 전송이 이루어지는데 이때 Discovery 과정이 완료된 상대는 Alice가 Bob에게 송신하는 데이터에 대해 수신이 가능하다. 때문에 데이터의 감청 혹은 감청한 데이터를 재가공하여 보내거나 수신지를 속이는 위험이 항상 존재한다.

위와 같은 문제를 해결하여 보안 위협에 대응하기 위해 기존 DDS에 보안 기능을 추가한 OMG의 DDS Security(이하 보안 DDS) 표준이 발표 되었다. 보안 DDS 표준은 보안 기능 제공을 위해 인증, 접근제어, 암호화, 로깅 기능을 제공한다. 제공되는 기능들은 기존 DDS 응용의 변경 없이 사용 가능하도록 SPI(Service Plug-in Interface)형태로 설계 및 구현되었다.

보안 DDS 표준에 따른 네트워크 통신은 데이터 교환 전 상호간의 인증과 권한확인 절차를 수행한다. 인증 과정에서 각 Node 내부의 Participant는 자신이 사용하는 인증서를 타 Participant와 교환 후 상호 권한을 확인/증명한다. 이 과정에서 각 Participant는 추후 통신에서 사용할 비밀키(Secret Key)를 각자 생성 후 공유한다. 권한확인 절차에서 상호간의 송/수신 권한과 도메인의 보안 정책을 확인 후 비인가 Participant의 통신참여를 제한한다.

인증 및 권한확인 후 각 Participant의 Discovery 과정이 완료되면 상호간 통신이 가능하다. 이때 전송되는 메시지는 암호화를 통해 보호된다. OMG의 보안 DDS 표준에서는 128bit와 256bit 암호화키를 이용한 DDS 메시지 암/복호화를 정의하고 있다. DDS 메시지 암호화는 Payload 암호화, Submessge 암호화, RTPS message 암호화 3단계로 이루어진다[4].

각 암호화 과정은 메시지를 암호화된 데이터로 변환하고 헤더(Header)와 태그(Tag)를 삽입해 암호화 정보와 무결성을 확인한다. 이때 각 암호화 방법은 단계별 독립적으로 이루어지며 사용자는 제공 되는 QoS를 통해 암호화 방법을 결정할 수 있다. 보안 설정 별 전송 메시지의 구조는 표 1에서 보여준다. 총 네 개의 방식으로 나뉘며, NONE(암호화 및 사인 사용하지 않음), SIGN(사인만 사용), ENCRYPT(암호화만 사용), SIGN& ENCRYPT(사인과 암호화 둘 다 사용)가 있다.

Table. 1 Message structure by security level.

Security Level	NONE	SIGN	ENCRYPT	SIGN & ENCRYPT
Message Structure	User Data	User Data Sign	Encrypted User Data	Encrypted User Data Sign

이를 위해 보안 DDS에서는 여러 파일을 사용하며 종류 및 각 역할은 아래와 같다.

1) CA 인증서 파일:
- CA 인증 정보 및 Public Key 정보
- Peer 인증 정보 검증을 위해 사용
- 기타 설정 파일의 유효성 검증을 위해 사용

2) Peer 인증서 파일:
- 해당 Peer 인증 정보 및 Public Key 정보
- 유효한 Peer 임을 증명하기 위해 사용

3) Peer 개인키 파일:
- Peer 인증 정보에서 추출된 개인키
- Discovery 과정 중 Participant간 핸드쉐이킹 메시지의 암호화에 사용

4) Governance 파일:
- 접근 제어 및 암호화 옵션 설정(비인증 Peer 접근 허가, 암호화 범위 등)

5) 접근 권한 설정 파일:
- 접근 제어 옵션 설정(Domain, Participant, Topic 등)

위의 기능 설명에서 유추 가능하듯 보안 DDS에서는 사용자 인증, 접근 제어, 암호화 등의 기능을 지원하기 위한 오버헤드가 기존 DDS에 대비해 증가했다. 그 중 DDS 초기 구동 단계인 Discovery 과정에 대한 부하가 급증하게 되었다.

