논문 20-45-12-16 The Journal of Korean Institute of Communications and Information Sciences '20-12 Vol.45 No.12
https://doi.org/10.7840/kics.2020.45.12.2123

PFDP 기반 DDS Security의 경량화 디스커버리 기법

이 주 원◆, 차 중 혁*, 이 종 우*, 김 경 선*, 김 동 성°

PFDP-Based DDS Security Lightweight Discovery Scheme

Ju-Won Lee◆, Joong-Hyuck Cha*, Jong-Woo Lee*, Gyeong-Seon Kim*, Dong-Seong Kim°

요 약

DDS(Data Distribution Service)는 높은 확장성을 바탕으로 무기공개 시스템 구조(weapon open system architecture)의 네트워크 미들웨어로 채택되고 있다. DDS의 확장성은 디스커버리 절차의 선행을 통해 제공되는데, 통신 참여자의 수가 증가함에 따라 네트워크 구성에 높은 수준의 네트워크, 메모리 및 컴퓨팅 리소스를 요구한다. 특히, 보안 성능이 강화된 DDS Security는 디스커버리 절차에서 인증 관련 정보 교환으로 부하를 급증시킨다. 이러한 문제점을 해결하기 위해 본 논문에서는 PFDP(Pre-authentication & Filtered permission Discovery Protocol)를 제안한다. PFDP는 사전 인증 및 경량화된 보안 핸드셰이크를 통해 기존의 디스커버리 절차가 갖는 부하를 절감한다. 네트워크 트래픽 모델 분석과 모의시험결과는 기존의 SSDP(Secure Simple Discovery Protocol) 대비 PFDP의 처리 지연 및 네트워크 성능이 향상됨을 보여준다.

키워드 : 무기체계, DDS, DDS Security, DDS 디스커버리, 경량화
Key Words : Weapon System, DDS, DDS Security, DDS Discovery, Lightweight

ABSTRACT

DDS, a middleware with high scalability, applies network middleware to weapon open system architecture. The scalability of DDS is provided through the preceding discovery process. As the number of participants increases, network configuration requires a high level of network, memory and computing resources. In particular, DDS with enhanced security function increases the load caused by the discovery process by exchanging authentication-related information. In order to solve this problem, this paper proposes a burden of discovery protocol with security plug-in through the PFDP. The network traffic model analysis and simulation results shows that PFDP improves the network performance compared to SSDP.

Ⅰ. 서 론

DDS는 OMG에서 국제 표준으로 정한 발간/구독 기반의 통신 미들웨어로 국방, 항공우주산업, 교통, 로봇, 증권 등의 분야에서 적용된다.[1] DDS는 데이터 중심적인 통신을 바탕으로 응용 프로그램이 메시지 전송과 관련된 동작으로부터 자유로워지고, 체계의 구성 변화에 유연하게 대응하여 높은 네트워크 확장성을 제공한다. 더불어 DDS가 제공하는 QoS 정책은 안정적인 데이터 송수신, 히스토리 관리 등 통신환경을 설정 할 수 있어, 데이터의 목적에 따라 효율적인 네트워크 자원활용을 가능하게 한다.[2] 높은 확장성을

◆ First Author : Hanwha Systems Infra SW Team 1, juwon2015.lee@hanwha.com, 정회원
° Corresponding Author : Kumoh National Institute of Technology Dept. of IT Convergence Eng., dskim@kumoh.ac.kr, 종신회원
* Kumoh National Institute of Technology Dept. of IT Convergence Eng., jh.cha@kumoh.ac.kr, 학생회원; whddn4547@kumoh.ac.kr, 학생회원; 20186114@kumoh.ac.kr, 학생회원
논문번호 : 202009-226-B-RN, Received September 16, 2020; Revised October 21, 2020; Accepted October 26, 2020

바탕으로 통신 특성을 자유롭게 설정할 수 있다는 부분은 공개 구조(Open Architecture)를 지향하는 무기체계 발전방향과 부합하며, 주로 DDS를 네트워크 미들웨어로 채택하는 이유라고 할 수 있다.

