ISSN 1226-9182

정보처리학회지

Korea Information Processing Society Review

www.kips.or.kr

KIPS

2017년 9월, 11월, 2018년 1월 | 제24권 제5호, 제6호, 제25권 제1호 | 합본

4차 산업혁명

사물 인터넷, 사이버 물리 시스템, 빅 데이터, 인공 지능 등의 기술에 의한 4차 산업혁명의 진행 상황

의약품 부작용 예측을 위한 빅데이터 분석 기술 동향

A Study on the Improvement for Military Cyber Protection Technology in the 4th Industrial Revolution

ICT 융합

수직 적층형 구조를 이용한 IoT기반 스마트 양식장의 산업화모델 개발

IoT 기반 전력망 센서 네트워크 구현을 위한 Small Cell 무선통신시스템 기술개발 현황

NIST 양자내성암호 표준공모전 제출물 분석 및 향후 연구전망

병렬 프로그래밍 기법

AVX-512를 활용한 인텔 차세대 프로세서에서의 효과적인 프로그래밍 방법

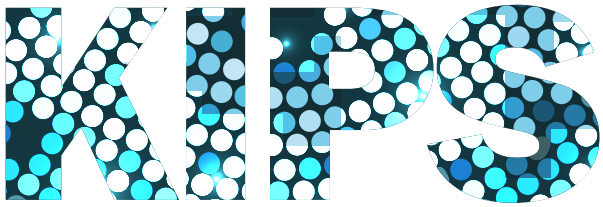
매니코어 시스템에서의 병렬 프로그래밍 최적화를 위한 분석 도구 및 벤치마크 성능 실험

사단법인 한국정보처리학회
KIPS Korea Information Processing Society

정보처리학회지

Korea Information Processing Society Review

www.kips.or.kr



제 23대 임원명단

이 사 | 강승석 (서울여자대학교) 강정호 (배화여자대학교) 고광만 (상지대학교) 공기식 (남서울대학교)
곽 진 (아주대학교) 권구락 (조선대학교) 권순일 (세종대학교) 권혁준 (순천향대학교)
길아라 (숭실대학교) 김기범 (국가보안기술연구소) 김미혜 (충북대학교) 김성기 (선문대학교)
김성수 (한국산업기술대학교) 김성우 (서울대학교) 김성환 (서울시립대학교) 김수균 (배재대학교)
김영욱 (KETI) 김 용 (한국방송통신대학교) 김인철 (경기대학교) 김종국 (고려대학교)
김종찬 (국민대학교) 김태근 (세종대학교) 김학만 (인천대학교) 노응기 (가천대학교)
노원우 (연세대학교) 문유진 (한국외국어대학교) 문현준 (세종대학교) 민세동 (순천향대학교)
민 홍 (호서대학교) 박능수 (건국대학교) 박상봉 (세명대학교) 박정민 (KIST)
박진호 (숭실대학교) 박찬열 (KISTI) 성연식 (동국대학교) 손태식 (아주대학교)
송왕철 (제주대학교) 신동일 (세종대학교) 신창선 (순천대학교) 아지즈 (충북대학교)
안상현 (서울시립대학교) 오세창 (세종사이버대학교) 유진호 (상명대학교) 윤주상 (동의대학교)
이경오 (선문대학교) 이경현 (부경대학교) 이근호 (백석대학교) 이기훈 (광운대학교)
이원규 (고려대학교) 이은영 (동덕여자대학교) 이의신 (충북대학교) 이장호 (홍익대학교)
이재광 (한남대학교) 이재호 (서원대학교) 이필우 (KISTI) 이호원 (한경대학교)
이화민 (순천향대학교) 임동혁 (호서대학교) 임승호 (한국외국어대학교) 장종수 (ETRI)
전유부 (순천향대학교) 정교민 (서울대학교) 정수환 (숭실대학교) 정순영 (고려대학교)
정윤호 (한국항공대학교) 정재화 (한국방송통신대학교) 정재희 (홍익대학교) 정창성 (고려대학교)
정화영 (경희대학교) 조수현 (홍익대학교) 최강선 (한국기술교육대학교) 최 성 (남서울대학교)
추현승 (성균관대학교) 허 경 (경인교육대학교) 허준범 (고려대학교)

협동이사 | 강동석 (NIA) 강 신 (코스콤) 고범석 (㈜자이네스) 구태언 (테크앤로법률사무소)
권문주 (NIPA) 김교은 (㈜베스트케이에스) 김성동 (KETI) 김성엽 (㈜블루코어)
김완섭 (㈜넥스첼) 김우성 (호서대학교) 김태섭 (㈜바른전자) 김평중 (충북도립대학)
김헌중 (라온피플㈜) 김현우 (동국대학교) 문정현 (한국정보산업연합회) 민석홍 (㈜민데이타)
박철균 (에코메이텍) 박형우 (KISTI) 서문규 (코인플러그) 서재철 (KISA)
서준서 (대우정보시스템㈜) 신우현 (데일리블록체인) 안유환 (㈜네오피엠) 엄두섭 (㈜센서웨이)
오형근 (국가보안기술연구소) 우종정 (성신여자대학교) 유환조 (포항공과대학교) 윤두식 (㈜지란지교시큐리티)
이갑수 (Korea IT Times) 이영구 (경희대학교) 이윤재 (SK텔레콤) 이재두 (NIA)
이종근 (㈜DSTi) 이 철 (LG CNS) 이현정 (중앙대학교) 이희승 (㈜티노스)
임경수 (ETRI) 정경균 (㈜달라이브) 정성무 (KERIS) 정원용 (원광대학교)
조태남 (우석대학교) 지석구 (NIPA) 진성철 (유넷시스템) 최동근 (롯데카드)
최지윤 (㈜한국IT컨설팅) 황일선 (KISTI)

지회

강원지회	김상춘 (강원대학교)	영남지회	김태철 (포위즈시스템)
제주지회	김형수 (제주한라대학교)	충청지회	류근호 (충북대학교)
호남지회	방상원 (송원대학교)		

연구회 위원장

e-Bridge	이정배 (부산외국어대학교)	IT융합서비스	박석천 (가천대학교)
IT정책	오길록 (숭실대학교)	빅데이터컴퓨팅	이필규 (인하대학교)
소프트웨어공학	박용범 (단국대학교)	스토리지시스템	신범주 (부산대학교)
에너지그리드정보처리	이봉재 (전력연구원)	우정기술	정 훈 (ETRI)
전산교육	김형진 (전북대학교)	전산수학	박진홍 (선문대학교)
전자정부	이재두 (NIA)	정보통신응용	오진태 (ETRI)
지식 및 데이터공학	진병운 (ETRI)	컴퓨터소프트웨어	박두순 (순천향대학교)

IT시니어봉사단

단 장 | 유기홍 (명지전문대학)

위 원 | 김홍진 (가천대학교) 이준상 (한국IT전문가협회) 정상근 (연성대학교) 정진욱 (인터넷윤리실천협의회)

IT장학사업본부

본 부 장 | 이상범 (단국대학교)

부 본 부 장 | 박정호 (선문대학교)

IT평가인증본부

본 부 장	김병기 (전남대학교)			
부 본 부 장	이상범 (단국대학교)	이영천 (호남대학교)		
위 원	김우성 (호서대학교)	김응수 (대전대학교)	김점구 (남서울대학교)	박석천 (가천대학교)
	박정호 (선문대학교)	박진양 (인하공업전문대학)	박태홍 (LG전자)	윤용익 (숙명여자대학교)
	이병수 (인천대학교)	이임영 (순천향대학교)	조동섭 (이화여자대학교)	조성갑 (단국대학교)
	최상록 (생산성본부)	최재혁 (신라대학교)	허문행 (안양대학교)	

인터넷윤리진흥본부

본 부 장	정진욱 (인터넷윤리실천협의회)
부 본 부 장	박정호 (선문대학교)

한민족IT평화봉사단

위 원 장	최 성 (남서울대학교)

선거관리위원회

위 원 장	정영식 (동국대학교)			
위 원	김동호 (숭실대학교)	박종혁 (서울과학기술대학교)	원유재 (충남대학교)	유헌창 (고려대학교)
	이기용 (숙명여자대학교)	정승원 (동국대학교)	조경은 (동국대학교)	최유주 (서울미디어대학원대학교)
	황광일 (인천대학교)			

인사위원회

위 원 장	남석우 (콤텍시스템)			
부 위 원 장	김상훈 (한경대학교)			
위 원	길준민 (대구가톨릭대학교)	김동호 (숭실대학교)	유헌창 (고려대학교)	정승원 (동국대학교)
	최유주 (서울미디어대학원대학교)	한연희 (한국기술교육대학교)	황광일 (인천대학교)	
간 사	이기용 (숙명여자대학교)			
감 사	정상근 (연성대학교)	이재철 (세기정보통신)		

포상위원회

위 원 장	최유주 (서울미디어대학원대학교)			
위 원	김동호 (숭실대학교)	원유재 (충남대학교)	유헌창 (고려대학교)	이기용 (숙명여자대학교)
	정승원 (동국대학교)	황광일 (인천대학교)		

전임회장 운영위원회

위 원 장	성기중 (프리CEO)			
위 원	조이남 (엑스게이트)	오길록 (숭실대학교)	정진욱 (인터넷윤리실천협의회)	오해석 (가천대학교)
	김홍기 (KTds)	이상범 (단국대학교)	변재일 (국회의원)	김병기 (전남대학교)
	최헌규 (前 다우기술)	이정배 (부산외국어대학교)	금기현 (청년기업가정신재단)	정태명 (성균관대학교)
	오경수 (제주도개발공사)	박석천 (가천대학교)	조성갑 (단국대학교)	박두순 (순천향대학교)
	구원모 (전자신문)	정영식 (동국대학교)		

여성위원회

위 원 장 | 조경은 (동국대학교)

위 원 |

길아라 (숭실대학교)	김경아 (명지전문대)	김미혜 (충북대학교)	김미희 (한경대학교)
문남미 (호서대학교)	박정민 (KIST)	성해경 (한양여자대학교)	송은하 (원광대학교)
신은경 (날리지큐브)	안상현 (서울시립대학교)	안은영 (한밭대학교)	오수현 (호서대학교)
윤회진 (협성대학교)	이유부 (성균관대학교)	이은영 (동덕여자대학교)	이정원 (아주대학교)
이화민 (순천향대학교)	임지영 (성서대학교)	최미정 (강원대학교)	최수미 (세종대학교)
최유주 (서울미디어대학원대학교)	최은미 (국민대학교)	한영신 (성결대학교)	한정란 (협성대학교)
홍헬렌 (서울여자대학교)			

학회지편집위원회

위 원 장 | 김종완 (삼육대학교)

부 위 원 장 |

금득규 (유한대학교)	오세창 (세종사이버대학교)	전정훈 (동덕여자대학교)	최유주 (서울미디어대학원대학교)

위 원 |

강경태 (한양대학교)	강윤희 (백석대학교)	김기범 (국가보안기술연구소)	김기병 (행정자치부)
김기연 (목원대학교)	김영환 (전자부품연구원)	김혜영 (홍익대학교)	김호원 (부산대학교)
박병호 (국방부)	박현주 (시옷(CIoT))	윤종희 (영남대학교)	이준환 (극동대학교)
이해연 (국립금오공과대학교)	임승호 (한국외국어대학교)	임유진 (숙명여자대학교)	장상현 (KERIS)
정원용 (원광대학교)	조광문 (목포대학교)	조두산 (순천대학교)	최경주 (충북대학교)
최 민 (충북대학교)			

JIPS 편집위원회

Editor-In-Chiefs
Jong Hyuk Park (Leading Editor) (Seoul National University of Science and Technology, Korea)
Vincenzo Loia (University of Salerno, Italy)

Executive Editors
Doo-Soon Park (Soonchunhyang University, Korea)
Hamid R. Arabnia (The University of Georgia, USA)
Young-Sik Jeong (Dongguk University, Korea)

Advisory Editor
Han-Chieh Chao (National Ilan University, Taiwan)
Javier Lopez (University of Malaga, Spain)
Jianhua Ma (Hosei University, Japan)
Jiannong Cao (The Hong Kong Polytechnic University, Hong Kong)
Laurence T. Yang (St. Francis Xavier University, Canada)
Mohammad S. Obaidat (Fordham University, USA)
Mo-Yuen Chow (North Carolina State University, USA)
Qun Jin (Waseda University, Japan)
Victor Leung (The University of British Columbia, Canada)
Witold Pedrycz (University of Alberta, Canada)
Yang Xiao (The University of Alabama, USA)

Associate Editor-In-Chief
Neil Y. Yen (The University of Aizu, Japan)

Managing Editor
Yunsick Sung (Dongguk University, Korea)

Senior Editors
Houcine Hassan (Universitat Politecnica de Valencia, Spain)
Ka Lok Man (Xi'an Jiaotong-Liverpool University, China)
Kim-Kwang Raymond Choo (The University of Texas at San Antonio, USA)
Luis Javier Garcia Villalba (Universidad Complutense de Madrid, Spain)
Muhammad Khurram Khan (King Saud University, Kingdom of Saudi Arabia)
Muhammad Younas (Oxford Brookes University, UK)
Naveen Chilamkurti (La Trobe University, Australia)
Stefanos Gritzalis (University of the Aegean, Greece)
Youn-Hee Han (Korea University of Technology and Education, Korea)

컴퓨터 및 통신 시스템(KTCCS) 논문지 편집위원회

위 원 장 | 한연희 (한국기술교육대학교)

부 위 원 장 | 백상헌 (고려대학교) 이관용 (한국방송통신대학교) 이덕규 (서원대학교) 최종명 (목포대학교)

위 원 | 강윤희 (백석대학교) 김경백 (전남대학교) 김원태 (한국기술교육대학교) 문병인 (경북대학교)
박광진 (원광대학교) 박능수 (건국대학교) 박재성 (수원대학교) 박희완 (한라대학교)
송두희 (원광대학교) 윤종희 (영남대학교) 윤주상 (동의대학교) 이종혁 (상명대학교)
이태규 (평택대학교) 이화민 (순천향대학교) 이훈재 (동서대학교) 최성곤 (충북대학교)
한영선 (경일대학교) 허 경 (경인교육대학교)

소프트웨어 및 데이터 공학(KTSDE) 논문지 편집위원회

위 원 장 | 길준민 (대구가톨릭대학교)

부 위 원 장 | 김영갑 (세종대학교) 박용범 (단국대학교) 전재욱 (성균관대학교) 정광식 (한국방송통신대학교)
조용윤 (순천대학교)

위 원 | 고명숙 (부천대학교) 김미혜 (대구가톨릭대학교) 김병욱 (동국대학교) 김상근 (성결대학교)
김성석 (서경대학교) 김수균 (배재대학교) 김영철 (홍익대학교) 김우열 (대구교육대학교)
김익수 (숭실대학교) 김정아 (가톨릭관동대학교) 김종호 (순천대학교) 김한성 (한국교육학술정보원)
박기남 (고려대학교) 박상준 (군산대학교) 오세창 (세종사이버대학교) 오효정 (전북대학교)
이공주 (충남대학교) 이대원 (서경대학교) 이성욱 (한국교통대학교) 이종혁 (대구가톨릭대학교)
이준호 (성균관대학교) 이현아 (금오공과대학교) 정영애 (선문대학교) 정재화 (한국방송통신대학교)
조상현 (네이버) 최종선 (숭실대학교) 한경호 (단국대학교)

2017년 9월호 특집 담당위원

특 집 위 원 | 양순옥 (가천대학교)

2017년 11월호 특집 담당위원

특 집 위 원 | 김호원 (부산대학교)

2018년 1월호 특집 담당위원

특 집 위 원 | 김종완 (삼육대학교)

ISSN 1226-9182

정보처리학회지

Korea Information Processing Society Review

www.kips.or.kr

KIPS

2017년 9월, 11월, 2018년 1월 | 제24권 제5호, 제6호, 제25권 제1호 | 합본

KIPS 권두언

‘4차 산업혁명’ 특집을 발간하며...

이번 특집호에서는 최근 사회의 주요 이슈로 회자되고 있는 ‘4차 산업혁명’을 정보통신 기술 관점에서 정리하고 4차 산업혁명이 어떤 기반 기술에 의해 어느 방향으로 개발이 진행되고 있는지 그 현황을 살펴보고자 하였습니다.

정보통신 기술 발전이 각 산업 분야에 스며들면서 4차 산업혁명이 시작되고 있습니다. 앞으로 다양한 산업 분야에 광범위하게 파고들어 더욱 빠른 속도록 변화를 이끌어 갈 것으로 전망됩니다. 이러한 변화는 상당 부분 컴퓨터 과학자들의 노력의 결과라고 할 수 있으며, 향후 그 역할이 더욱 중요해진다는 의미를 가집니다.

“컴퓨터 과학자들이 지금까지와 같이 세분화된 전문 분야의 연구에만 집중하면 이러한 변혁은 가능할까?” 라는 질문을 던져야 할 때인 듯합니다. 사회의 패러다임이 바뀌고 컴퓨터 과학자들에 대한 사회의 기대치가 커지면서 “컴퓨터 과학자들도 무엇을 어떻게 연구해야 할 것인가?” 라는 근원적인 고민을 해야 할 때인 듯합니다.

치열한 연구에 의해 기존에 없던 기술이 세상에 선보이게 되고, 상용화를 위한 추가적인 연구 개발로 인해 대중에게 친숙해지는 과정을 거치게 됩니다. 예를 들면, 인터넷도 그러한 과정을 거쳐 이제 누구나 이용하는 대중적인 기술이 되었습니다. 그리고 사물 인터넷, 클라우드 컴퓨팅, 빅 데이터, 가상 현실, 증강 현실, 인공 지능 등의 기술이 적용된 제품이나 서비스를 실생활 속에서 쉽게 발견할 수 있습니다. 이는 컴퓨터의 지식이 전문 지식이 아닌 대중적인 지식으로 일반화되는 것을 의미합니다. 이러한 지식의 일반화가 빠르게 진행되고 있으며, 그 범위도 확대되는 추세입니다.

또한 세분화 · 전문화되어 단절되어 가던 세상을 정보통신 기술은 협업과 협력이 가능한 연결과 소통의 장으로 바꾸어 놓았습니다. 실시간 소통과 협력이 가능한 세상은 많은 과정과 시간을 단축시키고 효율성을 높이며, 기존의 발상으로 생각하지 못하던 새로운 형태의 제품, 서비스, 상거래 등을 가능하게 하고 있습니다. 하지만 그와 함께 새롭게 등장하는 제품이나 서비스의 영역이 넓어지면서, 파생되는 문제들 또한 예측하지 못한 부분까지 확대되는 추세입니다. 이는 상당부분 컴퓨터 과학자들의 역할의 확대를 의미하며, 사회에서 거는 기대 또한 커지고 있습니다.