기본적으로 DDS 통신이 진행되기 위해서는 앞서 설명한 DDS Discovery의 안정적인 수행을 통한 다른 Participant 및 Entity와 정보 교환이 필요하다. 하지만 Discovery 과정의 특성 상 동일 네트워크에 존재하는 Participant의 수가 증가할수록 Discovery 과정 중 발생하는 네트워크 및 프로세싱 부하는 급증하고 이를 DDS Discovery Storm 현상이라 칭한다. 이때 간혹 일부 참가자들의 Discovery 과정이 끝나지 않는 상황이 발생한다. 이러한 DDS Discovery Storm 현상의 최소화를 위해 다양한 형태로 Discovery 과정 중 부하를 줄이는 기법들이 기존 DDS에는 적용되었다.

하지만 보안 기능의 추가로 인해 기존 방식으로는 해결할 수 없을 정도의 네트워크 및 프로세싱 부하가 발생하게 되었다. 가장 큰 부하 원인은 Participant 간 상호 Validation 단계를 위해 교환하는 사용자 인증서와 보안

권한 문서의 내용이다. PKI(Public Key Infrastructure) 기반의 사용자 인증 기능을 사용하는 보안 DDS에서 사용자 인증서는 PK7CS 포맷을 사용한다. 해당 파일의 크기는 2~4 KB 범위 안에서 결정된다.

권한 문서의 경우 SMIME 형식의 포맷을 갖는 XML 타입 문서이며, CA 인증서로 디지털 서명이 들어간 형태를 가진다. 크기는 권한 문서의 구성 및 네트워크 규모에 따라 달라질 수 있으나, 대부분 60KB 이상의 크기를 갖게 된다. 보안 DDS의 Discovery Storm 현상 시 대부분의 네트워크 부하는 이 권한 문서이다[9].

동일 네트워크에 1000개의 Participant가 Discovery를 수행할 경우 트래픽의 양은 1000*999*60KB = 59GB이다. 이러한 트래픽 양은 급작스러운 네트워크 부하를 야기한다. 또한 Participant 들은 이 권한 문서를 처리하고 분석하는 과정이 필요하기 때문에 높은 처리 지연시간까지 고려할 경우 원활한 Discovery의 진행이 힘들어진다.

Ⅲ. 보안 DDS 성능 시험

3.1. Discovery 성능 시험

본 절에서는 보안 DDS의 Discovery 성능 측정을 위한 시험과 기존 DDS와 보안 DDS의 메시지 전송 성능을 비교 및 분석한다.

보안 DDS의 Discovery 성능을 측정하기 위한 시험 환경은 그림 5와 같다. 각 노드에는 보안 DDS를 사용하는 시험 응용이 실행되며 모든 노드는 동일한 네트워크에 연결된 환경에서 시험을 진행한다. 사용한 장비의 경우 표 2에 기술하였다. 각 노드는 가상화 환경의 VM을 사용하며, 모든 노드는 10GB의 통신 환경에서 동작된다.

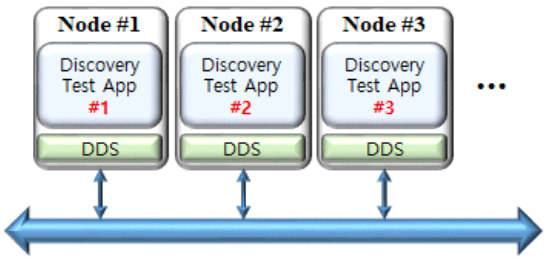

Fig. 5 Environment for discovery test.

Table. 2 H/W environment for test.

H/W	No.	Spec
VM	42	CPU: Intel Xeon Gold 6140 2.3 GHz Memory: 12 GB
Switch	3	Cisco NEXUS 3172PQ (10G)

보안 DDS의 Discovery 시험 결과 측정은 각 노드의 시험 응용에서 Participant 생성 후 동일 네트워크에 존재하는 모든 Participant와 Discovery 과정이 끝나는 시점을 측정하였다. Discovery의 경우 각 노드 내부의 Participant별로 종료 시점이 다르기 때문에 모든 Participant 중 Discovery 소요 시간이 가장 긴 Participant의 값을 결과로 사용하였다.