DDS가 데이터 중심적인 통신을 하기 위해서는 데이터의 생성자와 구독자를 미들웨어가 자동으로 연결시키기 위한 동적 디스커버리 기능이 반드시 필요하다. DDS 표준에 정의된 SDP (Simple Discovery Protocol)은 네트워크 상 유효한 참여자를 탐색하는 가장 기본적인 디스커버리 방법으로 각 말단 도메인(Domain) 참여자가 동일한 도메인 내에 소속된 타 참여자들과 1대 1로 토픽의 이름, QoS의 구성정보를 교환하는 방식이다. SDP는 Peer to Peer 기반으로 동작하기 때문에 통신 참여자의 수가 증가함에 따라 단말 장비 모두에 대해 높은 네트워크, 메모리 및 컴퓨팅 리소스를 요구한다. 이 과정에서 각 참여자는 최종적으로 자신과 통신을 수립하지 않을 다수의 참여자와도 통신 수립 여부를 판단하기 위해 정보를 교환하게 되고, 결과적으로 검색 과정에 네트워크, 메모리 및 컴퓨팅 리소스 일부가 불필요하게 낭비된다. 또한, DDS의 유연한 발간 / 구독 통신방식의 확장이 용이한 특성을 악의적으로 이용하는 DDS 기반 응용프로그램들로 인해 잠재적인 보안 문제를 고민하게 한다[3]. OMG에서 추가로 제정된 DDS Security 표준은 DDS의 통신 참여자 검색 과정에 인증서, 권한문서 등의 추가정보를 교환하여, 악의적인 통신 참여자를 막기 위해 제정되었다. 하지만 보안 기능에 대한 요구사항을 충족시키기 위해 도입된 보안 플러그-인(Security Plug-In)은 DDS의 디스커버리 절차로 발생하는 단점인 네트워크, 메모리 및 컴퓨팅 리소스 낭비를 더욱 두드러지게 만들었다[4].

DDS의 보안 플러그-인은 PK7CS, SMIME, Diffie Hellmann 알고리즘 등을 적용한 보안 핸드셰이크 과정을 통해 참여자 간의 보안 정보 교환을 진행하고, 이를 바탕으로 인증(Authentication), 접근 제어(Access Control), 암호화(Cryptograhpy) 등의 보안 기능을 제공한다[5,6]. 보안 핸드셰이크는 기존의 SDP 내에 포함되는 과정이다. 보안 기능이 강화되는 반면에 디스커버리 절차가 유발하는 부하는 더 증가하게 되고, 초기 통신 수립과정에 걸리는 시간과 비용은 증가하게 되었다. 시스템의 확장성을 제공하기 위한 이 디스커버리 비용은 시스템의 규모가 검색 시간과 관련된 성능에 악영향을 미친다는 것을 의미하며, 일종의 대규모 실시간 분산처리 환경인 무기체계에 적용될 경우, 전력화 시점에 대한 체계 요구사항 측면에서 특히 문제가 된다[7,8].

SDP와 보안 플러그-인의 문제점을 극복하기 위해, 본 논문에서는 보안 인증절차를 대리 수행할 데몬을 기반으로 인증절차와 디스커버리 절차를 일부 분리하여 부하를 경량화하는 검색 기법을 제시한다[9]. 제안하는 검색 기법은 도메인 참여자들이 서로를 검색하는 과정에서 낭비되는 네트워크, 메모리 및 컴퓨팅 리소스를 줄이고, 악의적인 통신 참여자의 네트워크 유입을 사전에 차단할 수 있다.

2장에서는 OMG DDS 및 SSDP(Secure Simple Discovery Protocol)의 주요 요소를 요약한다. 3장에서는 제안하는 디스커버리 기법에 대해 설명하고 트래픽 모델의 비교를 통해 그 실효성을 검증한다. 4장에서는 성능을 ns-3를 통해 시뮬레이션하여 제안하는 디스커버리 기법이 기존 Secure SDP 대비 복잡도가 개선되고, 네트워크, 메모리 및 컴퓨팅 리소스의 요구사항이 개선되었음을 보여준다. 5장에서는 결론과 향후 연구 방향성을 제시한다.

최근 컴퓨터 기술의 급속한 발전으로 인해 기존의 텍스트 위주의 사용자 환경에서 벗어나 이미지, 그래픽, 오디오 및 비디오 데이터 등을 제공하는 멀티미디어 사용자 환경으로 변화하고 있다.

Ⅱ. 연구 배경

2.1 DDS

OMG DDS 표준은 발간 / 구독 통신방식 기반으로 특정 토픽 데이터에 대한 생성자와 수신자를 연결하는 데이터 중심형 모델이다. 데이터를 중심으로 하는 느슨한 연결 방식은 곧 높은 확장성과 직결된다. 특히, DDS를 기반으로 개발자가 응용 소프트웨어를 개발하는 경우, DDS 계층에서 데이터 상태를 관리하기 때문에, 소프트웨어 개발과정에 개발자는 IP, 포트, 데이터 정렬 관리 등의 문제로부터 자유로워져 생산성 향상에도 기여한다.

데이터 중심으로 동작하는 DDS는 토픽의 '이름'을 중요한 요소로 사용한다. 모든 통신 참여자는 토픽의 이름과 함께, 송신 / 수신 여부를 선언하여 사용한다.