4차 산업혁명은 2016년 다보스포롬(Davos forum)에서 클라우스 슈밥(Klaus Schwab)이 언급하면서 전 세계적으로 주요 이슈로 부각되었습니다. 그리고 2011년 독일의 Industrie 4.0 프로젝트가 시작되면서 제조업에 사물 인터넷을 비롯한 선진 정보통신 기술이 도입되고, 경제시스템 전반적으로 혁신을 가져오면서 그 영향력이 확대되고 있습니다. 산업 인터넷을 기반으로 추진하는 미국, 로봇의 강점을 기반으로 추진하는 일본, 제조업 육성을 위한 산업정책을 추진하는 중국 등 여러 국가들이 미래 국가의 국운이 걸려 있다고 판단할 정도로 4차 산업혁명을 중요하게 인식하고 뒤처지지 않기 위해 정책적인 지원을 아끼지 않고 있습니다. 4차 산업혁명은 이미 시작되었으며 정점을 향해 기술이 성숙될수록 각 분야에서 고도화에 대한 요구도 점점 커지고 있습니다.

위와 같은 이유로 한국정보처리학회에서는 큰 사회적 변혁의 흐름인 4차 산업혁명의 중요성을 살펴보고 함께 고민해보고자 본 특집을 준비하였습니다. 이번 특집의 학회 원고 모집 공고에 여러 필자들이 응모하여 구성되었다는 점에서 컴퓨터 과학자들의 많은 관심을 확인할 수 있었습니다.

원고를 준비하고 보내주신 저자 분들께 감사드리며 원고를 준비 중이었던 분들께는 일정상 아쉽게도 다음의 기회를 약속드리며 인사를 대신하고자 합니다.

2017년 9월

한국정보처리학회 학회지편집위원장
가천대학교 초빙교수 양순옥

특집 01

사물 인터넷, 사이버 물리 시스템, 빅 데이터, 인공 지능 등의 기술에 의한 4차 산업혁명의 진행 상황*

양순옥 (가천대학교)

목 차

1. 개 요

2016년 다보스포럼에서 클라우스 슈밥(Klaus Schwab)이 4차 산업혁명을 주창하였다[1]. 4차 산업혁명은 정보통신 기술(Information and Communications Technology, ICT)이 여러 산업 영역의 기반 기술과 융합되면서 이루어낸 변화를 의미한다. 사람들은 기술의 발전이 가져올 미래를 기대하면서도, 산업혁명이라는 단어로 인하여 막연한 불안감을 갖기도 한다. 하지만 과거 인터넷을 위시한 디지털 기술에 의한 혁신을 생각해보자. 비록 초기에는 인터넷으로 인한 생활의 변화가 다소 낯설었지만, 시나브로 일상생활 깊숙이 파고들면서 이젠 없어서는 안될 기제(旣製)가 되었다. 이처럼 지금까지 기술의 진보는 세상을 더욱 편리하게 만들었다. 4차 산업혁명도 이와 유사한 발전 과정을 보일 것으로 예상된다.

4차 산업혁명은 (그림 1)과 같이 사물 인터넷(Internet of Things, IoT), 사이버 물리 시스템(Cyber Physical System, CPS), 빅 데이터(Big Data), 인공 지능(Artificial Intelligence, AI), 가상 현실(Virtual Reality, VR), 3D 프린팅, 로보틱스 등 다양한 기반 기술들이 개별적으로 발전하면서 융·복합화되고, 다시 여러 산업 분야에 적용되면서 구체화되고 있다[2,3].

이는 정보통신 기술이 타산업의 기반 기술이나 제품, 서비스 등에 큰 영향을 미치고, 더 나아가 인류의 생활방식, 산업구조, 생태계를 변화시킬 수 있는 혁신적 기술, 즉 다이버전스(Divergence) 기술이 되고 있음을 의미한다[4]. ICT가 다양한 분야에 적용되면서 관련 기술이나 제품, 서비스들이 크게 개선(upgrade)되는 것이 4차 산업혁명이 가져올 주요 특징 중 하나이다.

누구나 일상생활 속에서 의식하지 못한 상태에서 다양한 기술들의 혜택을 누릴 수 있는 단계

* 이 논문은 과학기술정보통신부 SW중심대학 사업의 일환인 가천대학교 SW중심대학 사업단의 지원을 받아 연구되었습니다.

(그림 1) 산업혁명 역사 속에서 제조 시스템의 진화 과정

로 발전하고 있다. 또한, 제품의 기획, 설계, 제조, 생산, 물류, 유통, 판매 등의 제조 시스템에 발전된 ICT가 적용되며 경제 시스템의 전반적인 변화를 가져오고 있다. 이러한 변화의 혜택을 누구나 누리게 되는 것이 4차 산업혁명이다.

본고에서는 4차 산업혁명 관련 주요 기술의 연구개발 수준이나 개요를 살펴보고자 한다. 먼저 사물 인터넷, 사이버 물리 시스템, 빅 데이터, 인공 지능에 대해 간략히 살펴본다. 그리고 자율주행차 분야나 차세대 지능형 교통 시스템을 통하여 4차 산업혁명이 가져올 사회 변화를 가늠해 보고자 한다.

2. 관련 기술

2.1 사물 인터넷

사물 인터넷은 각종 사물에 센싱과 통신 기능을 내장하여 네트워크를 통해 데이터를 전달하는 기술이다.

이에 대한 보다 일반적인 정의는 인간, 사물, 공간 세 가지 환경요소에 대해 인간의 개입 없이 상호 협력적으로 센싱, 네트워킹, 정보처리 등 지능적인 관계를 형성하는 사물 공간 연결망을 의미한다. 나아가 ICT를 기반으로 실세계(Physical World)와 가상 세계(Virtual World)의 다양한 사물들을 연결하여 진보된 서비스를 제공하기 위한 서비스 기반 기술이다[5].

사물 인터넷의 발전 방향이나 성숙도 모델에 대해 다양한 관점이 존재한다. (그림 2)와 같이 사물 인터넷의 발전 단계를 디바이스 연결 단계 (IoT 1.0), 인프라 구축 단계 (IoT 2.0), 산업별

(그림 2) 사물 인터넷 발전 단계

혁신 솔루션 개발 단계(IoT 3.0)로 구분한 IBM의 관점이 대표적이다[6]. 현재 사물 인터넷 기술은 연결성(Connectivity)과 관리 중심의 1.0에서 초연결성(Hyper-connectivity), 지능 중심의 2.0으로 진화하고 있다. 즉, 사물의 등록, 탐색, 연결을 통해 모든 것이 인터넷에 연결되는 IoT 1.0에서 사물에 지능을 부여하여 현장의 문제에 즉각적으로 대응하여 해결 가능한 2.0 시대로 진입하고 있다(그림 3 참조)[7].

사물 인터넷은 다양한 분야에 적용되면서 그 응용에 적합하게 기술적인 범위를 넓히고 있다. 한 예로, 최근 사물 인터넷을 제조 공장에 적용하기 위해 산업용 사물 인터넷(Industrial Internet of Things, IIoT)이 개발되었다. 센서가 부착된 기계 장비나 로봇이 주변 장비나, 기기, 인프라, 작업자와 연결되어 데이터를 주고받으면서 능동적으로 기능을 수행할 수 있도록 지원하는 기술이다. 이 기술로 인하여 이전 공장의 소품종 대량생산(Mass Production) 체제에서 다품종 맞춤형 적량·대량 생산(Mass Customization) 체제로 전환되고 있다[8](그림 4 참조). 이를 위해 공장의 특성에 적합한 센서 장비, 산업용 이더넷 네트워킹 기술, 보안 기술, 사이버 물리 시스템, 데이터 처리 기술 등이 개발되고 있다.

(그림 3) IoT 1.0과 IoT 2.0의 비교

2.2 사이버 물리 시스템(Cyber-Physical Systems, CPS)

사물 인터넷이 통신 기술에 기초하여 수많은 사물들을 연동하는 기술이라면, 사이버 물리 시스템은 가상공간의 컴퓨터가 네트워크를 통해 유기적으로 융합됨으로써 사물들이 서로 소통하며 자동적, 지능적으로 제어되는 시스템이다. 실제 물리 세계와 거의 동일한 사이버 모델을 구축한 후, 물리세계와 긴밀한 상호작용으로 동기화하면서 활용하는 실시간 자율제어 시스템의 사이버 모델, 즉 '디지털 쌍둥이'가 구축되어 활용된다(그림 5 참조)[9].

물리 세계의 다양한 센서를 통해 감지된 데이터가 사이버 세계의 컴퓨터에 전달되고 분석·처리된 후, 다시 물리 시스템을 제어하여 새로운 기능과 특성을 가능하게 한다. 사이버 물리 시스템은 인간이 물리 세계의 사물들과 소통하는 방식을 근본적으로 혁신시키고 있다. 이는 공장, 전력망, 교통 시스템, 공공 기초시설, 의료 시스템, 빌딩 시스템, 국방 시스템 등 복잡한 핵심 인프

(그림 4) 인더스트리 3.0 대 인더스트리 4.0

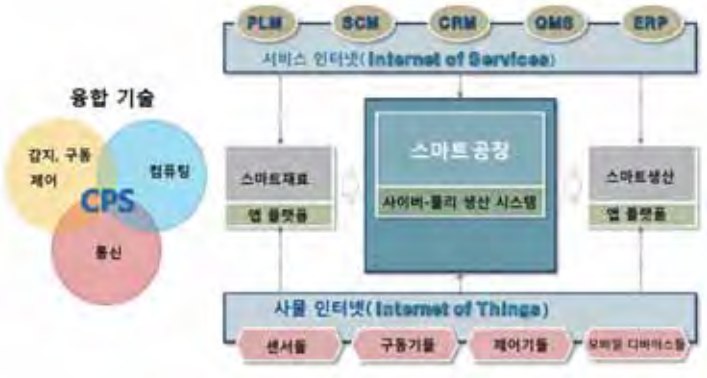
(그림 5) 사이버 물리 시스템 개념도

라에도 적용되고 있다. 제조 공장에도 사이버 물리 시스템 기술이 적용되고 있다[10]. 공장 내부 기기들이 생산, 제어, 안전 기능 등을 스스로 관리하는 스마트공장으로 전환되어 접속된 기기끼리 자율적으로 동작하여 자동화를 촉진시키고 있다. 이를 위해 사이버 물리 시스템 플랫폼을 중심으로 모든 사물과 서비스, 작업자들이 소통하며 동작한다(그림 6 참조).

구체적으로 효율적인 공장 내부 설계 및 운영을 지원하고, 공정이상, 설비고장 등의 상황 변화를 각종 센서 등으로 감지하고 판단한 후 적절한 대응을 수행한다. 다양한 프로세스 및 정보들을 가상으로 연결시켜 작업자, IT 시스템, 제조 프로세스 및 제품 간 양방향의 정보교환을 자유롭게 지원한다. 또한, 사이버 물리 시스템에서 수집된 대용량 데이터는 분석 작업을 거쳐 실제 제조 공정이나 의사결정 과정에 활용되어 유연한 제조 공정을 구현하는데 중요한 역할을 한다.

사이버 시스템의 연산 결과에 따라 물리 시스템의 상황이 변화하는 메커니즘의 상호관계를 밝혀내기 위해 물리 시스템을 수학적으로 표현하는 모델링 작업이 필요하다. 기존의 제어 시스템에 대한 이해가 아닌 자연과학을 기초로 하여 컴퓨터 과학을 융합한 새로운 융·복합적 학문 체계의 정립도 필요하게 된다[11].

사이버 시스템은 실시간으로 수집되는 대용량 데이터를 처리해야 하는 양적 복잡성과, 물리 세계에 있는 수많은 대상들을 연결해야 하는 질적 복잡성을 처리해야 한다. 이러한 복잡성 문제를 해결하기 위해 다양한 분야에서 연구개발이 이루어지고 있다. 예를 들면, 다양한 센서의 개발과 소형화, 빅 데이터 기술 등을 통해 센서가 생성해 내는 막대한 양의 데이터 중에서 특정 상황에 관련된 데이터를 실시간으로 처리하는 기술들이 개발되고 있으며, 머지않아 사이버 물리 시스템의 복잡성 문제를 극복할 수 있을 것으로 예측된다.



(그림 6) 스마트공장 구축을 위한 사이버 물리 시스템

CPS(Cyber Physical Systems) : 사이버 물리 시스템
PLM(Product Lifecycle Management) : 제품 수명 주기 관리
SCM(Supply Chain Management) : 공급 사슬 관리
CRM(Customer Relationship Management) : 고객 관계 관리
QMS(Quality Management System) : 품질 경영 시스템
ERP(Enterprise Resource Planning) : 전사적 자원 관리

2.3 빅 데이터

빅 데이터는 4차 산업혁명을 주도하는 기술 중 하나이다(그림 7 참조)[12]. 여러 응용에서 생성되는 대용량 빅 데이터를 수집하고 분석한 후, 여러 기술에 의해 해석되고 적절한 판단과 자율 제어를 수행함으로써 초지능적인 생산/서비스를 제공하게 된다.

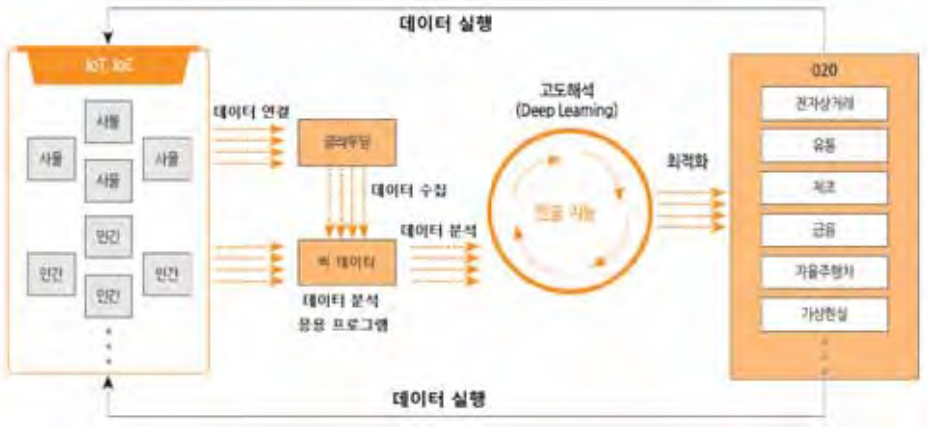
빅 데이터란 생성주기가 짧은 문자, 소리, 영상과 같은 다양한 형식의 데이터를 의미하며, 더 나아가 이러한 데이터를 분석하여 가치를 추출하는 기술을 의미한다. 즉, 생성된 지식을 바탕으로 능동적으로 대응하거나 변화를 예측하기 위한 정보화 기술의 총칭이다. 초기에는 데이터 규모와 기술적인 측면에서 출발했지만, 빅 데이터의 가치와 활용효과 측면으로 의미가 확대되는 추세이다. 분석 대상은 정형(Structured) 데이터뿐만 아니라 기존의 관리 방법이나 분석 체계로 처리하기 어려운 비정형(Unstructured) 데이터 집합도 포함된다.

저장할 데이터의 종류나 저장 방식을 결정하는 단계부터 시작하여 얻어진 데이터에서 의미 있는 정보를 추출해내는 전 과정에서 다양한 지원 소프트웨어와 분석 방법들이 지속적으로 개발되어 적용되고 있다.

대용량 데이터를 저장하고 처리할 수 있는 아파치 하둡(Apache Hadoop)이나 클러스터 컴퓨팅 프레임워크인 아파치 스파크(Apache Spark), 하이브 등 핵심 기술 중 상당 수가 개방형 소프트웨어로 제공되고 있어 그 활용범위가 다양해지고 있다.

4차 산업혁명은 여러 응용에서 수집된 빅 데이터를 어떻게 분석하고 활용할 것인가가 중요한 이슈가 된다[13]. 빅 데이터와 빅 데이터 처리 플랫폼은 아직 초기 인프라 구축과 데이터의 효율적 축적 기술에 머무르는 상황이다[14]. 빅 데이터 장점인 비정형 데이터 처리나 실시간 분석은 아직 본격적으로 활용하기에는 미흡한 실정이다.

하지만, 오픈 소스 기반의 플랫폼 기술의 성장으로 전통적인 클라우드 기업뿐만 아니라 수요자 중심의 맞춤형 소프트웨어를 제공하는 중소벤처기업들도 시장에서 성장할 수 있는 경쟁력을 갖추어 나가고 있다. 또한 왓슨, 알파고 등을 활용하는 인공 지능의 활용성에 대한 기대치도 높아지고 있다. 행정, 의료, 재난, 환경, 교육 등



(그림 7) 4차 산업혁명에서 데이터 처리 과정

의 서비스 제공에 필요한 정형·비정형데이터를 통합 관리할 수 있는 통합 플랫폼 개발 및 맞춤형 서비스 구현도 활발하게 진행되고 있다.

2.4 인공 지능

인공 지능은 인간이 지닌 지적 능력의 일부 또는 전체를 인공적으로 구현하는 기술이다. 대용량 학습 데이터를 이용하여 스스로 학습하면서 지식을 축적하여 의미 있는 정보를 도출한다. 즉, 기계(컴퓨터)가 인간 수준의 인지, 이해, 추론, 학습 등의 사고 능력을 모방할 수 있도록 고안된 것이다. 따라서 인공 지능 기술은 컴퓨터 과학의 여러 세부 영역과 연계되어 있다.

인공 지능은 인간과 동일하게 범용 분야에서 자율적 사고와 활동이 가능한 강(强) 인공 지능 분야와 기계학습, 딥 러닝, 빅 데이터 등에 기초하여 특정 문제 해결이나 추론을 하는데 중점을 둔 약(弱) 인공 지능 분야로 구분 된다[15].

궁극적으로 인공 지능 연구는 사람과 같은 감정이나 심리상태를 지닌 지능형 로봇을 구현하는 강 인공 지능을 목표로 진행하고 있다[16]. 즉, 컴퓨터가 인간의 감성을 이해하고 교감할 수 있는 인공 지능을 추구한다. 인간모방, 인간지원, 인간이해의 인간 중심 방향으로 기술은 진화하고 있다(그림 8 참조)[17].

인간모방은 인간이나 생명체의 기능 및 능력을 모방 또는 확장하는 기술 분야이다. 사물 인터넷을 비롯한 착용형 기술이 주로 여기에 활용된다.