시험 결과는 표 3과 같다. 총 42개의 노드에서 진행하였으며, 각 노드에 1개의 Participant가 존재할 경우에는 Discovery가 완료되었다. 하지만 각 노드당 5개 혹은 10개의 Participant가 존재할 경우에는 앞서 설명하였던 Discovery Storm 현상으로 인해 일부 Participant의 Discovery가 완료되지 않았다. 원활한 DDS 통신을 위해서는 모든 Participant가 상호간 Discovery 과정을 완료해야한다. 만약 1개 이상의 Participant가 Discovery에 실패할 경우 시스템 전체의 성능에 영향을 미칠 수 있다.

Table. 3 Results of discovery test.

Total No. of participant	Results [s]
42	18
210	X
420	X

3.2. 메시지 전송 시험

본 절에서는 기존 DDS와 보안 DDS의 메시지 전송 성능에 대해 비교 및 분석을 진행한다. 보안 DDS의 경우 기존 DDS 대비 암호화 기능으로 인한 오버헤드가 메시지 전송 시 추가적으로 발생한다. 이러한 오버헤드가 과도할 경우 기존 시스템에서 보안 DDS 사용 시 실시간성에 위배될 가능성이 존재한다.

시험의 경우 총 4대의 노드를 사용하여 진행하였으며, Windows OS와 Linux OS 각각 2대씩 사용하였다. 네트워크 스위치의 경우 Discovery 성능 시험에서 사용한 모델과 동일 모델을 사용하여 10G 환경에서 진행하였다. 메시지 전송을 위한 시험 시나리오는 표 4와 같다. 송수신측의 OS를 변경하며 시험한 이유는 OS별로 시

스템 자원을 사용할 때의 성능이 다르기 때문이며, 이를 통해 시스템 설계 시 적절한 OS 선택에 도움이 될 수 있다.

결과 값 측정 방법은 그림 6에서 보여주고 있다. 최초 Sender에서 Test Msg를 Receiver에 송신하고, 이를 수신한 Receiver는 Eco Msg를 송신한다. Sender에서 해당 Eco Msg를 수신 후 시험이 종료되며 이때까지의 총 소요 시간을 측정하여 결과 값으로 사용하였다.

Table. 4 OS for each node.

Case	Sender OS	Receiver OS
1	Windows	Windows
2	Windows	Linux
3	Linux	Windows
4	Linux	Linux

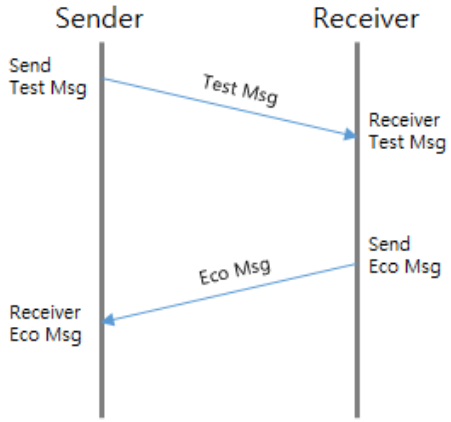

Fig. 6 Scenario of msg transmission test.

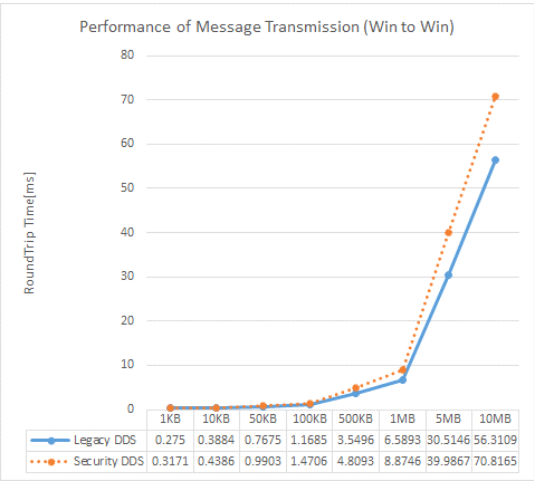

Fig. 7 Result of DDS msg transmission(win to win).