그림 1과 그림 2는 DDS GDS(Global Data Space)와 데이터 중심형 모델의 개념에 대해 잘 알려준다. 각 응용 소프트웨어들은 'TRACK'과 'ALARM'이란 이름을 갖는 데이터에 대해 송신 혹은 수신을 하겠다고 선언한다. 예를 들어, 'SW B'가 'ALARM' 데이터를 송신할 경우, GDS 상 'ALARM' 데이터가 갱신되고, DDS에 의해 'ALARM' 데이터를 수신하기로 한

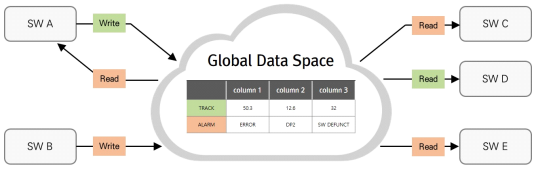

그림 1. DDS 개요
Fig. 1. Overview of DDS

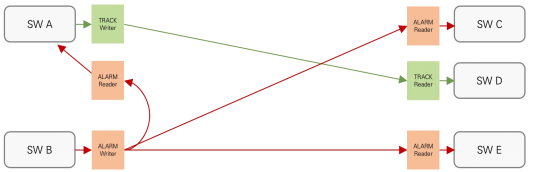

그림 2. DDS 개요
Fig. 2. Overview of DDS

'SW A', 'SW C', 'SW E'가 최신 'ALARM' 데이터를 확보하게 된다.

2.2 SSDP

OMG DDS RTPS(Real-time Publish-Subscribe) 표준은 PDP(Participant Discovery Protocol)와 EDP(Endpoint Discovery Protocol)로 구성된 디스커버리 프로토콜을 정의한다. 우선 PDP는 네트워크에서 통신 참여자가 서로를 발견하는 방법을 정의한다. 참가자 간의 상호 검색이 완료되면, EDP를 통해 참여자의 송/수신 등록정보에 대한 정보를 교환한다. SSDP는 SDP에 그림 3과 같이 보안 핸드셰이크와 키 교환 절차 추가를 통해 보안기능을 강화한다.

SPDP(Simple Participant Discovery Protocol) 단계에서 DDS 참여자는 SPDP 메시지를 작성하여, 네트워크 내에 식별된 모든 다른 참가자들에게 주기적

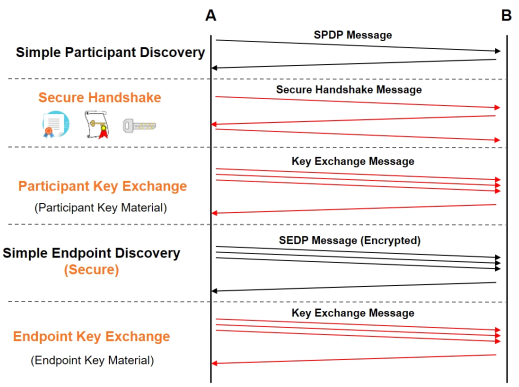

그림 3. LegacySDP와 SecureSDP 비교 분석
Fig. 3. Comparative Analysis of legacySDP and SecureSDP

으로 메시지를 송출한다. SPDP 메시지에는 참가자의 GUID(Globally Unique Identifier) 대신, 암호화된 별도의 BuiltinTopicKey, 로케이터 정보 및 QoS 정보가 포함된다. 다른 참가자로부터 SPDP 메시지를 수신한 경우, 데이터 내 포함된 보안 정보들을 토대로 유효성 검증 절차를 약식으로 진행한다. 한 쌍의 참가자가 SPDP 메시지를 서로 교환하면, 보안 핸드셰이크 절차로 전환한다. 보안 핸드셰이크 절차에는 상호 인증서 및 권한 문서의 유효성을 검증하는 과정과 키 교환 과정이 포함된다. 보안 플러그-인의 인증 및 접근제어 모듈은 교환한 정보를 바탕으로 인증, 권한 관리기능을 활성화하고, 암호화 모듈은 공유 비밀값을 기반으로 비대칭 키를 생성하여 양단 간 통신 과정의 암/복호화에 사용한다. 핸드셰이크 과정에서 유효성에 대한 검증절차와 키 생성단계를 성공적으로 진행하면, SEDP(Simple Endpoint Discovery Protocol) 단계로 전환된다. 이 시점부터 설정에 따라 양단간의 암호화 통신이 가능해진다. SEDP 단계는 SPDP 단계와 달리, 신뢰성 QoS 기반으로 SEDP 메시지 교환을 진행한다. 이 SEDP 메시지에는 토픽의 이름, 데이터의 유형 및 해당 참여자의 QoS 정보가 포함된다. 다른 참여자로부터 수신한 메시지의 토픽이름과 유형, QoS 등의 정보가 자신에게 설정된 정보와 동일한 경우, 상호 등록 절차가 진행되고, 이후로 설정에 따라 데이터를 송신 및 수신하는 통신 절차가 진행된다.

이러한 과정은 DDS의 유연한 네트워크 구성과 강화된 보안기능을 함께 제공해주는 반면, 디스커버리 과정이 유발하는 부하가 더 증가시키기 때문에, 초기 통신 수립과정에 필요한 시간과 비용은 크게 증가한다.

Ⅲ. PFDP(Pre-Authentication and Filtered Permission based Discovery Protocol)

3.1 PFDP

보안기능이 적용된 DDS 디스커버리 과정이 시스템 자원 및 네트워크 부하를 일으키는 원인은 인증서 및 권한문서를 연결하고자 하는 모든 참여자와 교환해야 하는 것과 그 문서를 인증하는 절차를 처리해야 하는 것이다. 위 과정에 의해 발생하는 시스템 자원 및 네트워크 자원을 PFDP를 통해 효율적으로 관리하고자 한다.