기술적 진보가 뒷받침되면, 착용형 기기는 인간의 활동과 생활에서 부족한 부분을 능동적으로 보조해 주는 인간지원 기술로 그 영역이 넓어질수 있다. 인간이해 기술은 인간의 감정 및 심리 등을 이해하여 이를 응용하는 분야이며, 뇌-

(그림 8) 인간중심 미래기술 전망

컴퓨터 연결 기술이 필수적이다. 인간의 뇌와 같이 능동적인 학습 및 추론이 목표인 딥 러닝 기술과 뇌-컴퓨터 연결 기술의 접목을 통하여 컴퓨터가 인간을 이해하고, 인간이 명령을 내리기도 전에 그 의도를 파악하여 도와주는 능동 사물 인터넷, 착용형 디바이스 기술 개발의 방향성이 되고 있다.

모든 대상에 인공 지능이 탑재될 경우, 인간-기계의 연결 및 기계-기계의 연결에 있어 높은 신뢰도의 제공은 중요한 문제로 부각될 수 있다. 이 분야에는 신뢰 분석을 위한 뇌공학 및 인공지능 기술 개발이 부상하고 있다.

인공 지능은 놀라운 속도로 발전하고 있고, 전 산업에 걸쳐 영향력을 확대하고 있다. 향후 인공지능의 주요 이슈는 자동화이다. 단순 데이터 분석 수준이 아닌 프로그램 운용의 자동 수행이 필수가 될 전망이다. 강(强) 인공 지능의 실현까지 아직 해결하지 못한 난제들이 많이 있지만, 인간이 통제 가능한 방법으로 발전해 나갈 것으로 예상된다.

3. 4차 산업혁명의 진행 상황

이 장에서는 4차 산업혁명의 현재 진행 상황

을 가늠해 보기 위해, 이전 장에서 정리한 사물 인터넷, 사이버 물리 시스템, 빅 데이터, 인공 지능 등의 기반 기술이 적용되는 자율주행차 분야와 차세대 지능형 교통 시스템 분야를 통해 살펴보고자 한다.

3.1 자율주행차

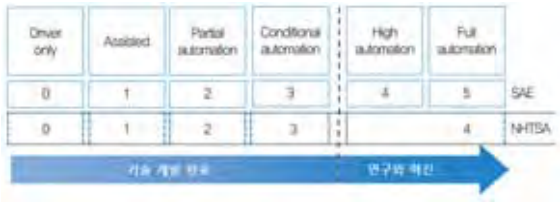
자율주행차란 운전자 도움 없이 스스로 주변 상황을 인지하면서 목적지까지 주행이 가능한 자동차를 의미한다[18]. 다양한 기반 기술들이 발전함에 따라 자율주행차의 연구개발이 활발하게 진행되고 있다.

차량이 스스로 움직이기 위해서는 주변 정보를 수집할 수 있는 센서 및 디바이스, 이들간의 통신을 지원할 수 있는 네트워크, 수집된 데이터 분석, 제어 시스템 등이 필요하다. 그 외에도 운전자 맞춤형 서비스 제공 기술도 요구된다.

우선 차량사물 통신(Vehicle to Everything communication, V2X)이나 빅 데이터 분석 기술에 의해 외부 데이터의 수집 및 분석이 가능해졌다. 인공 지능 기술을 활용하여 수집, 분석한 데이터로부터 적절한 의사결정을 수행함으로써 자동차 스스로 운행할 수 있다. 인공 지능은 주로 '인지 기능'을 담당하고 있으며, 센싱/측위/제어 영역으로 확대되고 있다. 또한, 자율주행차의 핵심 역할인 고가의 LiDAR 기능이 딥 러닝 기반의 실시간 깊이 추정 기술로 대체되고 있다(그림 9 참조). 이 외에도 클라우드 서비스, 운전자 상호작용, 차세대 텔레매틱스 등의 서비스 이용도 가능하게 되었다.

자율주행 기술은 크게 5단계(NHTSA 기준, SAE 기준으로는 6단계)로 분류할 수 있다(그림 10 참조). 0단계는 어떠한 자율 주행 기술도 적용되지 않은 상태이다. 차선 이탈 경고(Lane Departure Warning)/전방 충돌 경고(Forward Collision Warning, FCW)/고속도로 운전지원 시스템(Highway Driving Assist System)과 같은 기술이 적용되는 1-2단계는 다수의 상용화된 자동차에 구현되어 활용되고 있다. 구글 자동차나 아우디의 TTS는 운전자의 개입 없이 자동차가 스스로 차선을 변경하거나 추월이 가능하다. 기

(그림 9) 자율주행 자동차의 4가지 요소 기술



출처: EpoSS 2015 (재정립)

(그림 10) 자율주행차의 단계별 구분

상 악화와 같이 운전자의 개입이 필요한 경우에만 간헐적으로 개입하여 부분적으로 자율 제어하는 3단계의 기술이 적용되고 있다. 4단계는 인간 운전자 도움 없이 완전 운행이 가능한 수준을 의미한다. NHTSA는 2020년에 3단계 자율주행 기술을 장착한 차량 양산 시스템이 구축되고, 2025년에 4단계, 즉 완전 자율주행차를 볼 수 있을 것으로 전망한다.

3.2 차세대 지능형 교통 시스템

지능형 교통 시스템(Intelligent Transport Systems, ITS)은 교통수단이나 교통시설에 정보·통신·전자제어 등 첨단기술을 도입해 교통체계 운영의 효율성과 안전성을 높인 기술이다. 도로 전광판을 통해 차량의 정체 상황을 알리거나, 버스 정류장에서 도착정보를 확인하는 것, 고속도로 하이패스 단말기를 통해 통행료를 지불하는 것 등도 포함된다[19]. 차세대 지능형 교통 시스템(Cooperative-Intelligent Transport Systems, C-ITS)은 단순히 도로 구간 정보를 제공하는 데 그치지 않고, 도로·자동차·보행자가 차량 내·외부에 부착된 센서를 통해 서로 정보를 주고 받음으로써 사고를 예방하고 교통 효율성을 높이는 협력형 시스템이다(그림 11 참조). 차량 간 통신(Vehicle to Vehicle communication, V2V)과 차량과 도로시설 간 통신(Vehicle to Infrastructure communication, V2I)으로 상징되는 사물 인터넷 기술이 핵심이다.

특히 C-ITS는 V2V를 통해 다른 차량에 대한 정보를 빠르고 정확하게 수신하여 상황에 적절하게 대처할 수 있도록 지원한다. C-ITS와 자동 제동장치(AEBS), 차선 이탈 방지 장치(LDWS) 등을 연동하면 졸음운전 등으로 인한 위급 상황에서 차량의 자동 제어도 가능하다. C-ITS는 자율주행차 시대를 완성할 핵심 기술이며, 우리나라의 경우, <표 1>과 같이 2030년까지 전국 도로의 30%에 시스템을 도입할 계획이다.

(그림 11) 차세대 지능형 교통 시스템

<표 1> 차세대 지능 교통 시스템 추진 계획

출처: 국토교통부

2014~2016년	• 대전~세종고속도로 등 87.3km 대상 시범 사업 실시
2017~2020년	• 전국 고속도로에 전면 설치, '스마트 하이웨이' 달성
2021~2025년	• 대도시권 1만2,000km에 도입
2025~2030년	• 중소도시권 1만km에 도입, 전체 도로 30%에 설치

3.3 4차 산업혁명의 진행 상황

현재는 언제, 어디서나, 어떤 종류의 단말을 가지고, 어느 네트워크를 통해서든, 어떠한 콘텐츠를 이용할 수 있는 유비쿼터스(Ubiquitous) 시대에 진입하고 있다. 진보된 기술의 사회적·경제적 파급 효과가 커지면서 이러한 현상을 사회·경제학적인 관점으로 보면 4차 산업혁명이 되고, 기술적 관점으로 보면 유비쿼터스 혁명이 된다.

어떤 관점에서든 사회 전반에 커다른 변화를

가져온다는 점에서 그 파급력을 가늠하기는 쉽지 않다. 이를 위해 각 산업 분야와 함께 사회 인프라의 구축 측면을 동시에 살펴보아야 한다.

3G, 4G, LTE, 5G의 이동통신 기술과 WiFi, Bluetooth, ZigBee 등 근거리 무선 네트워크 기술의 발전으로 사물 인터넷이 실현되고 초연결성이 가능한 인프라가 구축되었다. 즉, 사회, 경제, 산업 전반이 초연결화, 초지능화, 초융합화라는 거대한 변화를 경험하게 되었다. 또한, 빅 데이터 기술의 성숙으로 초연결 상황에서 생성되는 방대한 데이터 분석이 가능해졌다.

이후 현실과 동일한 사이버 세계에서 제어하고자 하는 요구와 사람처럼 인지하고 판단하고자 하는 요구가 증가하면서 사이버 물리 시스템과 인공 지능 분야에서 관련 연구가 활발히 진행중이다. 이러한 기술이 <표 2>와 같이 공공안전, 경제산업, 생활복지 등의 분야에 광범위하게 적용되면서, 그 변화를 많은 사람들이 서서히 느끼며 4차 산업혁명을 체감하게 될 것이다.

또한, 인프라 구축으로 인한 초연결성의 실현은 고기능에 대한 요구를 수용할 수 있게 하였고, 그 결과 주요 산업 분야에 '스마트(Smart)'라는 접두어를 붙여 활용하려고 하고 있다[20]. 스마트공장, 스마트자동차, 스마트도시, 스마트그리드, 스마트헬스케어, 스마트홈/빌딩, 스마트국방, 스마트 재해대응 등이 대표적이다.

4차 산업혁명은 2011년 독일의 Industrie 4.0을 계기로 시작되어 자율주행차와 같이 경제적 파급효과가 큰 분야부터 빠르게 변화시키고 있다. 이러한 주요 산업 분야에서 안정성, 효율성, 신뢰성, 보안성에 혁신적인 변화를 가져와 새로운 부가가치를 창출하면서 변화를 선도하고, 다른 분야로 파급되어 전 산업 분야로 확대되어 가게 된다.

NHTSA는 2025년 완전 자율주행차의 상용화와 2030년경 자율주행차의 대중화를 전망한다. 이처럼 2030년경에는 각 산업분야에 사물 인터넷, 사이버 물리 시스템, 인공 지능 등의 기술이 스며들어 상용화되고 대중화될 것으로 예측된다. 이로 인한 사회적 경제적 파급효과가 커지면서 4차 산업혁명의 성숙기에 접어들 전망이다.

<표 2> 4차 산업혁명의 진행 분야

분야	부문
공공안전	재난·재해관리
	구조물 관리
	국방
	사회안전
	행정서비스
경제산업	비즈니스/상거래
	생산/제조
	금융
	물류/유통
	교통/운수
	농·축·수산
생활복지	생활
	관광/레저
	환경
	의료/복지

4. 결 론

본고에서는 4차 산업혁명을 견인하는 주요 정보통신 기술을 통해 4차 산업혁명의 진행 상황을 살펴보았다. 각 산업 분야에 스며드는 사물 인터넷, 사이버 물리 시스템, 빅 데이터, 인공 지능 기술의 개발 및 연구 방향을 살펴보고, 자율주행차 분야의 사례를 가지고 4차 산업혁명의 진행 상황을 가늠해 보았다.

4차 산업혁명은 계속 진행형이다. 관심을 갖고 꾸준히 모니터링을 해야 변화의 흐름을 파악할 수 있다. 큰 변화에는 기회의 요인과 위협의 요

인이 상존하는 속성을 가진다. 4차 산업혁명을 기회의 요인으로 인식하는 계기가 되었으면 한다.

참 고 문 헌

[1] 클라우스 슈밥, "제4차 산업혁명", 메가스터디(주), 2016.
[2] Dong-A Business Review, 2014.
[3] Cloud-based Manufacturing: Old wine in new bottles? 2013.
[4] 연승준, 한억수, 김수경, "혁신적 ICT R&D 정책 지원을 위한 ICT 다이버전스 패러다임 연구", 한국통신학회 2017년도 동계종합학술발표회, pp. 79~80, 2017.
[5] 양순옥, 김성석, "4차 산업혁명을 견인하는 다이버전스 기술 사물 인터넷(IoT)", 생능출판사, 2018.
[6] http://klabcamss.blogspot.kr/2014/08/iot-30.html
[7] 박준희 외 9인, "IoT기반 초연결 공간 분산지능 기술", 한국전자통신연구원, 2018.
[8] LG Business Insight, 2016.
[9] 손상혁, "융합의 또 다른 이름, 사이버 물리 시스템", 프런티어, 2016.
[10] Kagerman H, Wahlster W, Helbig J, "Recommendations for implementing the strategic initiative INDUSTRIE 4.0" in Final report of the Idustrie 4.0 Working Group, ACATCH, pp. 24, 2013.
[11] 임용재, 오영열, 박태준, 손상혁, "스마트한 신세계로의 초대, 사이버물리시스템", 방송통신 PM Issue Report, 2013.
[12] 복경수, "4차산업혁명과 빅데이터", 2017.
[13] SCM World-MESA, International Survey.
[14] 안춘모, "빅 데이터 플랫폼 현황 및 이슈 분석", ETRI Insight Report, 2017.
[15] 정병탁, 여무송, "Cognitive Computing I: Multisensory Perceptual Intelligence", 정보과학회지, 제30권 제1호, 2012.
[16] 윤장우, 허재두, "뇌과학과 인공지능 융합 미래 기술 발전 방향 예측", 전자통신동향분석 제33권 제1호, 2018.
[17] 김정태, 정지형, 이승민, "ECOsight 기반의 미래 기술전망-기술인문사회 통합적 기술 예측", ETRI Insight Report 13-2, pp. 172, 2013.
[18] 황영배, 조희영, "자율주행을 위한 인공지능 기술 동향", 한국산업기술평가관리원, 2016.
[19] http://conpaper.tistory.com/42838
[20] 양순옥, 김성석, 정광식, "사물 인터넷으로 발전하는 유비쿼터스 개론", 생능출판사, 2015.

저 자 약 력

양 순 옥

이메일 : soyang@gachon.ac.kr

- 1995년 고려대학교 원예과학과 (학사)
- 2002년 고려대학교 컴퓨터과학과 (석사)
- 2006년 고려대학교 컴퓨터과학과 (박사)
- 2006년~2008년 고려대학교 연구교수
- 2008년~2009년 연세대학교 연구교수
- 2009년~2010년 세종대학교 초빙교수
- 2010년~2012년 ETRI 선임연구원
- 2014년~2015년 미국 UTEP Post Doc.
- 2016년~현재 가천대학교 초빙교수
- 관심분야 : 사물 인터넷, 유비쿼터스 컴퓨팅, 분산 데이터베이스, 자율주행차, 스마트공장

특집 02

의약품 부작용 예측을 위한 빅데이터 분석 기술 동향

김현희 (동덕여자대학교)

목 차

1. 서 론

의약품은 여러 차례에 걸친 임상 시험을 통과하고 안정성을 평가받은 후 시판이 허가되지만, 임상 시험 단계에서 발견하지 못했던 중대한 부작용이 나타날 가능성이 항상 존재한다. 임신 초기 입덧에 효과적인 항구토제로 수년간 시판되었던 탈리도마이드는 후에 태아에서 사지결손증을 유발한다는 사실이 밝혀져 시판이 중지 되었으나, 이미 전세계 46개국에서 12,000명 이상의 기형아 출산을 야기하였다. 이 때 태어난 아이 중 40 %가 그해에 사망하였고 현재 생존자는 약 5,000명 정도로 추정된다[1]. 우리나라에서도 감기약 치료제로 널리 사용되었던 페닐프로판올아민 성분 제제가 출혈성 뇌졸중을 야기하는 것으로 밝혀져 판매 중지 되는 등 최근 10년간 국내외에서 의약품이 시판된 이후에 안전성 혹은 유효성 문제로 허가 취소되거나 판매 중지된 사례는 수십 건에 달한다[2].

의약품 부작용 (Side Effect)이란 의약품 등을 정상적인 용법에 따라 투여한 경우 발생하는 모든 의도되지 않은 효과를 말하며, 이 중에서 바람직하지 않은 징후, 증상 또는 질병을 이상 사례 (Adverse Event) 라고 한다[3]. 이러한 이상 사례의 원인은 허가 시점에서 얻을 수 있는 의약품 정보의 한계에서 기인한다. 즉, 시판 전 임상 시험 시 소아, 임산부 및 노인에 대한 시험이 제한되고 있으며, 임상 시험 후 일정 기간 동안 부작용 정보를 추적하므로 장기간이 지난 뒤 나타나는 부작용에 대한 발견이 어렵다. 또한 환자 개개인의 질환이나 병용되는 약물에 대한 고려되지 않는 경우가 많다. 따라서 의약품의 시판 후에도 부작용을 파악하고 관리하는 것이 필수적이다.

이와 같이 의약품 관련 문제의 탐지, 평가, 해석 및 예방에 관한 과학적 연구 및 활동을 약물

감시 (Pharmacovigilance) 라고 하는데[3], 약물 감시를 위해 자발적 부작용 보고 시스템이 구축되어 운영되고 있다. 미국 FDA에서 운영하는 자발적 부작용 신고 시스템 (Federal Drug Administration's Adverse Event Reporting System, FAERS) 의 경우 매년 60만건 이상의 부작용 신고가 접수되고 있으며, 세계 보건 기구 (World Health Organization)에서는 1968년 국제 약물 감시 체계를 구축하였고, 스웨덴의 웁살라 모니터링센터 (Uppsala Monitoring Center)에서는 1978년부터 전세계로부터 의약품 부작용 사례를 보고받고 있다[4]. 한국의 경우 한국 의약품 안전관리원에서 의약품 부작용 보고 시스템을 구축하고 데이터베이스를 관리 및 정보 제공을 담당하고 있다. 그러나 자발적 부작용 보고 자료는 의사나 약사, 간호사 등 의약 전문가나 제조회사에서 자발적으로 부작용 정보를 제공하는 것이므로 과소 보고의 제약점을 안고 있으며, 보고된 사례도 보고자에 따라 정보의 질이 현격히 다르다는 단점이 있다.

이와 같은 문제점을 극복하기 위해서 최근에는 부작용 보고 데이터베이스뿐만이 아니라 다양한 목적으로 구축된 데이터베이스들을 통합하여 정형화된 빅데이터를 구축하고 이를 약물 감시에 활용하고자 하는 연구가 활발히 이루어지고 있다. 특히 자발적으로 보고된 이상 사례 중에서 해당 의약품과의 인과관계를 배제할 수 없는 경우를 약물 이상 반응 (Adverse Drug Reactions)이라고 하는데, 빅데이터 분석을 통해서 약물 이상 반응을 탐지하고 약물과 약물 이상 반응과의 인과 관계인 실마리 정보를 찾아낸다면, 보다 신속한 의약품 부작용 관리가 이루어질 수 있다. 미국의 경우 하버드 대학을 협연 센터로 지정하고 전자 건강보험 청구자료, 입원 및 외래환자의 의무 기록, 환자 등록 자료 등을 통합하여 분산 데이터 분석 체계를 구축하였고, 유럽에서는 유럽의약품청 주도로 European Network of Centers for Pharmacoepidemiollogy and Pharmacovigilance (ENCePP)를 운영하여 유해성 조기 파악 방법론을 개발하고 있다. 국내에서도 병원전자의무기록자료, 건강보험심사평가원의 요양급여 청구자료 등을 연계하여 의약품과 부작용간 인과성 평가를 실시하였다[5].