그림 7에서는 송신측(Windows)과 수신측(Windows) 간 메시지 전송 성능을 기존 DDS와 보안 DDS를 비교하여 보여준다. 전송 시험 시 메시지의 크기 또한 중요한 요소이기 때문에 변경하며 시험을 진행 하였다.

송신측(Windows)과 수신측(Windows) 간 메시지 전송 성능에서 메시지 크기가 커질수록 기존 DDS와 보안 DDS의 성능차이가 커지는 것을 확인 할 수 있다. 원인은 메시지의 크기가 커질 경우 전송 메시지의 암/복호화에 필요한 프로세싱 소요 시간이 커지기 때문이다. 따라서 10MB 메시지 전송 기준으로 볼 경우 성능 차이는 약 14[ms]이며, 이를 통해 Windows에서 보안 DDS를 사용할 경우 10MB 메시지 암/복호화 1회에 필요한 시간이 약 3.5[ms]임을 추측할 수 있다.

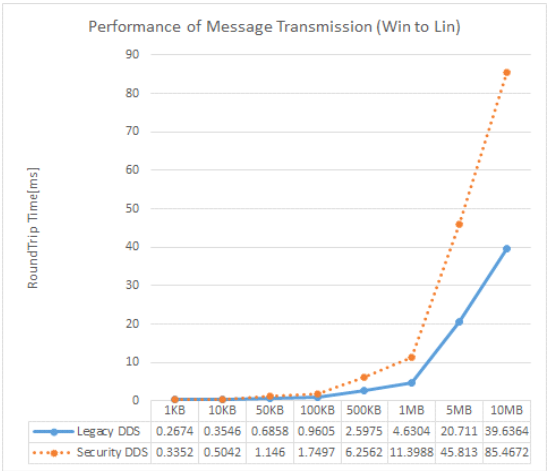

Fig. 8 Result of DDS msg transmission(win to lin).

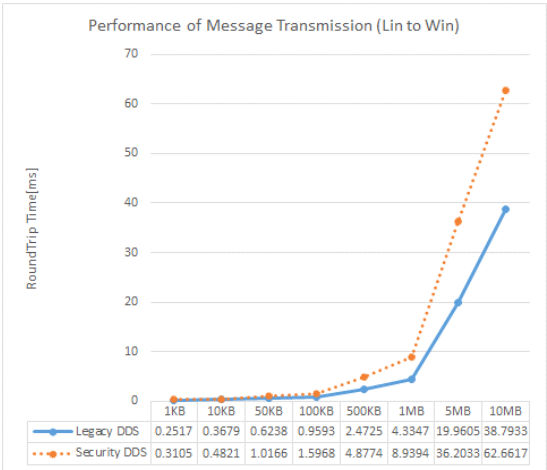

Fig. 9 Result of DDS msg transmission(lin to win).

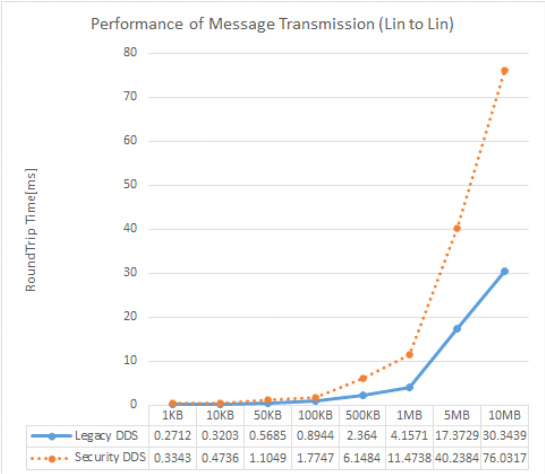

Fig. 10 Result of DDS msg transmission(lin to lin).

그림 8, 그림 9 그리고 그림 10에서는 Linux OS가 포함된 시나리오의 결과를 보여준다. 결과의 차이는 기존 DDS와 보안 DDS의 결과 폭이 크다는 점이다. 보안 DDS 전송 성능만을 따져보았을 때는 네 개의 시험의 차가 크지 않기 때문에 이러한 결과의 원인은 Linux가 Windows보다 기존 DDS의 처리 속도가 빠르기 때문으로 판단된다. 이러한 차이는 각 OS의 쓰레드 스케줄링, 메모리 접근 및 파일 입출력 방식의 성능 차이 때문이다 [10].