그림 4는 SSDP의 절차를 일부 수정한 PFDP의 절차를 나타낸다. 두 프로토콜 간 가장 큰 차이점은 AD(Authentication Delegator) 존재의 유무다. PFDP에서는 절차 내에 AD 모듈을 추가하여, 도메인 참여

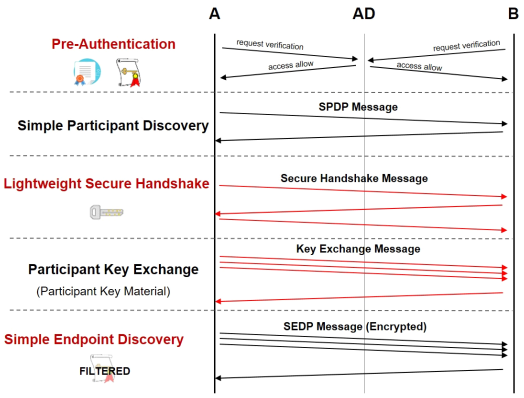

그림 4. 제안하는 PFDP의 순서도
Fig. 4. Sequence of Proposed PFDP

자 간 1:1로 이뤄지던 보안 결함 검증 절차를 위임 처리하여 디스커버리 과정에 발생하는 트래픽을 최적화하고자 한다.

3.1.1 사전 인증

PFDP의 동작을 위해 AD 모듈은 CD(Collision Domain) 영역 당 하나를 운용한다. AD는 DDS 통신 참여자들의 유효성을 검증하는 모듈로 비인가 참여자의 네트워크 접근 방지를 위해 동일한 CD 내 Gateway Switch의 In/Out bound 정책에 대한 접근권한을 갖고 있어야 한다. (본 논문에서는 SDN 네트워크 스위치의 컨트롤러를 응용, 운용함을 가정한다.) 모든 DDS 기반 네트워크 참여자들은 자신이 소속된 CD에 소속된 AD의 네트워크 정보를 QoS 프로파일을 통해 설정할 수 있다.

AD는 참여자의 인증문서와 권한문서를 도메인 참여자로부터 수신하고, 적어도 하나의 문서에 결함이 있는 것으로 판단되면, 해당 참여자를 유효하지 않은 것으로 보고, 참여자의 네트워크 접속을 스위치를 통해 선제적으로 차단하여 체계에 불필요한 디스커버리 패킷의 발생을 방지한다. 인증, 권한문서의 유효성 검증 절차는 AD에 의해 이미 수행되었으므로 허용된 참가자들은 사용자 인증문서 및 권한문서에 대한 상호교환, 검증 절차가 제외된 경량화 보안 핸드셰이크를 수행한다.

Algorithm Authentication Delegator Action

function ON_PACKET_RECEIVED(PK)
  Extract $Cert_{dp}$ *from* PK_{dp}
  Extract $Perm_{dp}$ *from* PK_{dp}
  if $Cert_{dp}$ is NOT NULL **then**
    Validate $Cert_{dp}$ *by* $Cert_{delegator}$
    if $Cert_{dp}$ is Unavailable **then**
      Add DP to ParticipantFiltering
      break
  if $Cert_{dp}$ is NOT NULL **then**
    Validate $Perm_{dp}$ by $Cert_{delegator}$
    if $Perm_{dp}$ is Unavailable **then**
      Add DP to ParticipantFiltering
      break
  Send Allow Message to DP

3.1.2 경량화 보안 핸드셰이크

사전 인증과정을 통해 인증문서와 권한문서의 검증 절차는 생략되어, 접근제어 권한 확인은 권한문서를 요약한 별도의 구조를 사용하여 inline QoS 형태로 상대방 참여자에게 전달한다. 인증문서는 대체로 고정된 크기를 갖지만, 권한문서는 체계의 특성과 보안수준에 따라 가변성을 갖는다. 따라서, 권한문서가 압축되는 정도는 PFDP의 성능, 실효성 관점에서 중요한 변수가 된다.

그림 5는 SSDP와 PFDP 간의 권한정보 교환에 대한 차이점을 표현한다. 그림에 표현된 용어의 설명은 다음과 같다.