또한 환자들이 소셜 네트워크에 올린 글이나 웹상의 게시물 등 비정형 텍스트 데이터를 활용하여 약물 이상 반응을 탐지하는 연구도 활발히 이루어지고 있다. 환자들의 소셜 네트워크 서비스인 patientslikeme[6]의 경우, 같은 질환을 가진 환자들끼리 증상, 부작용, 처방 기록 등의 정보를 주고받는 사이트로 기존의 데이터베이스에서 간과한 환자들의 의견이 고스란히 반영된 질병 정보 데이터를 제공하고 있다. 이와 같은 소셜 미디어 빅데이터의 활용은 임상 시험에 비하여 다양한 연령층 및 질환군을 포함할 수 있고, 의약품의 장기 사용에 의한 부작용 정보를 발견할 수 있다는 장점을 갖는다. 뿐만 아니라 시판 이후 부작용이 발견되고 평가를 거쳐 시판이 철회되기까지 비교적 많은 시간이 소요되므로 빅데이터 분석을 통한 부작용 예측은 그 시간을 단축시키는데 중요한 역할을 할 수 있다.

본 고에서는 제 2장에서 데이터 마이닝을 이용하여 부작용 보고 자료로부터 실마리 정보를 찾기 위한 분석 기법들을 알아보고, 제 3장에서 비정형 텍스트 분석을 통한 부작용 보고자료 분류 및 약물 이상 반응 탐지를 위한 소셜 미디어 분석에 활용된 기계 학습 기법들을 살펴본다. 제 4장에서 딥러닝을 활용한 디지털 약물 감시에 대해 소개한 다음, 제 5장에서 결론을 맺도록 한다.

2. 데이터 마이닝 기반 실마리 정보 검색 (signal detection) 기법

현재까지 가장 많이 알려진 부작용 실마리 정보 검색 기법은 미국 FAERS 데이터베이스에 데이터 마이닝 알고리즘을 적용하여 정량적인 방법으로 실마리 정보를 찾는 것이다[7,8]. 이중에서도 보고분율비 (Proportional reporting ratios, PRRs)와 보고오즈비 (Reporting odds ratios, RORs)가 가장 일반적이며 해석하기 쉬운 실마리 정보 검색 기법으로 널리 사용되고 있다. 표 1에서 보는 바와 같이 데이터베이스에 보고된 전체 보고건을 n 이라 하고, 약물 i가 갖는 부작용 j에 대한 보고건을 n_{ij} 이라고 하자. 이때 n_i는 약물 i 에 대한 보고건이고, n_j는 부작용 j에 대한 보고건이다[9].

보고분율비란 특정 약물 보고건의 특정 부작용 분율을 다른 약물 보고건의 부작용 분율로 나눈값을 말하며 다음 식과 같이 정의된다.

$$PRP = \frac{n_{ij/}n_i}{(n_j - n_{ij})/(n - n_i)}$$

보고오즈비란 특정 약물에 노출된 환자에서 발생한 특정 부작용 발생 오즈(odds)를 다른 약물에 대한 특정 부작용의 발생 오즈(odds)로 나눈 것으로 다음 식과 같이 정의된다.

$$ROR = \frac{n_{ij/}(n_j - n_{ij})}{(n_i - n_{ij})/(n - n_i - n_j + n_{ij})}$$

이밖에도 약물과 부작용간의 상관관계를 베이지안 방법을 활용하여 측정하는 Bayesian confidence propagation neural network (BCPNN) 방법[10]도 실마리지표 산출에 사용되고 있으며, 다양한 통계 기반의 데이터 마이닝 알고리즘들이 개발되고 있다. 이와 같은 데이터 마이닝 기반의 실마리 정보 검색 기법은 임상 시험이 갖는 여러 가지 제약점들을 극복하고 약물과 약물이상반응과의 인과 관계를 보다 신속하게 발견할 수 있다. 다만, 자발적 부작용 보고 제도는 과소 보고 문제를 항상 포함하고 있으므로 데이터 마이닝을 활용한 실마리 정보는 인과 관계의 가능성을 찾아주는 도구로서 보아야 할 것이다.

3. 기계 학습 기반 비정형 텍스트 분석과 활용

보다 최근에는 정형화된 의료 정보 빅데이터 뿐만이 아니라 비정형 텍스트 데이터에 대한 관심이 높아지고 있다. 바이오의약학 문헌은 약물간의 상호작용에서 오는 부작용 예측에 활용되고 있으며, 트위터와 같은 소셜 미디어도 환자들의 직접적인 목소리를 반영하므로 적극적으로 빅데이터 분석에 활용되고 있다. 텍스트 데이터

<표 1> 2 × 2 분할표

	부작용 j에 대한 보고건	부작용 j를 제외한 보고건	전체 보고건
약물 i에 대한 보고건	n_{ij}	$n_i - n_{ij}$	n_i
약물 i를 제외한 보고건	$n_j - n_{ij}$	$n - n_i - n_j + n_{ij}$	$n - n_i$
전체 보고건	n_j	$n - n_j$	n

의 경우는 직접적으로 부작용 예측에 활용되기 보다는 부작용 보고 자료를 기계 학습을 통해서 자동 분류하고, 소셜 미디어 데이터를 분석하여 약물 이상 반응에 대해 언급한 메시지를 분류하는 등 의약품 부작용을 파악하고 관리하기 위한 보조적인 툴로서 활용되고 있다.

본 장에서는 먼저 텍스트 데이터를 활용한 의약품 부작용 보고자료의 자동 분류 기법을 소개하고, 다음으로 소셜 미디어를 분석하여 약물 이상 반응을 탐지하기 위한 기계 학습 기법을 소개한다.

3.1 텍스트 데이터를 활용한 의약품 부작용 보고자료 분류

국내에서는 한국의약품안전관리원의 의약품이상사례보고시스템 (The Korea Adverse Event Reporting System, KAERS)을 통해서 자발적 보고자료를 등록하고 있다. 이때, 의사, 약사, 혹은 제약회사와 같은 보고자는 보고자료와 실제 부작용과의 인과성을 평가하고 평가에 대한 의견을 자연어로 기술하고 있다. 전문가 의견 텍스트 데이터를 가진 보고건수는 1989년에서 2015년 6월까지 약 90,552건으로 아직까지 전문가 의견 텍스트 데이터가 의약품 부작용 연구를 위해 활용된 적이 없다[11]. 일반적으로 부작용 보고자료는 인과 관계 평가기준으로 정의된 가이드라인에 따라서 확실함(certain), 상당히 확실함(probable), 가능함(possible), 가능성 적음(unlikely), 평가곤란(unclassified), 그리고 평가불가(unassessable)의 7개 카테고리로 나누어진다. 전문가 텍스트를 활용하여 보고자료를 인과관계에 따라 4개의 범주로 자동분류하고, 인과관계가 확실한 보고자료들만 미리 선별하여 부작용 보고 데이터베이스 활용 시 데이터의 질을 향상시키고자 하였다[12].

그림 1은 전문가 의견 텍스트 데이터베이스를 활용한 보고자료 자동 분류 구조를 나타낸다. 자동 분류를 위해서 나이브 베이즈 알고리즘을 사용하였으며, 학습 단계에서 각 카테고리에 해당하는 단어들을 효율적으로 학습시키기 위해 tf-idf 가중치 기반의 단어 사전을 구축하였다. 단어 사전은 전문가 의견 문서를 텍스트 마이닝하여 주요 단어를 추출하여 반자동적으로 구축하였다. 또한 보고자가 서술한 전문가 의견이 국영문 혼합문으로 되어 있으므로 이를 처리하기 위해서 WHO Adverse Reaction Terminology (WHO-ART) 온톨로지를 구축하였다. WHO-ART 코드[13]는 WHO에서 정의한 약물 부작용에 관한 표준 용어 정의로서, 국문 용어를 영문으로 통합하기 위해 사용하였다. 예를 들면, 국문으로 사용된 “구토”라는 단어는 WHO-ART 온톨로지에 의해 “vomiting”이라는 표준 용어로 변환되고 이를 통해 분류 정확도를 향상시켰다.

(그림 1) 텍스트 데이터를 활용한 부작용 보고자료 자동 분류 구조

3.2 약물 이상 반응 탐지를 위한 소셜 미디어 분석

임상 시험은 임상 시험 대상자의 연령, 임상 시험 기간, 규모 등 제약을 가진 환경에서 실시

되는 반면 소셜 미디어를 활용하면 보다 다양한 환자들의 실시간 데이터를 분석하여 부작용 예측에 활용할 수 있다는 장점이 있다. 특히 트위터 게시물에 언급된 약물 이상 반응의 경우 FAERS에 보고된 사례와 통계적으로 유의한 상관 관계가 있음이 입증되었다[14]. 트위터 게시물을 분석하여 약물 이상 반응을 탐지하는 연구의 대부분은 해당 트위터 게시물이 약물 이상 반응에 해당하는 게시물인지 그렇지 않은지를 분류하기 위해 지도 학습을 활용한이진 분류가 주를 이루고 있다. 트위터 게시물에 사용되는 용어들은 약물 이상 반응을 나타내는 표준화된 용어들과 상이하므로 국제 분류 체계인 Medical Dictionary for Regulatory Activities (MedDRA)에서 정의한 용어들로의 매핑이 필요하다. 뿐만 아니라 잘못된 철자나 인터넷 용어 등 증상을 나타내는 다양한 표현들을 표준 용어를 변환하는데 많은 전처리 작업이 요구되며, 용어 사전이나 온톨로지를 사용하여 용어의 표준화를 실시하고 있다.

[15]에서는 나이브 베이즈, 서포트 벡터 머신, 그리고 최대 엔트로피 기반 분류기를 활용하여 트위터 메시지를 이진 분류하였다. 성능을 향상시키기 위해서 약물 이상 반응에 관련된 어휘들을 정의하였으며, tf-idf 가중치를 사용하여 유사어 집합을 정의된 어휘들에 포함시켰다. 또한 토픽 모델링을 적용하여 특정 토픽에 해당하는 키워드를 찾아내어 어휘 정의에 활용하였다. 실험결과 서포트 벡터 머신이 다른 분류기에 비하여 가장 뛰어난 성능을 보임을 확인하였으며, 특히, 지도학습 기반의 분류기의 경우 토픽 모델링이나 감성 분석, 그리고 다중 코퍼스 활용 등을 통한 약물 이상 반응과 관련된 용어의 추출이 텍스트 분류의 성능 향상에 크게 기여했다는 것을 알 수 있다.

4. 딥러닝 기반 디지털 약물 감시

FAERS에 의해 보고되는 부작용 사례는 실제 사례의 1-13 % 정도로 추정되고 있으며, 보고까지 시간이 걸리는 경우가 많고, 보고 내용도 내원 환자의 경우로 치우친 경우가 대부분이다[16]. 이러한 점에서 소셜 미디어를 통한 부작용 보고는 다양한 연령대를 포함하며, 신속하게 보고되므로 기존의 자발적 의약품 부작용 보고 제도를 보완할 수 있는 대안으로 떠오르고 있다. 소셜 미디어를 활용한 약물 이상 반응 탐지를 디지털 약물 감시라고 하며 웹 페이지, 환자들의 소셜 네트워크 서비스, 트위터 등으로부터 약물이나 건강 상태 혹은부작용에 대한 텍스트를 수집하여 다양한 분석을 시도하고 있다. 대표적으로 활용되고 있는 소셜 미디어인 트위터 분석의 경우, 약물과 증상 및 부작용에 대한 용어 정의 및 표준 용어로의 매핑 작업이 큰 부분을 차지하며 용어 사전의 활용이 분석 성능을 좌우한다. 이러한 문제점을 보완하기 위해서 최근에 트위터 분석을 위해 딥러닝을 활용하여 트위터 메시지로부터 약물 이상 반응을 탐지하고자 하는 연구가 이루어지고 있다[16].

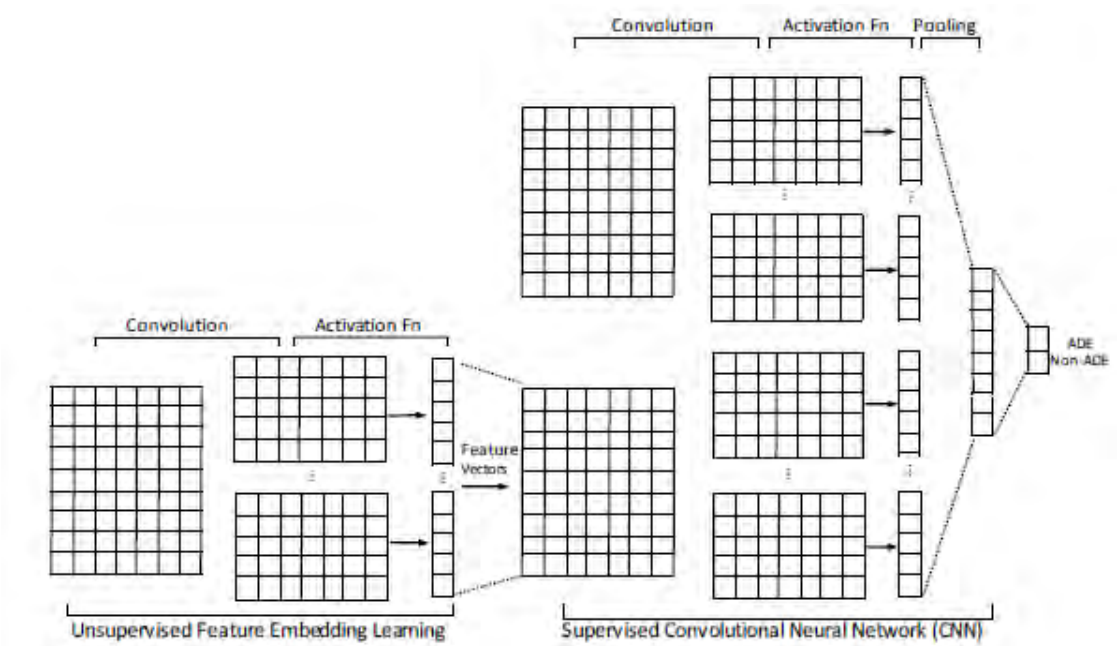
딥러닝 모델은 전통적인 기계 학습 알고리즘과 달리 도메인 지식을 활용하지 않고 데이터를 학습하여 특징 추출이 이루어지므로 성공적으로 대량의 텍스트 분류에 활용되고 있다. 따라서 트위터 메시지로부터 약물 이상 반응에 해당하는 메시지를 분류하는 작업 역시 딥러닝이 효과적으로 활용될 수 있다. 그러나 딥러닝이 좋은 성능을 발휘하려면 명확하게 분류된 대량의 텍스트가 필요한데, 실제 트위터 메시지 중에서 약물 이상 반응에 대해 언급한 메시지는 턱없이 부족하다. 이러한 트위터 데이터의 제약점을 극복하

고자 준지도 학습 기반 컨볼루션 신경망 모델이 활용되었다.

그림 2는 컨볼루션 신경망을 이용하여 트위터 메시지로부터 약물 이상 반응을 검출하는 방법을 나타낸다[17]. 이 방법은 크게 두 단계로 나뉘는데, 먼저 비지도 학습 단계를 통해서 트위터에서 사용되는 의학 용어, 약물명, 건강 상태 및 약물과 건강상태를 나타내는 구문들을 학습시킨다. 다음으로 학습한 구문 임베딩과 레이블을 갖는 트위터 메시지들을 가지고 약물 이상 반은 탐지 분류기를 위해 다시 학습시킨다. 약물에 관한 메시지, 건강 조건에 관한 메시지, 약물 조건에 관한 메시지 등 다양한 모델을 생성하고 실험을 실시한 결과 전통적인 기계 학습 분류기를 사용한 경우보다 높은 분류 성능을 보였다.

5. 결 론

임상 시험이 갖는 현실적인 제약 사항 때문에 의약품에 대한 시판 후 감시 및 관리는 필수적인 요인이다. 자발적 부작용 보고 제도를 통해서 부작용 자료를 수집하고 분석하여 정보를 제공하고 있으나, 이는 실제 일어나는 부작용 사례에 비해서 매우 작은 수의 보고 자료를 기반으로 한다. 따라서 전자 건강 기록 및 보험 청구 데이터베이스 등과 같이 다양한 목적으로 구축된 데이터베이스들을 빅데이터로 통합하여 보다 유용한 정보를 제공하고자 하는 노력이 이루어지고 있다. 또한 바이오 의약학 전문 서적이나 논문이나 전문가 의견 문서등과 같은 비정형 텍스트를 분석하여 부작용 실마리 정보를 찾는데 도움을 주고자 하는 연구도 활발하다. 보다 최근에는 실시간으로 환자들의 건강 상태를 반영하는 소셜 미디어 데이터를 활용한 디지털 약물 감시도 점차



(그림 2) Semi-Supervised CNN[17]

로 중요성을 더하고 있다.

전통적인 통계적 데이터 마이닝 기법은 정형화된 빅데이터로부터 실마리 정보를 찾는데 널리 활용되어 왔다. 비정형 텍스트 데이터의 경우는 지도 학습 기반의 분류 알고리즘을 이용하여 약물 이상 반응과 관련된 텍스트를 분류하는 연구들이 진행되고 있다. 특히, 트위터와 같은 소셜 미디어의 경우는 전통적인 기계 학습 분류기보다 딥러닝을 활용하는 것이 분류 성능을 향상시킴을 알 수 있다.

현재 빅데이터는 의약학 분야에서 의약품 부작용의 예측 외에도 신약 개발을 위한 후보 물질 선정이나 개인별 맞춤 약물 치료제 개발 등에 활용되고 있다. 이러한 빅데이터 활용 분야 전반에 걸쳐 많은 투자와 연구 및 개발이 필요한 시점이다.

참 고 문 헌

[1] WG. McBride, Thalidomide and congential abnormalities. Lancet, Vol 2, pp. 1358, 1961.

[2] D. Choi, M. Choi, and A. Ko, Current status of pharmaceutial safety management in Korea, J. Korean Med. Assoc. Vol. 55, No. 9, pp. 827-834, 2012.

[3] 한국의약품안전관리원, http://www.drugsafe.or.kr/

[4] NK Choi, J. Lee and BJ Park, Recent international initiatives of drug safety management, J. Korean Med. Assoc. Vol. 55, No. 9, pp. 819-826, 2012.