이러한 결과를 통해 기존 DDS만을 사용하는 환경에서는 Linux OS가 강점을 보였다. 하지만 보안 DDS의 기능 중 동일한 메시지 암/복호화 방식을 사용할 경우 OS 별 성능차이는 크게 존재하지 않음을 알 수 있다.

Ⅳ. 결 론

본 논문에서는 기존 DDS의 보안 위협을 해결하기 위해 보안 기능이 추가된 보안 DDS의 Discovery 및 메시지 전송 성능을 분석하였다.

보안 DDS의 기능을 위해 추가된 작업으로 인해 기존 DDS 대비 상대적으로 성능이 저하되었다. 특히, Discovery의 경우 Participant의 수가 많아질 경우 급격히 증가된 네트워크 패킷과 처리량에 의한 Discovery Storm 현상으로 Discovery가 완료되지 않았다. DDS 통신의 특성상 상호간 메시지 전송을 위해서는 Discovery 과정이 필수이기 때문에 보안 DDS를 사용할 경우 동일 네트워크 내 Participant 수를 일정 수준 유지하도록 시스템을 설계할 필요성이 있다.

메시지 전송 성능 시험의 경우 Windows OS와 Linux OS의 프로세싱 성능 차이로 인해 송신과 수신 측 OS에 따른 메시지 전송 성능이 차이를 보였다.

향후에는 보안 DDS의 Discovery 성능 향상 방안과 메시지의 종류 및 크기에 따른 DDS QoS 최적화에 대해 연구하겠다.

References

[1] OMG, *Data Distribution Service for Real-time Systems Version 1.4*, Apr. 2015.

[2] OMG, *The Real-time Publish-Subscribe Protocol (RTPS) DDS Interoperability Wire Protocol Specification*, Sep. 2014.

[3] OMG, Std. *DDS Security Version 1.1*, OMG, 2018.

[4] J. H. Han, "Message Encryption Methods for DDS Security Performance Improvement," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 22, no. 11, pp. 1554-1561, Nov. 2018.

[5] M. G. Kang, H. J. Jun, and Y. S. Choi, "A Effective Sending Message Mechanism for Smart DDS in Multi-node," in *Proceeding of the 2014 Conference of Korea Institute of Military Science and Technology*, Jeju, pp. 444-445, 2014.

[6] RTI community. Discovery [Internet]. Available: https://community.rti.com/glossary/discovery.

[7] RTI Open topic with navigation. *Simple Participant Discovery* [Internet]. Available: https://community.rti.com/static/documentation/connext-dds/5.2.3/doc/manuals/connext_dds/html_files/RTI_ConnextDDS_CoreLibraries_UsersManual/Content/UsersManual/Simple_Participant_Discovery.htm.

[8] RTI Open topic with navigation. *Simple Endpoint Discovery* [Internet]. Available: https://community.rti.com/static/documentation/connext-dds/5.2.3/doc/manuals/connext_dds/html_files/RTI_ConnextDDS_CoreLibraries_UsersManual/Content/UsersManual/Simple_Endpoint_Discovery.htm.

[9] J. W. Lee, "A Study on the OMG DDS Security Spec's Lightweight Necessity," in *Proceeding of 2019 Conference of Korea Institute of Military Science and Technology*, Daejeon, pp. 306-307, 2019.

[10] W. Fan, C. Wong, W. Lee, and S. Hwang, "Comparison of

Interactivity Performance of Linux CFS and Windows 10 CPU Schedulers," in *Proceeding of 2020 International Conference on Green and Human Information Technology (ICGHIT)*, Hanoi, pp. 31-34, 2020.

임진용(Jinyong Im)

2014년 금오공과대학교 전자공학부 학사 졸업.
2016년 동대학 대학원 IT융복합공학과 석사 졸업.
2016년 ~ 현재 동대학 대학원 IT융복합공학과 박사 과정 수료.
2017년 ~ 현재 한화시스템 근무.
※관심분야 : 함정전투체계, DDS, 네트워크 기반 분산제어 시스템