- DP(Domain Participant) : 통신 참여자
- DW(Data Writer) : DP 내, 데이터 전송 객체
- DR(Data Reader) : DP 내, 데이터 수신 객체

SSDP와 PFDP의 차이는 DP1과 DP2 사이에 교환하는 토픽 권한 정보에서 확인할 수 있다. SSDP의 경우, 서로 취급하고 있는 토픽 정보와 상관없이 각자 자신이 보유하고 있는 권한정보 전체를 상대방에게 전송한다. PFDP는 디스커버리 과정에서 필터링된 권한정보를 DP 간에 공유하는 과정을 보여준다. 각 DP는 상대 DP와의 통신에 유효한 토픽의 정보만을 권한문서로부터 필요한 정보만을 필터링하여 권한정보를 구성하고, SEDP 시점에 Inline QoS를 통해 상대 DP

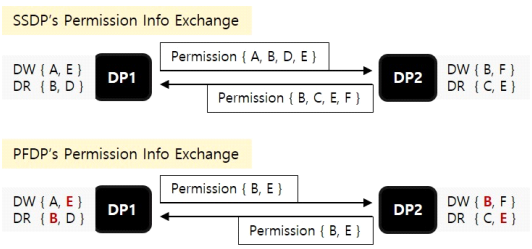

그림 5. SSDP와 PFDP의 권한 교환 비교
Fig. 5. Permission Exchange Comparison of SSDP and PFDP

에게 전달한다. 기존의 SSDP 대비 인증문서와 권한문서 내 정의된 정보의 사용률에 따른 PFDP 적용효과는 3.2 절에서 수학적 모델을 통해 확인한다.

3.2 SSDP와 PFDP 비교 분석

3.1장에서는 제안한 PFDP의 실제 통신 수립 과정이 SSDP와 어떤 차이점을 갖는지 확인했다.

본 절에서는 PFDP를 채택하여 네트워크를 구성할 경우, 기존의 SSDP 대비 부하 절감효과가 있는지 트래픽을 분석을 통해 확인한다. 디스커버리 트래픽 분석은 디스커버리 과정에서 발생하는 전체 메시지 수량과 크기, 디스커버리 참여 개체의 수량 등으로 분석할 수 있다. Table. 1에 트래픽 분석을 위한 표현을 확인할 수 있다. 디스커버리 과정은 도메인 참여자 P 간의 일련의 트래픽 교환으로 표현할 수 있다. 이 트래픽 교환은 모든 참여자 간 1회 이상 진행되고, 형성되는 모든 연결 쌍을 L로 표현한다. R_{match}는 각 도메인 참여자간의 연결 형성 시, 상호 교환 가능한 정보의 일치율을 나타내며, 이 일치율이 높을수록 연결된 두 참여자 간 교환해야할 정보량이 높아진다고 할 수 있다. R_{doc}는 DDS 통신에 보안 기능 추가로 디스커버리 과정에서 교환하는 두 종류의 문서 간 크기 비율을 나타내는 값이다. 네트워크 구성이 커질수록 참여자 간 교환 정보의 구성이 복잡해지고 권한문서의 크기가 크게 설정되므로, R_{match}는 작아지고, R_{doc}은 커지는 경향이 존재한다. 더불어, 본 분석에서는 모든 참여자가 별도의 노드에 분산되어 운용됨을 가정하고, 디스커버리 과정 중 완벽히 동일하게 발생하는 SPDP 과정에 대한 트래픽은 분석 대상에서 제외한다.

표 1. 트래픽 분석에 사용되는 표기법
Table 1. Notation used for Traffic Analysis

Notation	Definition
P	Number of Participant in a Domain
L	Number of Link in a Domain, $L=\frac{P\times(P-1)}{2}$
R_{match}	Ratio of the number of matching Topics
R_{doc}	Ratio of the certification Document to permission Document

3.2.1 SSDP 의 절차 및 트래픽 분석

SSDP의 디스커버리 과정은 최초 도메인 참여자가 상호 발견한 다른 도메인 참여자들에게 자신의 인증정보를 전송하면서 진행된다. 여기서 발생하는 핸드셰이크의 순서는 SPDP를 통한 GUID 비교를 통해 결정한다. 우선순위를 갖는 참여자를 A, 후 순위 참여자를 B라고 할 때, 핸드셰이크 과정에서 교환하는 메시지는 아래의 식 1과 2로 표현할 수 있다.

$$M_{AtoB}=M_{certA}+M_{permA}+M_{begin} \tag{1}$$

$$M_{BtoA}=M_{certB}+M_{permB}+M_{reply} \tag{2}$$

참여자 A와 B는 자신의 인증문서와 권한문서를 교환하여, 사용자 인증절차 및 접근권한제어 절차를 수행하여 상대 참여자가 유효한 참여자인지 검증한다. 그리고 인증문서, 권한문서 정보 외에 주고받은 M_{begin}과 M_{reply} 정보를 통해 키 교환 및 생성 절차를 진행하여 공유 비밀값을 생성한다. 실질적인 암호화 통신 절차는 해당 정보의 교환 이후에 이뤄진다. 네트워크 상 모든 인증문서 및 권한문서의 크기가 동일하다고 가정할 경우, 두 참여자 간에 교환되는 메시지는 다음 식 3과 4로 표현할 수 있다.

$$M_{handshake}=M_{begin}+M_{reply} \tag{3}$$

$$M_{link}\cong 2M_{cert}+2M_{perm}+M_{handshake} \tag{4}$$

모든 참여자 간의 연결은 동일한 절차를 갖는다. 따라서, SSDP의 디스커버리 과정을 통해 교환되는 전체 디스커버리에 대한 네트워크 메시지 부하는 식 5로 표현할 수 있다.