[5] BJ Park, Application of big data for public health, J. Korean Med. Assoc. Vol. 57, No. 5, pp. 383-385, 2014.

[6] patientslikeme, http://www.patientslikeme.com/

[7] A. Bate and SJ Evans, Quantitative signal detection using spontaneous ADR reporting, Pharmacoepidemiol Drug Saf. Vol. 18, pp. 427-436, 2009.

[8] T. Tamura, T. Sakaeda, K. Kadoyama, et al. Aspirin- and clopidogrel-associated bleeding complications: Data Mining of the public version of the FDA Adverse Event Reporting System, Int. J. Med. Sci, Vol. 9, pp. 441-446, 2012.

[9] K. Sarvnaz et al., Text and Data Mining Techniques in Adverse Drug Reaction Detection, ACM Computing Surveys, Vol. 47, No. 4, pp. 56:1 - 56: 39, 2015.

[10] T. Sakaeda, A. Tamon, K. Kadoyama, and Y. Okuno, Data Mining of the Public Version of the FDA Adverse Event Reporting System, Int. J. of Med. Sci., Vol. 10, pp. 796-803.

[11] H. Kim and KY Rhew, Analysis of Adverse Drug Reaction Reports Using Text Mining, Korean J. Clin. Pharm, Vol. 27, No. 4, pp. 221-227, 2017.

[12] H. Kim and KY Rhew, A Machine Learning Approach to Classification of Case Reports on Adverse Drug Reactions using Text Mining of Expert Opinions, Lecture Notes in Electronic Engineering, Vol. 474, pp. 1072-1077, 2018.

[13] KH Lim, et al, Comparison of WHO-ART Versus MedDRA, Internationally Standardized Terminology of Adverse Drug Reaction Classification, Korean. J. Cli. Pharm. Vol. 17, No. 1, pp. 46-52, 2007.

[14] CC Freifeld, JS Brownstein, CM. Menone, et al., Digital drug safety surveilance: monitoring pharmaceutical products in Twitter, Drug Saf., Vol. 37, No. 5, pp. 343-350, 2014.

[15] A. Sarker and G. Gonzalez, Portable automatic text classification for adverse drug reaction detection via multi-corpus training, Journal of Biomedical Informatics, Vol. 53, pp. 196-207, 2015.

[16] A. Cocos, A. G. Fiks, and A. J. Masino, Deep

learning for pharmacovigilance: recurrent neural network architectures for labeling adverse drug reactions in Twitter posts, J. of the American Medical Inoformatics Association, Vol. 24, No. 4, pp. 813-821, 2017.

[17] K. Lee, et al, Adverse Drug Event Detection in Tweets with Semi-Supervised Convolutional Neural Networks, In Proc. of International World Wide Web Conference, Perth, Australia, pp. 705-714, 2017.

저 자 약 력

김 현 희

이메일 : heekim@dongduk.ac.kr

- 1996년 이화여자대학교 컴퓨터학과 (학사)
- 1998년 이화여자대학교 컴퓨터학과 (석사)
- 2005년 이화여자대학교 컴퓨터학과 (박사)
- 2005년~2006년 LG 전자 디지털 미디어 연구소 / 선임 연구원
- 2006년~현재 동덕여자대학교 정보통계학과 부교수
- 관심분야 : 기계학습, 빅데이터 분석, 의약품 부작용 예측

특집 03

A Study on the Improvement for Military Cyber Protection Technology in the 4th Industrial Revolution

Chulhyun Park · Jingul Kim · Daesol Kim (Korea Army Academy at Youngcheon)

Contents

1. Introduction

1.1 The 4th Industrial Revolution and Defense Cyber Protection System

The core technologies of the 4th Industrial Revolution are known as AI(Artificial Intelligence), IoT(Internet of Things), Big Data, Cloud Computing, 3D printing and Cyber Security. This heralds the era of uncertainties beyond the predictable age based on the Hyper-connectivity & Super-intelligence through the distribution and convergence of global data, and self-evolving technologies. Meanwhile, Ju said that various hacking attacks, resulting from the vulnerability of convergence of these key technologies or newly-developed weaknesses, are taking place throughout the world and will continue to rise in the future. He suggested cyber attack patterns such as Ransomware, the increase in the number of attacks, and the diversification of attack methods. One of the biggest concerns in the age of Hyper-connection is the information security threat such as voluntary and involuntary information leakage. The Ministry of National Defense is also trying to conform to the 4th industrial revolution through Cloud Computing and Big Data, starting with the establishment of Defense Integrated Data Center and the launch of Military IoT(M-IoT). As the intelligence and communication environment is becoming more sophisticated, it has become a movement to build a huge network integrating current command and control systems, wired and wireless communication networks and weapon systems software linked to them. Various information assets that are distributed and operated by organizations and systems will be

integrated into Cloud Computing systems in application, server and information service environment. In addition, applications and information services will evolve into a single sign-on environment, and the network environment will expand and integrate with IP(Internet Protocol) technology. However, as the defense networks expand and become automated, the vulnerabilities and the number of targets that the enemy can attack are increasing. In particular, the hacking attack in August 2016 indicates the vulnerability of current cyber protection technologies, which resulted in an attack on the vulnerability of connections to the network via the antivirus update server between the Internet and the Intranet. Now, in operating the information and communications system, such as a massive chain of defense networks, Cyber Protection Technology also needs to establish a system for mutual monitoring, identifying vulnerabilities and warning. Accordingly, this paper analyzes the factors of the 4th industrial revolution that will be applied to the defense information and communications system in the future and the vulnerable elements that can be caused by them, and presents directions for operating and enhancing the Cyber Protection Technology.

2. Current Status

2.1 Development of Defense Big Data and AI Technology

Big data technology, one of the core technologies of the 4th industrial revolution, is expected to be gradually applied to the military. According to Han and Kang, U.S. military spends more than $ 250,000 a year on Big Data in the defense sector, using it to prepare for the enemy's cyber attacks as well as physical attacks(In addition, they suggest using Big Data to military promotions and CRM(Customer Relationship Management) through SNS analysis, as well as utilizing it to inventory management of military supply items, and to help troubled soldiers). They said the ROK military is also collecting data on North Korean forces and analyzing their patterns precisely to predict and prepare for their military action.

The ROK military is operating the Defense Integrated Data Center in the field of non-weapon systems, which integrating Army, navy and air force service systems into one. It was built on the defense network which is a peace time network in the military. In particular, it has a search function similar to the knowledge portal search function, which is commercially available in the Internet network, and is continuously upgrading functions for database extension and convenience enhancement. In the field of weapon systems, the functions are applied to C4I System (Command, Control, Communications, Computer and Intelligence System) to support commanders' decisions in case of emergency by collecting and analyzing real-time data from each individual soldier to higher units. In other words, after processing the received data into

useful information, it is expected to be automated to derive analysis factors for decision making from given information, and to give priority to them. We also expect that the uncertainty of the battlefield will increase more as the number of cases is generated and the prediction is repeated by analyzing past data to support the current optimal decision-making process. Moreover, military data and information collected at strategic levels, when they are linked with national central agencies, can also support the Chief Executive Officer's decision, which means that a huge amount of data will circulate in and out of the military. However, data to be distributed might include many sensitive data such as personal information and tactical situations, which are directly related to military security issues. Although the military has been preparing security measures using encryption and authentication system for sensitive computer files including military documents, systematic information protection systems such as masking of a large amount of data are not established yet. Futhermore, the military has not established any countermeasures in cases where sensitive information (personal information, confidential information, etc.) is predicted by deliberate tracing methods which work on intentionally excluded sensitive date when information from more than two objects is provided in externally distributed documents, PC files and mobile transmission. In other words, as the decision support system becomes more automated, more information will be circulated, and if a little bit of the sensitive information is exposed, the enemy will be more easily informed of our intention.

2.2 Development of Hyper-Connectivity and IoT Technologies

Hyper-Connectivity in the 4th Industrial Revolution will be applied to support the optimal decision-making by interlinking the core information and communication networks of the military such as the tactical network currently being built, C4I systems, the weapon systems software and the Weapon Systems Embedded Software. It is also believed that the area will include the military IoT(M-IoT) which is currently initiated. We can expect the future tactical communication system to be mutually interlinked as shown in Fig. 1. Shin and Kim suggested that there are many areas in which M-IoT can be introduced such as recruitment training, military barrack, surveillance, reconnaissance, accident prevention, military logistics innovation and military

* W.S.E.S. : Weapon Systems Embedded Software

(Fig. 1) Future tactical communication system

medical system. Among them, it was judged that recruitment training and the improvement of military barracks would be the first. They also predicted that wearable devices for small-scale special forces would be used in the early stages of the military strategy to increase combat capability awareness and combat power by utilizing weapon systems and two-way data systems, and the next stage will be extended to the large-scale battle systems that include C4I systems. The ROK military is extending the scope of M-IoT by launching the Wearable Health Care System using wearable devices, the Logistics Management System, etc. They are also building TICN(Tactical Information Communication Network) composed of complex sub systems such as high-capacity wireless transmission systems, small wireless transmission systems, telecommunications systems, combat radio systems, tactical mobile communication systems and network control systems. As a core tactical network of ROK armed forces, TICN supports communications from a small unit to large troops. It can be utilized for real-time information distribution and optimal command determination in conjunction with the C4I system or the individual battle information system to be deployed in the subsequent IoT format. However, as "Security is a chain of various cyber security capabilities. The overall level of security is determined by the weakest parts of the chain.", vulnerabilities exposed in the weakest parts of the network can be directly targeted to enemy cyber attacks. Attacks and risks against tactical networks are shown in Table 1.

And threats of IoT linked with tactical networks, such as increased threat of the illegal system access and utilization by unauthorized users, increase in the possibility of compromising confidential information and difficulty in verification of accuracy and reliability of information. Also, Weapon Systems Embedded Software that is linked to tactical networks and M-IoT is vulnerable to its

<Table 1> Risk factors for tactical networks

Main attacks		Degree of vulnerability	Effect	Degree of Risk	Counter -measures
Passive	Eavesdrop	Low	High	Low	Cryptography
	Traffic Analysis	High	Low	Medium	Traffic Obfuscation
Active	Dos	Low-High	High	Low-High	Layer Specific Mechanism
	Masquerade	Low	Very High	Medium	Trust System
					Cryptography
	Modification	Low	High	Low	Cryptography
	Jamming	High	High	High	Anti-Jamming
					Cognitive Radio

Common defense methodology : Cryptography, Authentication, Tunneling, Anti-Jamming, Cross-layer Approach, Policy-based Management

own defects and external attack due to insufficient Maintenance Management compared to its importance. In particular, the secure coding is not applied, which can be the most realistic alternative to minimizing infringement caused by its own vulnerability during software development. Threats to Weapon Systems Embedded Software including a total of 59 vulnerable factors have been studied in the categories of software modulation, software implementation, hardware external, hardware terminal, hardware component intrusion, hardware replication, data, visual information, user interface, system access and password implementation. These factors act as links to security vulnerabilities, causing significant damage to allies in case of emergency. An example of this is the failure of a timely interception due to an embedded software defect of an interceptor missile against an enemy ballistic missile attack.

2.3 Human resource training and education

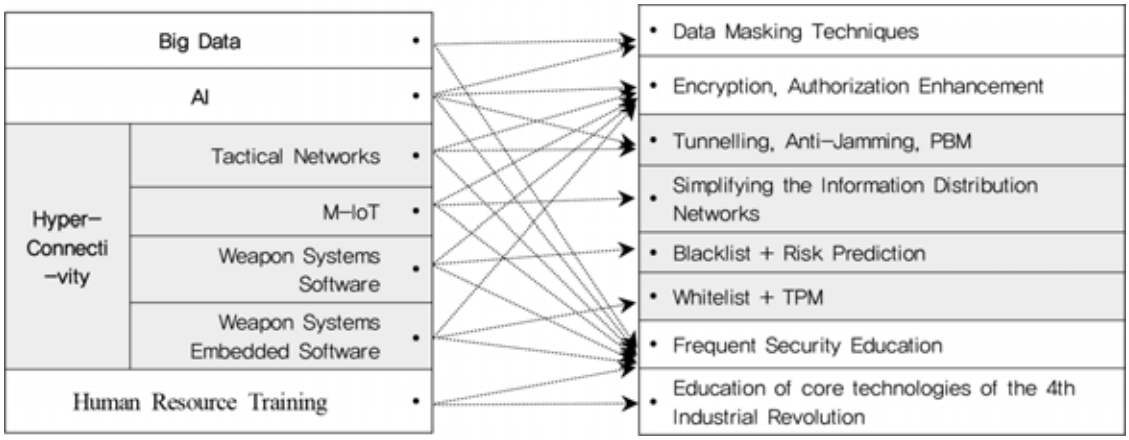
The lack of professional personnel and professional education programs to carry out cyber protection in the military is an ongoing problem. Intermediate technical education for Cyber Warfare or Intelligence Protection is taught at each military Intelligence-Communications School only for commissioned officers who are in the branch of Communications. Seo et al. argued that it is difficult to say that the officers were educated as Cyber Warfare professionals only by completing the education because those schools only provide the level of understanding the concept of Cyber Warfare and Intelligence Protection. Thus, they emphasized the importance of the education in basic education institutes that include universities. On the other hand, Eom argues that cyber security education in S. Korea is mainly centered on basic education institutes, and the intermediate and higher technology education that can improve the cyber security capability is not systematically implemented. That is, cyber protection education should be continuously managed from basic education institutes such as universities, private and public agencies to practical cyber training institutes. Particularly, as the age of the 4th Industrial Revolution comes, for Cyber Warfare experts have to cultivate their ability to deal with Big Data analysis, IoT and artificial intelligence, both the basic and the higher technology curriculum should be strengthened. Eom et al. suggest that Cyber warriors in the defense sector should be differentiated and specialized as compared to Cyber security experts in the private sector, because the Cyber Warfare is conducted in conjunction with physical warfare. They also said that cyber warriors in the defense sector should have specialized expertise and knowledge in defense policies, military strategy, operations, tactics and cyber attack & defense skills.

3. Improvement

We derived cyber protection technologies required during the 4th Industrial Revolution era through several practical discussions and research from January to May 2017, participated by the personnel in charge of Information Planning in each military service and university professors. As a result, the core technology elements of the 4th Industrial Revolution and the required cyber protection technologies were intersected and matched as shown in Figure 2. Details are discussed in the following sections.

3.1 Improvement for Defense Big Data and AI Technology

As described in the previous chapter, for the military's decision-making system is automated and the vulnerability further increases, Park et al. suggested a classification method which can identify and deal with high-risk information using the disclosure risk measure. Data can be categorized into micro data including private data for individuals, households and businesses, and macro data such as division tables or spreadsheets provided to government agencies, academics and research institutes. Especially, the Big Data technology to be applied to the military has to support the commander's determination by distributing and processing real-time (or near real-time) micro data, so we should consider the risk of direct object exposure or deliberate reasoning in the process. Thus, we need to classify and manage the data in accordance with exposure risk in case the sensitive information is inferred by acquiring part of the data using social engineering techniques. The higher the risk of exposure, the more protective measures should be taken before providing information to the outside. In this regard, data protection techniques such as anonymization, sample provisioning, population size restriction, concealment, data exchange, noise addition, blurring, Micro-Aggregation and



(Fig. 2) Operation Strategy for Cyber Protection Technology

etc. have been studied. Some public institutions have applied these technologies to protect sensitive information. However, since the ROK military does not apply protection technologies as well as techniques for measuring exposure risk, it is urgent to take measures against them.

3.2 Improvement for Hyper-Connectivity and IoT Technologies

Table 1 shows Cryptography, Authentication, Tunneling, Anti-jamming, and Policy-based management (PBM) as countermeasures against tactical network threats. Shin and Kim proposed strengthening of cryptography and authentication, and simplification of information distribution network as security countermeasures against M-IoT. On the common defense methodology, these are all universal and essential security elements. Advances in the 4th Industrial Revolution have been developed by artificial intelligence systems, which automatically identifies the threat of unknown threats, but the ROK military hasn't introduced them, so the military has to rely on a lot on security system operators for the next several years. Therefore, it is very important to educate the people who operate security systems because it is known as 'the greatest enemy of security is human beings'. In other words, we have to constantly check that the security measures to be operated are in operation, and to continue to educate on the latest updates for malware information, up-to-date security patches and enhanced personnel security against social engineering attacks. In order to improve the defense cyber protection, we need to build a system to detect and block cyber threats and to monitor threat situation, abnormal status and log information throughout the system and network by adding to current integrated security control system. And the system should support identification of unknown cyber threats through comprehensive analysis using Big Data technologies. Unknown threats target both tactical networks, C4I systems, and Weapon Systems Embedded Software, so protection schemes are needed for their own characteristics. Park et al. introduced the Whitelist + TPM (Trusted Platform Module) Solution as a countermeasure against weakness of the Weapon Systems Embedded Software. Weapon Systems Embedded Software has the characteristics of being limited to specific areas of work, closed or stand-alone format and low specification in comparison to other weapon systems software, so Whitelist techniques that block unknown threats can be applied. Since the typical weapon systems software has a wider operating range than Weapon systems embedded software, Blacklist technique is applied to them rather than Whitelist technique to cope with relatively known malicious code. In this case, we need to constantly predict unknown malicious code by frequent updates and the Big Data technologies. In contrast, the Weapon Systems Embedded Software is relatively small in scope, so it is effective to apply a method that blocks all but the specific allowed executable files. Moreover,

the Weapon Systems Embedded software can strengthen security by intelligently filtering malicious code at the hardware level before access control through the Whitelist. Using such techniques, we can cope with physical attacks such as hardware terminals, component intrusion and duplication. In this regard, Park et al. introduced the application of Trusted Platform Module (TPM) which is a chip type module that can block unknown attacks such as Zero-Day Attack at the hardware level. It can function as a reliable computing platform for storing cryptographic keys or passwords in nonvolatile space and providing access to storage space, integrity verification of remote hosts, reliability based communication, and providing secure communication channels. Consequently, the Weapon Systems Embedded Software can use TPM at the hardware level to ensure integrity and then apply the whitelist at the software level to enhance protection. Figure 3 shows a application of Whitelist + TPM solutions to Weapon Systems Embedded Software.

(Fig. 3) Application of Whitelist + TPM Solutions to Weapon Systems Embedded Software

3.3 Improvement for Human Resource Training and Education

Seo et al. analyzed basic fundamentals for training a Cyber Warfare expert as shown in Table 2. The analysis results show that the weight of 'Firm view of the nation' is higher than that of the Programming technique and the Basic knowledge of information security. In order to cultivate a firm view of the nation, we need to emphasize the recognition of the reality of the nation's military and the importance of cyber warfare in national security. To this end, we have to continue to educate the latest version of cyber threats and cases first in order to ensure that the students understand the international situation and the changes in cyber warfare. Second, education on cyber warfare as a part of war should be strengthened. That is, the operational training of cyber warfare at the strategic level should mainly contain a comparative analysis of competence among major countries, the use of cyber psychological warfare in war, the countermeasures against cyber attacks and related statutes (such as Tallinn Manual).