$$M_{SSDP}=M_{link}\times L \tag{5}$$

3.2.2 PFDP의 절차 및 트래픽 분석

PFDP의 디스커버리 과정은 사전인증단계와 보안 핸드셰이크 단계로 구성된다. 네트워크상에서 운용을 시작한 모든 도메인 참여자들은 해당 CD 내 AD에게 유효성 검증을 위한 정보를 송신하고, 이때 발생하는 메시지는 식 6과 같이 표현한다. 앞선 SSDP의 가정과 동일하게, 모든 DP가 동일한 크기의 인증문서와 권한문서를 보유, 네트워크 전체를 기준으로 사전인증 단계에서 발생하는 메시지는 식 7과 같이 표현 가능하다.

$$M_{preCert}=M_{cert}+M_{perm} \tag{6}$$

$$M_{preCertT}\cong M_{preCert}\times P \tag{7}$$

사전 인증단계 이후 이어지는 보안 핸드셰이크 과정을 권한문서가 압축된 정도(R_{match})를 바탕으로 정리하면 식 8, 이를 바탕으로 PFDP의 디스커버리 과정 전체에 발생하는 메시지 트래픽은 식 9로 표현 가능하다.

$$M_{postCertT} = (2M_{perm} \times R_{match} + M_{handshake}) \times L \quad (8)$$

$$M_{PFDP} = M_{preCertT} + M_{postCertT} \quad (9)$$

3.2.3 PFDP 실효성 검증

PFDP의 적용 시, SSDP 대비 네트워크 부하 절감의 효과를 얻기 위한 최소 조건은 식 10과 같이 나타낼 수 있으며, 이를 네트워크 참여자에 대해 정리하면 식 11이 도출된다.

$$M_{SSDP} \geq M_{PFDP} \quad (10)$$

$$P \geq 1 + \frac{1}{1 - \frac{R_{match}}{1 + R_{doc}}} \quad (11)$$

PFDP 적용이 유효한 최소 조건을 판단하는데 R_{match}, R_{doc}외에 $M_{handshake}$는 영향을 주지 않는다. 실제로 SSDP 및 PFDP를 통해 교환되는 $M_{handshake}$의 구성은 유의미한 변화를 갖지 않기 때문에, 식 11과 같이 최소 조건은 R_{match}과 R_{doc}의 영향으로 결정된다고 볼 수 있다.

식 11을 도식화한 그림 6은 PFDP가 효과를 얻기 위한 최소 참여자의 수에 대한 요구사항이 권한문서의 압축율(R_{match})이 높을수록, 권한문서의 규모(R_{doc})가 작을수록 낮아진다는 것을 보여준다. 예를 들어, $R_{match} = 0.7$, $R_{doc} = 0.1$인 경우는 권한문서가 인증문서 대비 10배의 크기를 갖고, DP간의 평균적인 권한문서 압축율이 30%일 경우, DP를 4개 이상 구성한 네트워크에 PFDP를 적용하면 효과를 얻을 수 있음을 의미한다.

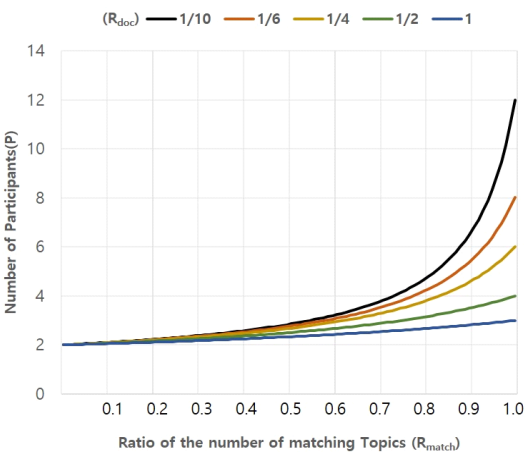

그림 6. R_{match}와 R_{doc} 최소값 P 비교
Fig. 6. R_{match} and R_{doc} minimum P Comparison

Ⅳ. 모의시험 및 평가

이번 장에서는 SSDP와 PFDP를 비교하기 위한 모의시험을 진행하고, 동일한 환경에서 디스커버리 종료 시점을 측정하여 PFDP 적용에 대한 효율성을 확인한다. 시험 환경은 ns-3를 통해 무기체계 환경을 모사했다. ns-3의 OFswitch 라이브러리를 통해 AD를 구현하고, SSDP 및 PFDP를 모사한 노드의 동작을 구현하였다. 인증, 패킷연산 등의 처리지연에 대한 수치는 한화 시스템에서 개발한 SmartDDS Secure의 운용 결과 값을 참고하여 모사했다. 시험은 디스커버리 종료 시점과 시험과정 간 노드의 네트워크 사용량을 측정하는 것으로 R_{match}, 네트워크의 참여자의 수를 달리하여 진행했다.

4.1 디스커버리 완료 시간 비교

그림 7은 SSDP 와 PFDP의 디스커버리 절차가 완료되는데 까지 소요되는 시간을 측정한 값을 보인다. 참여자 수가 많을수록, PFDP는 R_{match}가 작을수록

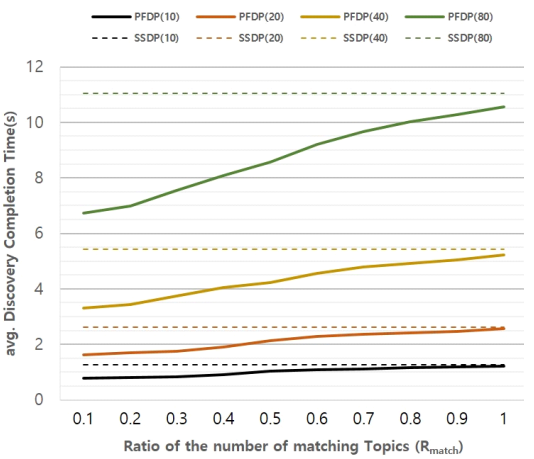

그림 7. SSDP와 PFDP의 디스커버리 완료 시간 비교
Fig. 7. Discovery Completion Time Comparison of SSDP and PFDP

SSDP 대비 부하절감 효과가 크게 나타나며, 환경에 따라 SSDP 대비 절반이상 단축된 디스커버리 완료시간을 보였다. 반면, R_{match}가 0.8을 초과하는 경우, SSDP 대비 부하절감 효과가 없거나 오히려 높은 부하를 보인다. 즉, PFDP는 규모가 큰 네트워크에 적용할수록 디스커버리 성능 개선효과가 상승하며, 소규모의 네트워크의 경우, SSDP 보다 디스커버리 성능에 부정적인 효과를 줄 수 있다고 해석할 수 있다.

4.2 디스커버리 트래픽 비교

$P=40$ 인 환경에서 한 노드의 트래픽 I/O를 프로토콜 및 R_{match}에 따라 표현하면 그림 8과 같다. R_{match}가 0.1인 경우의 PFDP는 SSDP 대비 1/3 이상 트래픽이 감소함을 보인다. 반면, 1.0인 경우는 오히려 SSDP 대비 높은 트래픽이 필요하여 트래픽 절감 측면에서 손실이 확인된다. 앞서 설명한 바와 같이 R_{match}는 네트워크 규모와 반비례하는 요인으로, 그림 8의 결과 역시, 네트워크 규모가 클수록 PFDP의 적용 효과가 상승할 것이라는 해석으로 연결할 수 있다.

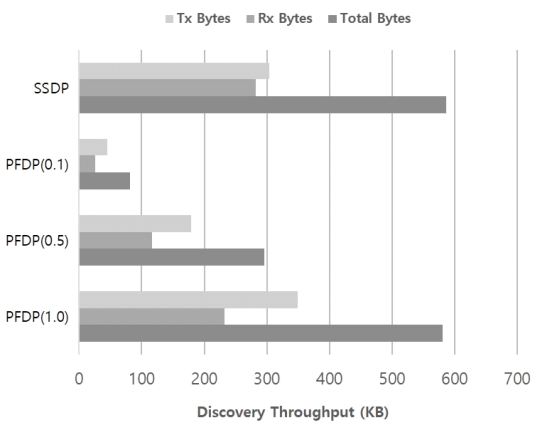

그림 8. SSDP와 PFDP의 디스커버리 트래픽 사용 비교
Fig. 8. Discovery Traffic Comparison of SSDP and PFDP

4.3 정리

본 논문의 목적은 디스커버리 성능 문제가 발생하는 대규모의 실시간 네트워크 환경에서 디스커버리 성능을 개선하는 것이다. PFDP는 네트워크의 규모가 커질수록(R_{match}가 작을수록, 참여자 수가 늘어날수록) 디스커버리 과정에서 발생하는 트래픽의 규모를 절감하고, 디스커버리 소요시간도 단축하여 성능을 개선할 수 있음을 보였다. 따라서, 규모가 큰 환경일수록 성능개선 효과가 두드러지는 PFDP가 무기체계에 적용될 경우 설계목적에는 부합하여 디스커버리 성능이 개선될 것이라고 예측할 수 있다.

V. 결 론

무기체계에서의 초기 구동까지 소요되는 시간은 중요한 요구사항으로 경량화를 통한 소요 시간 단축은 반드시 고민해야 할 부분이다. 본 연구는 보안 플러그인의 도입으로 증가한 디스커버리 지연 현상을 프로세스의 개선을 통해 경감시키는 것을 목적으로 한다. 이를 위해 DDS에 보안 기능 적용으로 발생하는 디스커버리지연 현상에 대한 분석하고, AD 및 권한문서 압축방식을 적용한 PFDP를 제안했다.