Third, cyber operations training should be strengthened, namely Cyber Attack & Defensive Operations and Network Operations. We have to train students to equip themselves with basic skills to use tactics as soldiers because war is a strategic aspect, but military operations are operational and tactical. Degree courses in Cyber warfare mainly deal with computer architectures, operating systems,

<Table 2> Basic Fundamentals for Cyber Warfare experts

( ) : Weight value

1st layer(Civil, Military)	2st layer(Civil, Military)
Sense of duty (0.344, 0.376)	Firm view of the nation (0.514, 0.419)
	Ethics (0.281, 0.299)
	Challenge spirit (0.205, 0.282)
Planning Capacity (0.287, 0.213)	Programming (0.495, 0.535)
	Document Writing (0.194, 0.184)
	Basic knowledge of information security (0.312, 0.281)
Internationality (0.200, 0.211)	Global cultural awareness (0.506, 0.506)
	Foreign language ability (0.494, 0.494)
Leadership (0.169, 0.199)	Insight and judgment (0.461, 0.488)
	Cooperation (0.300, 0.189)
	Driving force (0.239, 0.323)

programming languages, information protection, digital forensics, system and web security and cyber battle exercises, which are related to technical aspects (programming, basic knowledge of information security and etc.).

Particularly, in the case of the cyber battle exercise, it is necessary to construct a training facility capable of both attack and defense, but is mainly focused on defense. Eom et al. emphasized that defense cyber warriors should conduct training in cyber training facility optimized for specific cyber domains. This is because defense related information and communication systems are constructed in various ways, such as production and transmission of national security related defense documents, communication of military confidential data, collection of key information, analysis and dissemination of information. In addition, Big Data, IoT and artificial intelligence programs should be added to both basic and upper middle class curriculum in order to meet the 4th Industrial Revolution era. For example, the basic curriculum needs to reinforce basic statistics and data analysis to deal with Big Data, and network programming and network security for the IoT. And higher education institutions such as Information-Communications Schools should supplement the process to be immediately applicable to higher-level practices than basic curricula, such as Big data analysis using toolkits, intermediate network programming and security. In order to broaden the experiences of students, we need to set up opportunities to actively participate in the Korea Information Technology Research Institute (KITRI) 's Next Generation Security Leader Course (BoB : Best of the Best), Hacking Defense Competition, etc.

4. Conclusion

Currently, S. Korea is entering the era of the 4th Industrial Revolution beyond the level of computerization and automation based on the National Informatization. Some of the technologies of the 4th Industrial Revolution are already expanding to the base of our society beyond the R&D stage, so the ROK military can not be an exception. The Ministry of National Defence is planning to build the optimal decision-making system which based on the integration of tactical networks, C4I systems, M-IoTs and the establishment of the Integrated Data Center, using the key technologies such as Big Data, Artificial Intelligence and IoT. However, as the network which implementing Hyper-connectivity & Super-Intelligence expands and becomes automated, the security vulnerabilities that can cause major disruptions to the network are increasing, which highlights the importance of cyber protection in the 4th Industry. As a result, we suggest the data masking techniques for Artificial Intelligence, and encryption techniques, enhancement of authentications, tunneling, Anti-jamming and PBM for tactical networks, encryption techniques, enhancement of authentications and simplifying the information distribution networks for M-IoTs, the Blacklist techniques + Risk Prediction technology for weapons systems software and the Whitelist techniques + TPM for Weapon Systems Embedded Software. We also provide the necessary security education for the security system operators. Additionally, as the necessary preconditions for applying these technologies, we have indicated the need for enhancing the core technical training of the 4th Industrial Revolution to improve both basic and practical skills required for the cyber warfare experts.

The expansion of the 4th Industrial Revolution makes our daily lives more convenient, but targets in the cyber space that can be attacked by North Korea are increasing. Therefore, through this study, we hope the ROK military will be interested in the proper functioning of cyber protection technology and continue to improve it. We will also investigate what should be supplemented and improved when the cyber protection technologies proposed in this paper are actually applied.

참 고 문 헌

[1] Ju, D., What should we do for 4th Industrial Revolution and National Cyber Security?, The 4th Industrial Revolution and the National Cyber Security Policy Forum, Presidential Commission on Broadcasting and Communications / National Cyber Security Association, S. Korea, Keynote presentation, 2017.

[2] Cho, S., The Study on Threats of Information Security and Their Solutions in the Fourth Industrial Revolution, Korean security science review, Vol.51, pp.11-35, 2017.

[3] Choi. I., Defense cyber protection development direction, Weekly defense review, KIDA, S. Korea, Vol.1659, pp.1-8, 2017.

[4] Han, C. and Kang, W., The Utilization of Big Data Technologies in the ROK Army, Journal of Business Administration Research, S. Korea, Vol.9, No.1, pp.5-24, 2016.
[5] Shin, S. and Kim, Y., A Study on the Cyber Cyber-Construction and Countermeasures by Introducing IoT, KINX2016257139, ROK. Joint Chiefs of Staff, S. Korea, pp.81-84, 2016.
[6] Ha, Y., Chung, Y., Lim, Y. and Yang, H., A Study on the Development of UAVs for the Public Switched Information System in Korea, KICS, S. Korea, Proceedings of the Summer Conference, 2009.
[7] Schneier, B., Secrets & Lies, John Wiley& Sons, 2000.
[8] Ross, R. S., Managing Information Security Risk: Organization, Mission, and Information System View, Special Publication (NIST SP), 800-39, Mar. 2011.
[9] Kidston, D., Li, L., Tang, H. and Mason, P., Mitigating Security Threats in Tactical Networks, Communications Research Centre (CRC), White Paper, 2010.
[10] Park, C., An, H., Kim, S. and Bae, J., Strategies to Improve the Management System of Weapon Systems Embedded SW and to Construct its Information Security System, Journal of Security Engineering, SERSC, S. Korea, Vol.12, No.4, pp.363-378, 2015.
[11] S. Korea's Defense Acquisition Program Administration, A Handbook on the Development and Management for Weapon Systems SW, 2013.
[12] Seo, S., Oh, W. and Kim, H., Research on cyber warfare manpower training strategy for securing Defense Information System using AHP analysis, Journal of Security Engineering, SERSC, S. Korea, Vol.12, No.2, pp.109-120, 2015.
[13] Eom, J., The Improvement Plan of a Customized Cyber-Training Structure for enhancing the Capability of Cyber Security, Journal of Security Engineering, SERSC, S. Korea, Vol.12, No.6, pp.567-580, 2015.
[14] Eom, J., Lee, W. and Park, K., A Construction Plan of Specialized Cyber Training Scheme for Enhancing the Capability of Military Cyber Warriors, Journal of Security Engineering, SERSC, S. Korea, Vol.13, No.2, pp.99-112, 2016.
[15] Park, C., Kim, C., Kim, S., An, H. and Bae, J., Improvement of Personal Information Protection Level in the Military Using the Measurement of Disclosure Risk, Journal of Security Engineering, SERSC, S. Korea, Vol.12, No.6, pp.581-596, 2015.
[16] Eurostat, Manual on Disclosure Control Methods, Luxembourg, Office for Official Publication of the European Communities, 1996.
[17] Techtarget Network, http://whatis.techtarget.com/definition/policy-based-management, 2011.
[18] Network Times, Whitelist Security, 153-162, 2010.
[19] Choi, J., Park, W. and Park, C., A Framework of Secure Access to iSCSI Network Storage based on TPM, KCC2009, Vol.36, No.1D, pp.5-9, 2009.

저 자 약 력

박 철 현

이메일 : kmanp@cnu.ac.kr

- 1999년 육군사관학교 물리학 (학사)
- 2003년 국방대학교 무기체계학 (석사)
- 2016년 충남대학교 수학통계학 (박사)
- 2016년~현재 육군3사관학교 컴퓨터공학/사이버전학과 조교수
- 관심분야 : 큐잉이론, 시뮬레이션, 소프트웨어공학, 사이버전 등

김 진 걸

이메일 : c15247@gmail.com

- 2007년 육군사관학교 전산학 (학사)
- 2015년 미 USC 컴퓨터공학 (석사)
- 2015년~현재 육군3사관학교 컴퓨터공학/사이버전학과 강사
- 관심분야 : 시스템/네트워크 보안, 운영체제, 사이버전 등

김 대 솔

이메일 : a1088342256@gmail.com

- 2010년 육군사관학교 프랑스어학 (학사)
- 2016년 프랑스 ISEP 정보공학 (석사)
- 2016년~현재 육군3사관학교 컴퓨터공학/사이버전학과 강사
- 관심분야 : 데이터마이닝, 보안모델링, 사이버전 등

KIPS 권두언

‘ICT 융합’ 특집호를 발간하며...

본 특집에서는 양식장과 전력 산업에 ICT 기술을 접목한 사례와 이때 사용한 ICT 융합 기술을 다루고 있습니다. 또한, ICT 융합 분야에서 가장 중요하게 인식되고 있는 보안/암호 분야의 최신 동향인 양자내성암호(Post-Quantum Cryptography)도 다뤘습니다.

최근 디지털 변혁(Digital Transformation)과 4차 산업혁명이라는 용어가 많이 회자되고 있으며, 이러한 변화의 기조에는 지금까지 우리 주변에서 쉽게 듣던 ICBMS(IoT, Cloud, Big Dat a, Mobile, Security)-AI, 블록체인과 같은 신기술이 있다는 것을 우리는 잘 알고 있습니다. 또한, 이러한 기술은 2000년대 초, 많은 관심을 받은 유비쿼터스 기술, 그리고 그 이후에 정부 주도하에 이뤄졌던 IT-839 전략과 IT 융합 정책 등과도 그 괘를 같이 한다고 볼 수 있습니다. 이러한 정부 주도하에 신기술을 개발하고 우리 사회와 산업, 생활을 변화시켜려던 정책은 그 동안 미흡한 적도 있었지만 방향성은 옳았다고 생각하며 나름 많은 성과를 이뤘다고 생각하고 있습니다.

최근의 4차 산업혁명을 위한 노력은 혁신과 산업 발전이라는 측면에서 보면 이전에 비해 미흡한 부분이 많지만, 국민 생활 개선을 강조한다는 관점은 잘못된 방향이라고 볼 수는 없을 것 같습니다. 하지만, 급변하는 변화를 선도하거나 효율적으로 대응하지는 못한다는 생각은 떨쳐버릴 수가 없습니다. 본 고에서는 현재와 같은 급변하는 기술 세상에서 학계와 산업체가 수산 양식업과 전력 산업, 그리고 미래 암호 분야에서 어떻게 대응하고 있는지를 볼 수 있으며, 변화를 선도하기 위해 어떤 기술적인 부분을 고려해야하는지를 알 수 있을 것입니다.

우선 첫 번째 원고에서는 부산외국어 대학교의 신규재 교수 연구실에서 지역적인 수요(양식업)에 첨단 사물인터넷 기술을 접목시킨 좋은 사례를 보여주고 있습니다. 양식업은 적절한 산소 공급과 수질 유지, 그리고 이에 사용되는 전력 사용량 절감이 중요한 요소인데, 이를 사물인터넷 기술과 구조역학 기술을 사용한 사례를 보여주고 있습니다. 두 번째 원고는 한전 전력연구원에서 기고한 논문으로서, 국가 산업의 근간인 전력 산업에서 송배전 자동화/지능화 사례와 IoT 기술 적용 동향, AMI 기술에 대해 전체적으로 다루고 있습니다. 우리나라의 송배전 관리 기술은 세계적으로도 우위에 있다고 알려져 있는데, 이러한 최신 기술을 접목하고자 하는 자동화/지능화 노력은 더욱더 높은 경쟁력을 가져올 것으로 보입니다. 또한, 마지막 원고에서는 양자컴퓨터 시대에는 기존 암호 체계가 심각한 취약성 문제에 직면하게 되는데, 이러한 양자컴퓨터 시대에 적합한 양자내성 암호의 최신 동향을 살펴볼 수 있습니다. 암호/보안 기술은 산업과 우리 사회에 지대한 영향을 주는 분야이므로 해당 동향을 반드시 알고 있어야 할 부분입니다.

본 특집호를 위해 원고 집필을 수락해 주시고 원고를 작성해주신 모든 저자 분들께 감사의 말씀을 드리며 함께 참여해주신 위원장님을 비롯한 편집위원님들과 한국정보처리학회에 진심으로 감사의 말씀을 드립니다. 또한, 본 특집호에 실린 논문을 읽는 독자에게 도움이 되었으면 하는 말씀으로 마무리하고자 합니다.

2017년 11월

부산대학교 사물인터넷 연구센터장 김 호 원

특집 01

수직 적층형 구조를 이용한 IoT기반 스마트 양식장의 산업화모델 개발

김병준·신규재 (부산외국어대학교)

목 차

1. 서 론

최근 제4차 산업혁명의 일환으로 세계적으로 스마트 양식장에 대한 연구개발이 활발히 이루어지고 있다. 노르웨이와 덴마크 등의 북유럽 국가를 중심으로 참치, 다랑어 등의 연근해 스마트 양식장 산업이 급속하게 성장하고 있으며, 육상에서는 동남아 국가를 중심으로 민물 양식어종을 중심으로 강가 또는 해변에서 스마트 양식이 발전하고 있는 실정이다. 양식장의 운영은 매우 힘든 3D업종으로써 산업적으로 많은 노동력을 요구하고 있고 환경에 변화에 따른 수질상태는 한순간에 양식어에 큰 피해를 줄 수 있기 때문에 순환여과방식을 이용한 정밀한 수질제어가 필요하다. 또한 여름과 겨울철에는 수온변화에 따른 양식어 폐사하는 문제가 발생하고 있는 실정이다[1].

전력 발전사들은 해안을 중심으로 운영되고 있는데, 이는 발전하는 과정에서 회전기기 터빈과 발전기 열을 냉각시키기 위해 해수를 사용한 후, 발생한 온배수는 해안으로 방출되고 있다. 양식장에는 수온관리를 하는데 큰 비용이 발생하기 때문에 수열에너지를 공급하는데는 경제적으로 매우 중요하다. 따라서 효율적인 스마트 양식장을 운용하기 위해서는 발전소에서 폐수로 방출되는 온배수 에너지원을 재생에너지로 활용하여 이 열을 저장하고 양식수조에 공급하는 온배수 히트펌프의 수온 제어시스템과 양식수조의 최적화 설계를 위하여 새로운 형태의 육상수조 양식구조와 수질과 수온을 제어하는 IoT(Internet of Things)기반의 스마트 양식장이 필요하다. 본 연구에서는 이러한 문제를 해결하기 위하여 발전소 온배수 에너지를 활용하고 구조물은 수직형 구조를 가지는 아파트 형태의 스마트 양식장 개발을 목표로 하고 있으며, IoT기반으로 온배수

를 공급하는 히트펌프 제어시스템과 양식수조의 수질과 수온센서를 탑재하고 최적의 생육환경을 제어하는 스마트 양식제어시스템을 설계한다. 또한 스마트 양식장의 최적화 설계 및 운용자의 편의를 제공하기 위한 목적으로 원격모니터링과 원격제어를 기능을 설계하였다. 히트펌프와 스마트 양식장 수조의 데이터 모니터링하기 위해 안드로이드 모바일 응용 프로그램과 웹 응용 프로그램을 제작하였고, 양식수조의 환경제어를 위한 마이컴 제어반과 운용 프로그램을 개발하였다. 특히 스마트 양식장의 무인자동화를 위해서 센서 네트워크을 구성하였고 전동 밸브를 자체 개발하여 웹 또는 모바일을 활용하여 원격 제어로 수질상태를 제어할 수 있도록 설계 제작하였다[2,3].

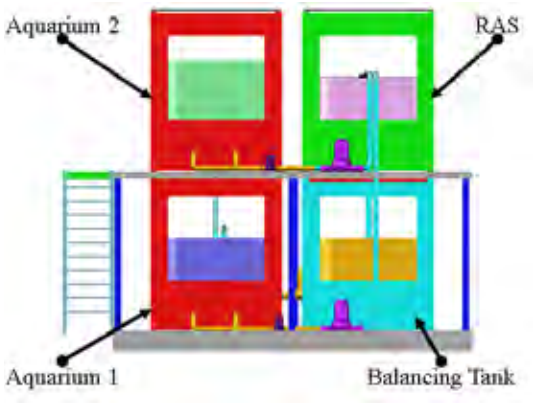
제안된 스마트 양식장은 2015년 8월부터 2017년 10월까지 부산에 위치한 한국남부발전과 부산외국어대학에 IoT기반의 플랫폼을 구축하고 히트펌프 설계 및 성능시험평가와 스마트 빌딩 양식장의 설계, 제작 및 성능시험에 연구가 진행되었다[4]. 실험결과, 온배수 에너지를 활용한 스마트 양식장의 경제성이 분석되었고 설계 제작된 히트펌프의 열량제어장치와 스마트 양식장의 수온 및 수질제어 시스템의 우수한 성능을 검증하였다. 추후 본연구는 우리나라 연근해 및 육상양식의 수산양식에 대한 첨단화에 기여하고 해산물 유통산업과 치어 및 열대어 양식에 큰 기여할 것으로 기대된다.