3장에서는 PFDP 적용의 실효성을 SSDP와 PFDP의 네트워크 트래픽 모델을 바탕으로 진행하여 유효한 네트워크 구성 조건을, 그리고 를 통해 표현하고, 네트워크 규모에 의해 유효성이 결정된다는 것을 확인했다. 4장에서는 한화시스템에서 개발한 SmartDDS Secure와 ns-3를 기반으로 모의 환경을 구성하고 모의시험을 진행했다. SSDP와 PFDP 간의 통신 수립지연 시간과 트래픽 I/O를 측정을 통해 PFDP를 무기체계에 적용할 경우, 무기체계의 규모가 클수록 SSDP 대비 초기 통신수립 지연시간의 개선 효과를 얻을 수 있음을 확인했다.

SmartDDS Secure를 기반으로 PFDP의 구현하여 본 논문에서 다루지 않았던 AD 및 통신 참여자가 소속된 단말 노드의 시스템, 컴퓨팅 리소스의 효율과 관련하여 디스커버리 성능 시험을 진행할 예정이다. 또, PFDP로 인해 발생할 수 있는 보안상의 위협들에 대해 분석하고, 그 해결 방안에 대한 연구를 진행하고자 한다.

References

[1] *DDS Executive Summary 2011 The Data Distribution Service : Reducing Cost through Agile Integration*, OMG, 2010.

[2] OMG Std. *Data Distribution Service for Real-time Systems Version 1.2*, OMG, 2007.

[3] M. J. Michaud, T. Dean, and S. P. Leblanc, “Attacking OMG data distribution service(DDS) based real-time mission critical distributed systems,” in *2018 13th MALWRE*, pp. 68-77, 2018.

[4] K. Beckman and J. Reininger, “Adaptation of the DDS security standard for resource-constrained

sensor networks," in *2018 IEEE 13th SIES*, pp. 1-4, 2018.

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

[6] J. H. Han, "Message encryption methods for DDS security performance improvement," *J. KIICE*, vol. 22, no. 11, pp. 1554-1561, Nov. 2018.

[7] S. J. Ko, "Network centric warfare to prepare for combat systems development and future direction," *J. IEIE*, vol. 37, no. 11, pp. 1123-1134, 2010.

[8] Y. S. Choi, "Smart DDS middleware localization and weapon system application," *Commun. of KIISE*, vol. 34, no. 10, pp. 43-46, Oct. 2016.

[9] M. K. Kang "A study on efficient discovery method through daemon process in Smart DDS," in *2016 KIMST Annu. Conf. Proc.*, pp. 661-662, 2016.

이 주 원 (Ju-Won Lee)

2014년 2월 : 금오공과대학교 전자공학부 학사 졸업

2016년 2월 : 금오공과대학교 IT융복합공학과 석사 졸업

2015년 1월~현재 : 한화시스템 기반SW1팀 선임연구원

<관심분야> 통신공학, 미들웨어, 산업용 통신망 및 IoT 시스템

차 중 혁 (Joong-Hyuck Cha)

2016년 2월 : 금오공과대학교 전자공학부 학사 졸업.

2017년 8월 : 금오공과대학교 IT융복합공학과 석사 졸업.

2017년~2020년 : ICT융합특성화연구센터 연구원.

2020년~현재 : 금오공과대학교 IT융복합공학과 박사과정재학 중.

<관심분야> 미들웨어, 산업용 통신망 및 IoT 시스템, 엣지 컴퓨팅

이 종 우 (Jong-Woo Lee)

2018년 2월 : 금오공과대학교 전자공학부 학사 졸업.

2020년 2월 : 금오공과대학교 대학원 IT융복합공학과 석사 졸업.

2020년~현재 : 금오공과대학교 대학원 IT융복합공학과 박사과정재학 중.

<관심분야> 미들웨어, 네트워크 기반 분산 제어 시스템, 블록체인

김 경 선 (Gyeong-Seon Kim)

2018년 2월 : 금오공과대학교 전자공학부 학사 졸업.

2020년 2월 : 금오공과대학교 대학원 IT융복합공학과 석사 졸업.

2020년~현재 : 금오공과대학교 대학원 IT융복합공학과 박사과정재학 중.

<관심분야> 미들웨어, 네트워크 분산시스템, 엣지 컴퓨팅

김 동 성 (Dong-Seong Kim)

1992년 2월 : 한양대학교 전자공학과 학사 졸업.
2003년 3월 : 서울대학교 전기 및 컴퓨터공학부 박사 졸업.
2004년 : Cornell 대학교 ECE 박사 후 연구원.
2019년~현재 : 금오공과대학교 산학협력단장.
2014년~현재 : ICT 융합특성화연구센터 센터장(과기정통부 ITRC 및 연구재단 중점연구소).
2014년~현재 : IEEE/ACM Senior 회원.
2015년~2018년 : 금오공과대학교 융합기술원 원장.
2016년 9월~현재 : 국방부 CIO 자문위원.
<관심분야> 실시간 통신망 및 IoT 시스템, 네트워크 기반 분산 제어 시스템, 실시간 S/W