2. IoT 기반 스마트 양식 시스템 설계

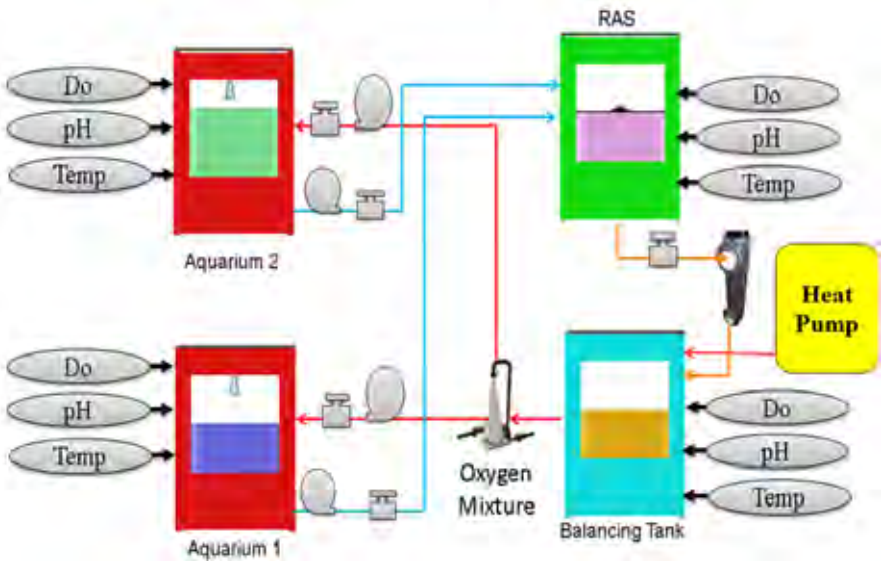
2.1 스마트 양식장 설계

스마트 뱀장어 양식 시스템의 구조는 그림 1과 같이 4개 수조 형태의 IoT 기반 스마트 양식장을 설계한다. 양식어를 사육하는 1층 양식수조(Aquarium 1)와 2층 양식수조(Aquarium 2), 양식수조의 오염된 고형물을 제거하기 위한 순환여과장치(RAS)와 여과된 물을 저장하고 수온과 산소를 공급하여 최상의 수질을 생성하는 밸런싱 수조(Balancing Tank)로 구성된다. 컨테이너 내부에 수조를 설치하는 구조로써, 그림1과 같이 수직과 수평의 적층이 용이한 모듈형 구조로 양식장 설치가 편리한 장점을 갖는다. 각 수조에는 수위 및 수질을 계측하는 초음파센서, 온도, 용존산소(DO) 및 pH 센서와 센서신호 컨디셔너가 설치된다. 이러한 양식시스템은 도심과 건축물 내부에 설치가 용이하며, 특히 산간벽지, 사막, 초극지 등의 같은 극한 환경에서도 그 용도에 따라 자연현장 맞춤형으로 설치가 가능하다.

그림2는 IoT기반 스마트 양식장의 센서, 온배수 에너지와 산소 공급시스템 구성을 나타내며, 원격제어 및 모니터링을 위하여 전동식 전자밸브와 센서 신호컨디셔너 및 마이컴 제어반이 설계되었다. 스마트 양식장의 양식어종은 민물 뱀장어이며, 스마트 양식장의 제어대상은 수량(수조의 물 높이), 수온, 용존산소량(DO)과 pH이다. 또한 수조 내에 외부대기 산소와 유속을 생성하여 뱀장어



(그림 1) IoT 기반 스마트 양식장 설계



(그림 2) IoT기반 스마트 양식장의 센서, 온배수에너지와 산소 공급시스템 구성

의 운동과 산소공급을 목적으로 벤츄리를 사용함으로써 최적화된 생육환경을 제공한다. 양식장의 최대비용이 발생하는 수온관리비의 저감을 위하여 발전소에서 터빈과 발전기의 냉각과정에서 생성되는 온배수를 48[USRT] 히트펌프를 이용하여 온배수 열에너지를 저장하고 열교환기를 통하여 양식수조에 온수 에너지원을 공급한다[2].

뱀장어를 생육하는 과정에서 먹이를 공급하고 남은 먹이와 밤장어 배출물에 의해서 수질을 악화시키는 고형물이 발생하게 된다. 이는 수질을 오염시키는 주요물질로 고형물을 제거하는 것은 양식장에서 매우 중요한 프로세서로써 이를 제거하기 위한 목적으로 순화여과시스템(Recirculating Aquaculture System; RAS)을 설계하였다. 최적의 수질을 관리하기 위해서는 물이 정체됨이 없이 일정한 유속으로 각 수조에 물이 순환되는 것이 필요하다. 이를 위하여 밸런싱 탱크(Balancing Tank)에서 최적상태의 온도, 산소, pH를 생성하고 전자밸브를 이용하여 수조1과 수조2에 수량을 제어하게 된다. 수조1과 수조2에 유입된 물은 뱀장어가 생육하는데 최적의 물을 유지하고 물 정화를 위하여 순환여과수조로 유출된다. 순화여과시스템(RAS)은 3단계 정화를 거치게 되는데 1단계로 오염수를 물리적으로 여과하는 프로세스와 2단계와 3단계에서는 알갱이 크기가 다른 바이오 모래를 이용하여 수조 내에 서식하는 박테리아를 이용하여 생물학적인 여과를 수행한다. 4단계로는 필터재를 활용하여 2층 순환여과수조에서 1층 밸런싱 탱크으로 위치에너지를 이용하여 물을 여과작업을 수행한다. 이러한 순환여과작업은 마이컴 제어반에서 자동수행되어 자체 설계한 전자밸브와 펌프에 의하여 지속적으로 수행된다[3].

효율적인 에너지관리를 위하여 발전소의 온배수의 48[USRT] 히트펌프를 표 1과 같이 설계하였다. 하계와 동계의 수온관리를 위하여 이원 사이클 방식을 적용한 히트펌프를 활용하여 하계에는 냉각, 동계에는 난방하는 기능으로 냉온수를 제어하게 된다. 히트펌프는 압축기, 응축기,

<표 1> 설계된 온배수 히트펌프 설계사양

항목	단위	수치
용량	USRT	48.15
소비전력	Kw/RT	2.89
순환수량	LPM	57.78
난방수량	Kcal/H	145,600
성능계수	COP	6.8

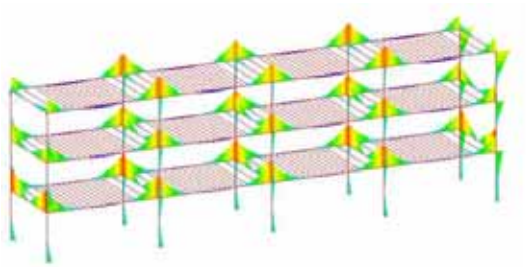
팽창, 증발밸브로 구성되며, 설계사양은 용량 48.15[USRT], 소비전력 2.89[KW/RT], 순환수량 57.78[LPM], 난방수량 145,600[Kcal/H], 성능계수(COP) 6.8이다.

3. 수직 적층형 스마트 양식장의 구조물 해석

설계된 수직 적측형태의 스마트 양식장 구조물의 안정성에 대한 구조물 해석을 수행하여 태풍과 지진등의 외부적 요인에 의한 안정성 평가를 수행하였고 또한 최적의 수질제어를 위하여 수조1과 수조2에서 물이 유출되는 과정에서 설계된 배수가 용이한 바닥면 구조물에 대한 고용물 제거현상을 유동해석을 통해 분석 하였다[5,6].

3.1 수직 적측형 스마트 양식장의 구조해석

스마트 양식장의 구조는 공간 면적당 양식 밀집도를 향상하기 위하여 그림3과 같이 컨테이너를 수직방향과 수평방향으로 적층하는 아파트 형태의 구조물로 양식장을 설계한다. 구조물의 안정성을 평가모델로써 3×4배열의 구조물을 구성하여 구조물의 해석한 결과는 그림 3과 같다. 이때 표 2와 표 3과 같은 설계사양 조건을 으로



(그림 3) 작동, 풍하중, 모멘트 구조해석 결과

작동하중, 풍하중, 포락 모멘트, 전단 모멘트와 같은 다양한 하중과 모멘트에 대한 해석을 수행하였다.

구조물 분석을 위하여 ANSYS Software를 사용하였고 분석 대상 수조는 그림3과 같이 3층 12개 수조로 구성되어 있으며 수조와 수조안에는 물과 뱀장어가 포함된 지속적인 부하조건을 고려하였다. 외부 환경은 좌우로는 벽으로 막혀 있고 앞뒤로는 개방되어 있는 조건하에 해석을 하였다. 시뮬레이션 결과로 하중, 풍압, 진동 시험을 분석 하였으며, 10개의 기둥 빔과 12개의 상판 부분의 연결된 구조물 조건으로 구조물 분석이 수행된다. 시물레이션 결과, 모서리(붉은색) 부분에서 가장 강한 힘을 받는 부위이며 하중을 견디기에 좋지 않은 부분이다. 제안된 구조물은 기둥과 상판이 결합되는 부분에 힘을 분산 시킬 수 있도록 기둥 빔과 결합체를 보강하여 설계하였다. 따라서 수직, 수평 변위를 고려하여 해석결과, 설계 강도, 하중, 풍하중, 모멘트가 설계사

<표 2> 양식장 구조물의 재료조건

Condition	Strength $[N/mm^2]$	Material condition
concrete	$fck = 21$	Compression Strength
steel	$fy = 400$	KSD3504, SD40
steel frame	$fy = 235$	SS400
anchor bolt	$fy = 235$	KSB1002

<표 3> 양식수조 구조물의 부하 조건

Condition	Load [Kg]	Combined load [Kg]
container	6,750	D + L = 55,750
water	30,000	
tank & support	15,000	1.2D + 1.6L = 68,500
Dead Load(D)	51,750	
Live Load(L)	4,000	

양에 만족하는 결과로 구조물의 안정성이 검증되었다.

3.2 양식수조 고형물제거의 유동해석

스마트 양식장의 유동해석으로 각 수조의 유동을 분석하고 고형물이 수조에서 제거되는 상태 및 시간을 확인 하였다. 초기 해석 조건은 각 수조의 물은 전체 용량 대비 약 50%의 물이 채워진 상태에서 유동장을 생성 하였다. 특히, 순환여과시스템(RAS)은 필터 형상이 매우 조밀하여 ANSYS CFX 프로그램상의 수치기법을 다공성 매체 기술을 사용하여 단순화된 모델을 적용하였다.

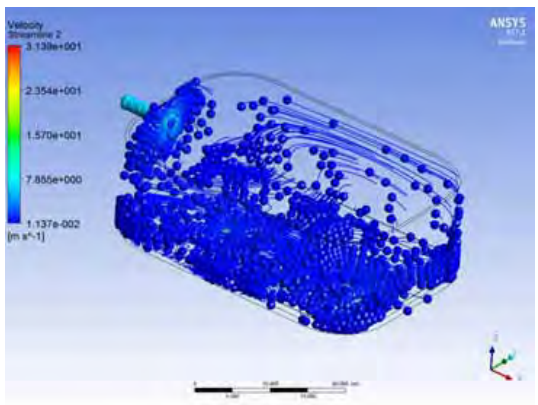
$$\frac{-dp}{dx_i} = \frac{\mu}{K_{perm}} U_i + K_{loss} \frac{\rho}{2} |\cup| U_i \qquad (1)$$

식 (1)과 같이 외력을 제외한 손실 계수를 적용하고 양식 수조의 유동해석을 위한 경계조건은 표 4와 같다. 분석 모델의 격자는 Hexa, Tetra Mesh와 벽면에 경계층 흐름을 고려하여 Prism 사용하여 1,340,589노드를 생성하고, 입구와 출구 유량은 1.25[L/sec], 난류모델은 SST모델, 작동유체는 다상 유체모델의 공기, 물을 적용시켜 정상상태 해석을 하였다.

<표 4> 양식수조의 유동해석을 위한 시뮬레이션 경계 조건

Boundary condition	Value
Mass flow[L/sec]	1.25
Turbulence model	SST
Woking fluid	Air, water
Analysis	Steady state
Node[point]	1,340,589
Element	4,266,471

제안된 양식수조의 구조물 분석결과, 1층 수조와 2층 수조의 최고 유속 0.15[m/s], 최저 유속 0.01[m/s], 최대 압력 1,700[Pa]은 이었고, 1층 수조의 유선은 비대칭, 2층 수조의 유선은 대칭적인 유동 흐름 패턴을 보여 주었으며, 그림 4와 같이 재순환 구역 및 저속 구역에서의 고형물의 이동방향 추적을 통하여 고형물의 제거상태 및 시간을 분석한 결과, 수조 유출구로 고형물이 순조롭게 이동을 하고 고형물이 완전 제거되는 시간은 30분이 소요됨으로써 고형물 제거가 용이함을 확인하였다.



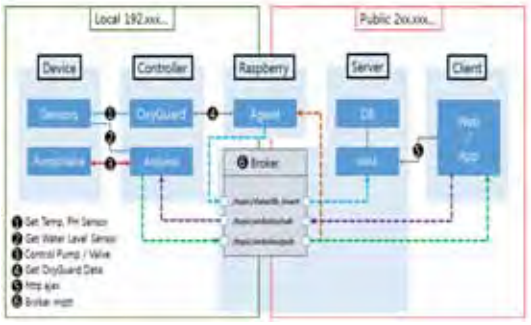
(그림 4) 양식수조의 고형물 제거 성능 시뮬레이션 결과

4. IoT 기반 원격제어 및 모니터링

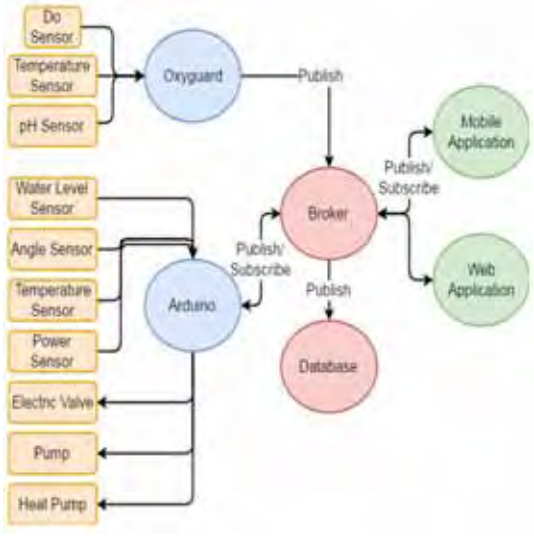
IoT기반의 스마트 양식장은 그림5와 같이 Loacal 양식장과 Public 원격제어 및 모니터링으로 구분된다. 스마트 양식장의 무인자동화를 위하여 수조의 수위를 계측하기 위한 초음파센서, 수질상태를 계측하기 위한 온도, DO, pH 센서를 각 수조에 설치하였다. 이 센서 신호는 OxyGuard의 센서 신호 컨디셔너를 통하여 아듀이노 마이컴 제어반에 전송되며 자체 개발한 Smart Fisherman 운용프로그램에 의하여 각 수조에 설치된 펌프와 전자밸브를 이용하여 유량제어를 구현한다. 아듀이노를 이용한 마이컴 제어반은 DIO 입출력 포트, ADC(Analog to Digital Converter), 릴레이가 구성되어 펌프, 전자밸브를 이용하여 유량제어를 수행한다[5]. 또한 원격제어 및 모니터링을 수행하기 위하여 Raspberry PI를 적용하고 MQTT 프로토콜을 이용하여 Broker와 웹 또는 모바일 앱과 연동된다. 브로커는 옥시가드 센서에서 라즈베리 파이로 센서 데이터를 받아 서버로 전송되고 클라이언트에서 원격제어와 모니터링을 수행하게 된다[7,8].

MQTT는 M2M(Machine-to-Machine)/IoT 연결 프로토콜이며 기존의 HTTP보다 빠르게 데이터 처리가 가능하고 작은 용량의 코드로 큰 대역폭의 원격제어가 가능하다[9][10]. 그리고 통신 데이터 크기는 2byte가 필요하고 1:1통신. 1:n, 1:0과 같은 통신이 가능하여 매우 안전한 통신 방식으로 데이터를 처리 한다.

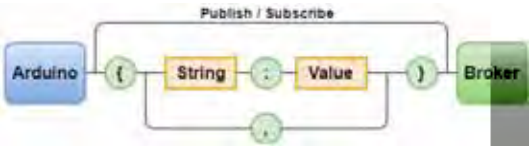
MQTT의 아키텍처는 그림 6과 같으며, Local 제어반인 아두이노는 밸브, 펌프, 히트펌프를 정확하게 제어한다. 전자밸브가 회전할 때 포테셔미터로 오차 각도를 측정함으로써 유량제어가 가능하며, 안드로이드, IOS의 모바일 폰 앱과 웹 상에서의 원격제어와 모니터링이 가능하다. 스마트 양식장의 컨트롤러는 수위, 각도, 센서 데이터를 서버로 일정한 시간 간격으로 읽고 보낸다. 데이터의 전송 효율을 높이기 위해 JSON을 사용하여 데이터 전송을 그림 7과 같이 웹과 모바일에 일반 표준 데이터 값을 전송하게 된다. 제안된 스마트 양식 시스템은 실시간으로 웹 사이트 및 모바일 폰 어플리케이션에서 전자밸브를 이용하여 원격제어를 할 수 있고, 계측 데이터를 모니터링 할 수 있고 이와 관련된 제어정보와 계



(그림 5) 스마트 양식장 제어 데이터 흐름도



(그림 6) IoT기반 자동화 기기의 MQTT 아키텍처



(그림 7) 아두이노와 브로커의 JSON 데이터 통신

측 데이터는 일자별로 저장관리 할 수 있다 [11][12].

5. 실험결과

제안된 IoT기반 스마트 양식장은 발전소 온배수 에너지를 활용하고 구조물은 수직형 구조를 가지는 아파트 형태로 그림 8과 표 5와 같이 스마트 양식장의 산업화 모델을 개발하였고, IoT 기반으로 온배수를 공급하는 히트펌프 제어시스템과 양식수조의 수질과 수온센서를 탑재하고 최적의 생육환경을 제어하는 스마트 양식제어시스템을 설계하였다.

본 산업화 모델의 연구개발은 2015년 8월부터 2017년 10월까지 부산에 위치한 한국남부발전에서 IoT기반의 수직 적측형 스마트 양식장 플랫폼을 그림8과 같이 구축하고 히트펌프 설계 및 성능시험평가와 스마트 빌딩 양식장의 설계, 제작 및 성능시험에 연구가 진행되었다. 스마트 양

(그림 8) 설계·제작된 IoT기반의 스마트 양식장 플랜트

<표 5> 양식장 수조의 설계제원

구조물	크기제원	중량
1층 구조물	3000×1500×2000[mm]	0.9[ton]
2층 구조물	3000×1500×1500[mm]	0.68[ton]
1층 수조	3000×1500×1000[mm]	4.5[ton]
2층 수조	3000×1500×1000[mm]	4.5[ton]

식장의 양식어종인 뱀장어는 표 6과 같이 최적생육을 위해서 수질을 제어 목표값으로 수질제어르 수행하였다. 최적의 수질환경을 구축하기 위하여 그림 8과 같이 수조는 수직 적층형 구조로 컨테이너 1층과 2층 구성하고 측면 육상에 순화여과장치(RAS)가 설치하여 운용시험을 진행하였다.

민물 뱀장어을 양식하는데 필요한 생육환경 조건은 표 6과 같다. 일반적으로 뱀장어는 난류성 어류로써 최적의 생육 온도는 25 ± 5[℃]이고, pH 6.5~8.5, 용존산소 5[mg/L]이상으로 최적화 제어가 필요하다. 발전소에서 방출되는 수온은

<표 6> 민물 뱀장어 생육환경의 수질 제어 목표 사양

	제어대상	목표값
1	PH	6.5 ~ 8.5
2	용존산소량(DO) [mg/L]	5 이상
3	생육 수온[℃]	25±5

(그림 9) 설계·제작된 48[USRT]의 온배수 히트펌프

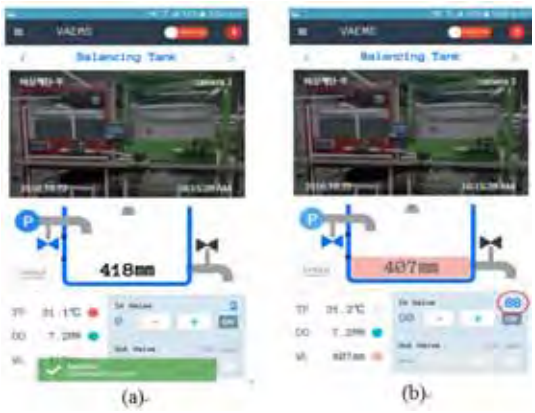
(그림 10) 마이컴 제어반과 제어신호 인터페이스

동계에는 13~15[℃]이고 하계는 25~35[℃]이다. 따라서 히트펌프는 동계와 하계에는 열에너지를 상승과 하강하는 2원 시이클 방식의 열제어 관리가 필요하다. 따라서 본 실험에서는 그림 9와 같이 이원사이클의 온배수 히트펌프를 설계하였으며, 제작된 히트펌프의 용량은 48.15[USRT], 소비전력은 2.89[KW/RT], 순환수량 57.78[LPM], 난방수량 145,600[Kcal/H], 성능계수(COP) 6.8의 출력성능을 가지며 온수에너지원은 최대 온도 70[℃]이고 수처리 용량은 12[Ton]이다. 설계 제작된 히트펌프는 열교환기를 통하여 수조의 온도를 장어가 성장시기에 가장 적합한 25~30[℃]로 수온제어를 수행한다.

IoT기반 스마트 양식장의 최적화 운용하기 위한 목적으로 원격제어 및 모니터링이 가능한 마이컴 제어반을 그림9와 같이 설계 제작하였다. 히트펌프와 스마트 양식장 수조의 데이터 모니터링하기 위해 모바일 응용 프로그램과 웹 응용 프로그램을 제작하였고, 양식수조의 환경제어를 위한 마이컴 제어반과 운용 프로그램을 개발하였다. 특히 스마트 양식장의 무인자동화를 위해서 센서 네트워크을 구성하였고 전동 밸브를 자체 개발하여 웹 또는 모바일을 활용하여 원격 제어로 수온, pH, 용존산소량을 제어할 수 있다.

설계된 IoT기반의 스마트 뱀장어 양식장은 그림 11과 그림12와 같이 웹과 모바일 앱과 연동되어 원격제어 및 모니터링이 가능하다. 양식수조, 순환여과장치와 밸런싱 탱크의 온배수 열에너지의 효율적인 관리와 스마트 양식장의 최적화 환경제어를 위한 센서 데이터인 전력량, 온배수 입출수 온도와 수질상태의 DO, pH, 온도, 수위 및 밸브 각도가 표시된다. 또한 양식장에서

(그림 11) 웹과 모바일 앱 어플리케이션

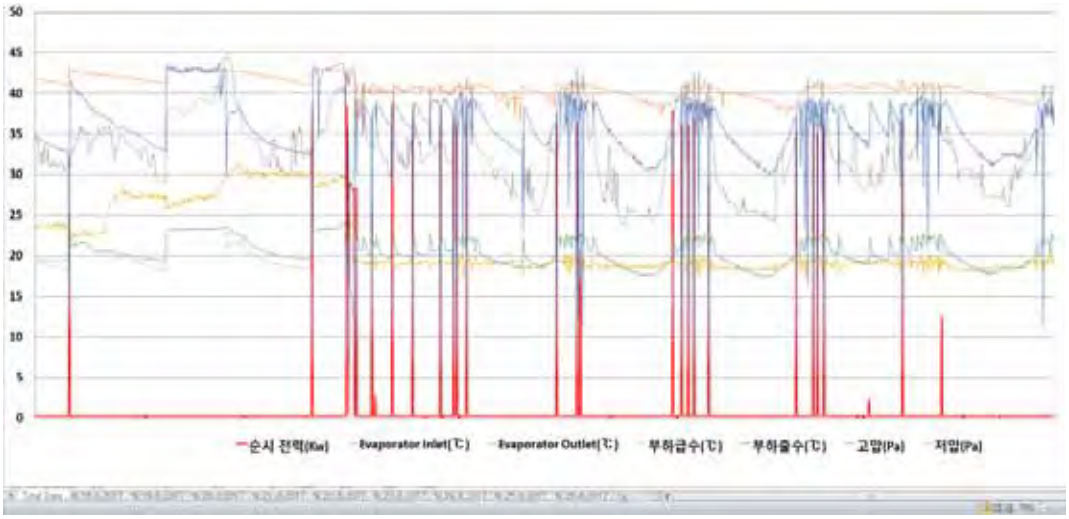


(그림 12) 스마트 양식장의 모바일 제어 앱
(a) 초기 동장상태, (b) 원격제어 동작 상태

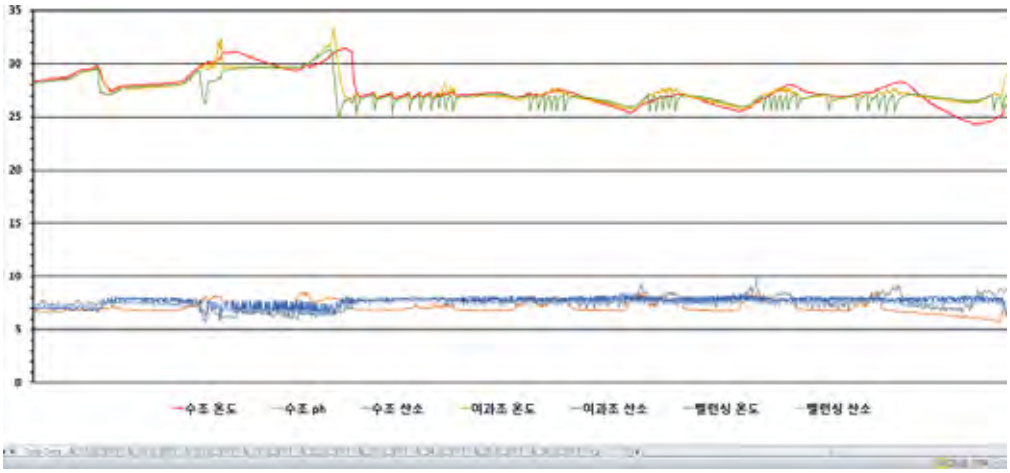
긴급한 상황이 발생되면 원격제어 모드를 이용하여 웹 또는 모바일을 이용하여 원격으로 제어할 수 있다. 모바일을 이용한 원격제어는 그림12와 같다. 그림 12의 (a)는 모바일에 의한 원격제어 이전의 초기 작동 상태를 나타낸 것 이고 그림12의 (b)는 밸브 각도를 2에서 88도까지 제어할 수 있으며 제어 된 센서 데이터를 확인 할 수 있다.

제안된 산업화 모델은 2017년 6월부터 10월까지 4개월간 온배수 히트펌프의 온배수 열에너지 와 스마트 양식수조의 수질제어에 대한 성능시험이 수행되었다. 그림 13은 2017년 8월 22일부터 2017년 9월 5일까지 2주간 온배수 열에너지의 입출수와 소비전력량에 대한 시험결과이다. 여기서 측정값은 온배수 히트펌프 작동 순시전력[Kw], 응축기 입출구 온도[℃], 부하급수 온도[℃], 출수 온도[℃]와 송수관의 압력[Pa] 데이터를 나타낸다. 히트펌프는 온배수 에너지 저장탱크의 온도가 양식수조 목표값이 25±5[℃]에 도달 하면 정지하고 온도가 떨어지면 작동하여 온배수 열에너지를 효율적으로 제어함을 알 수 있다. 또한 온도가 많이 하강되는 저녁부터 아침시간에는 자동적으로 가동됨을 확인할 수 있다.

또한 그림 14는 스마트 양식 수조의 온도, DO, pH 값을 시험 결과값이다. 순환여과조(RAS)의 수질제어 성능시험을 수행한 결과, 하절기에 시험이 수행되어 서은이험 초기에는 수온이 30[℃]를 초과한 상텡서 히트펌프에서 공급된 수냉에너지원에 의하여 25~27[℃] 범위내로 수온이 제어됨을 확인하였고, 용존 산소량 DO는



(그림 13) IoT기반 스마트양식장의 히트펌프 성능시험 결과



(그림 14) IoT기반 스마트양식장의 양식수조 성능시험 결과

6.5[mg/L]에서 8.5[mg/L], pH는 6.5~8.5 범위 내로 제어되어 설계사양 조건을 모두 만족함을 확인하였다. 상기의 성능시험을 통하여 제안된 IoT기반의 스마트 양식장 시스템의 성능은 설계사양 조건을 만족함을 확인하였다. 추가로 제안한 산업화 모델은 국제인증 시험기준 평가를 통하여 시험인증을 수행한 결과 설계된 스마트 양식장의 성능을 검증하고 인증시험을 완료하였다.

6. 결 론

제안된 발전소 온배수 에너지를 활용한 IoT기반의 스마트 양식장의 개발을 목표로 하고 있다. 설계된 IoT기반의 스마트 양식장의 산업화 모델은 그림1과 같은 수직 적층형 스마트 양식장 구조물로 설계되었고 뱀장어의 최적화된 생육환경을 제공하기 위한 목적으로 수위와 유량제어를 구현한다. 유량제어는 자체 개발한 스마트 피쉬맨 운용 프로그램에 의해 수질제어를 위한 구성장치인 벤츄리 4개, 원심 펌프 5개, 각 전자밸브를 제어함으로써 최적의 생육환경을 유지한다. 이 연구는 지난 2015 년 8 월부터 2017 년 10 월까지 한국 남부 발전에 설치된 열 펌프 및 수족관 에너지 관리 시스템 설계 및 성능시험 평가를 수행하였다.

본 연구를 통하여 수직적층형태의 아파트 형태의 빌딩양식에 대한 구조물 평가를 ANSYS 구조해석 시뮬레이션 통하여 안정성을 확인하였고, 웹과 모바일의 MQTT를 활용하여 수조센서 및 제어반과 컴퓨터 및 통신기기간의 데이터 통신과 양식장 운용 프로그램을 그림 11과 같이 모바일 및 웹 응용 프로그램을 통해 제어 및 모니터링을 성공적으로 수행하였다. 시스템은 원격제어를 수행하기 위하여 센서 네트워크를 구성하고, 전동 밸브를 설계하여 무인자동화된 IoT기반의 스마트 양식장을 설계 제작하였다[2][3][4].

수족관 시스템 분석 및 설계된 스마트 어 양식 시스템에 대한 실험 결과를 수위, 유량, 수온, 용존산소 및 pH 제어를 실험적으로 성공적으로 수행하여 설계사양 성능을 만족하였다. 또한 제안된 산업화 플랫폼 모델의 성능을 검증하기 위하여 국제 인증시험을 수행하여 인증서를 획득하였다. 또한 제안된 뱀장어 양식장의 양식면적 200여평에서 12톤 수처리를 하는 스마트 양식장

을 대상으로 경제성 분석을 실시한 결과, 년간 수량 22만톤 수처리를 수행하고 24시간 온배수 히트펌프를 가동할 시에 730[REC]가 발생하여 년간 9천여만원 정도의 경제성이 검증되었다. 제안된 IoT기반의 스마트 양식장은 수직 적층형 양식장 구조로 양식어의 생육환경을 개선하고 생산량을 증대시킬 수 있으며, 이 산업화 모델은 향후 우리나라의 스마트 양식장 보급과 해외 수출시장 개척에 큰 기대가 된다.

참 고 문 헌

[1] 이상철, 마창모, “첨단 스마트 양식 기술 발전 동향 분석,” 제어로봇시스템학회, 제22권, 3호, pp. 26-33, 6, 2016.

[2] K.J. Shin, A.V. Angani, "Design of 40URT Heat Pump for Vertical Aquarium Using Processed Waste Hot Water from Power Plants" IEEE Future Technologies Confer- ence , San Francisco, United States December 2016.

[3] K.J. Shin, A.V. Angani, “Development of Water Control System with Electrical Valve for Smart Aquarium”, IEEE International Conference on Applied System Innovation, Sapporo, Japan, pp.1-4, May 2017.

[4] K.J. Shin, A.V. Angani, M. Akbar, “Fully Automatic Control System for Smart Vertical Aquarium” IEEE International Conference on Applied System Innovation, Sapporo, Japan, pp.1-4, May 2017.

[5] ANSYS Inc., Release 13 Documentation for Ansys, No.1, pp.153-162, 2007.

[6] ANSYS-CFX ver. 13 Solver Guide, "The K omega and SST models", ver. 13, pp 99. 2007.

[7] Raymond James & Associates, “The Internet of Things - A Study in Hype, Reality, Disruption, and Growth”, http://sitic.org/wp-content/ The Internet of Things A Study in Hype Reality Disruption and Growth, January 2014.

[8] E. Brians, “Beginning Arduino Programming–Writing Code for the Most Popular Microcontroller Board in the World, ” Technology in Action, USA, 2011.

[9] V. Lampkin, W.T. Leong, L. Olivera, S. Rawat, N. Subrahmanyam, R.Xiang, “Building Smarter Planet Solutions with MQTT and IBM WebSpehere MQ Telemetry”, IBM Redbooks, pp. ix, USA, September 2012.

[10] D. Barata, G. Louzada, A. Carreiro, A. Damasceno, “System of acquisition, transmission, storage and visualization of Pulse Oximeter and ECG data using Android and MQTT”, HCIST 2013 - International Conference on Health and Social Care Information Systems and Technologies, Elsevier, pp.1265–1272, Portugal, 2013.

[11] R. Rischpater, “JavaScript JSON Cookbook, ” PACKT Publishing, pp. 1-3, Birmingham, UK, June 2015.

[12] S. Leon, R. Richard “Web Application Architecture Principles, Protocols and Practices”, John Wiley & Sons, England, 2003.

저 자 약 력

김 병 준

이메일 : kbj@bufs.ac.kr

- 2014년 한국해양대학교 기계공학과 (학사)
- 2016년 동 대학원 기계공학과 (석사)
- 2017년~현재 부산외국어대학교 ICT 창의융합학과 (박사과정)
- 2017년~현재 미래융합기술연구소 주임연구원
- 관심분야 : 기계제어 및 응용, 모델링 해석, 전기차량 BTMS, 수중 로봇, 스마트양식, 스마트팩토리 자동화기계.

신 규 재

이메일 : kyoojae@bufs.ac.kr

- 1985년 원광대학교 전자공학과 (학사)
- 1988년 전북대학교 전기공학과 (석사)
- 2009년 부산대학교 전기공학과 (박사)
- 1988년~1990년 해군기술병과학교 기술교관
- 1990년~1997년 두산(주) 방위산업기술연구소 주임연구원
- 1997년~2014년 순천제일대학교 전기자동화과 교수
- 2014년~현재 부산외국어대학교 전자로봇공학부 교수
- 2015년~현재 부산외국어대학교 미래융합기술연구소 소장
- 관심분야 : 동적 안정화 자세제어시스템, 극한환경 로봇, 수중 및 물고기로봇, 전기차량 및 배터리 열제어 시스템, 태양광발전 원격제어, IoT기반 스마트양식, 스마트 팩토리 자동화기계, 스마트 팩토리 설계

특집 02

IoT 기반 전력망 센서 네트워크 구현을 위한 Small Cell 무선통신시스템 기술개발 현황

김영현 · 강수경 · 박명혜 (한전 전력연구원)

목 차

1. 서 론

국내 전력산업은 신기술의 발달에 따른 패러다임의 변화, 산업-기술간 융합 확대, 부가가치가 높은 서비스에 대한 관심 증대 등으로 산업 전반에 걸쳐 큰 전환기를 맞이하고 있다. 과학기술 및 정보통신기술(ICT)의 발전으로 산업-기술간 융합이 확대되는 전력산업구조 개편이 진행되고 있다. 전력산업구조 개편과 스마트그리드 도입 등 전력시장의 환경변화에 따라, 전통적인 전력산업은 컴퓨터, 인터넷, 무선통신 등의 정보통신기술과 융합하면서 근본적인 혁신의 바람을 타고 있다. 특히, 스마트그리드의 경우 다른 신기술에 비해 상대적으로 산업 전반적인 융·복합적인 성격이 강하다는 점이 특징적이며, 스마트그리드 자체의 확산에 전통적인 전력과 전기산업 분야 뿐만 아니라, 통신, 신재생에너지, 전기자동차, 가전분야, 건설산업 등 다양한 시장참여자가 생겨나고 있다.

한전에서는 2020년 완료를 목표로 하는 AMI 구축, 2030년을 완료 목표로 하는 전력망 지능화 사업 등 국가차원으로 대규모 통신망 구축사업이 진행중에 있음에 따라 관련 사업을 원활하게 지원하기 위한 유무선 통신인프라 구축 및 운영기술이 요구된다.

지금까지의 스마트그리드 통신망은 유선기술, 특히 PLC 기반의 연구가 주로 수행되었으며, 장기적인 관점에서 무선통신에 대한 현장 활용기술연구가 시급하다. 일례로, 기존 통신망은 변압기를 중심으로 통신망이 설계·운영되었으나, 무선의 경우 변압기 중심이 아닌 수용가 밀집도 및 무선신호 세기를 기반으로 망 설계가 이루어져야 한다. 현재 개발된 운영시스템의 경우 무선의 지형조건 및 수용가 분포를 기반으로 망 설계 및 운영기능을 지원하고 있지 않아 무선기반 시스템 구축사업에 많은 어려움을 겪고 있어 한전에서 보유하고 있는 주파수 자원 및 비면허 대역을 이용, 무선망 활용정책에 대한 연구를 수행하고 더 나아가 한전에서 기확보한 IoT 표준기술(e-IoT : energy Internet of Things)을 기반으로 무선망 설계 기술을 확보하고자 한다.

2. 본 론

IoT 기반 전력망 센서 네트워크 구현을 위한 Small Cell 무선통신시스템 기술개발은 전력망에 최적화된 근거리무선통신망 솔루션 e-WSN (energy Wireless Sensor Network) 구현을 목표로 하고 있다.

추진전략으로서, 시범대상은 전체적으로는 기존 전력제어용 서비스와 IoT 등의 신규시범서비스 분야를 고려하여 크게 전력제어 (現 무선적용: DAS TRS), IoT (現 무선적용: 항공장애등감시 LoRa),AMI (現 무선적용: AMI Wi-SUN), 사회안전망서비스 (드론 활용 등)을 적용대상으로 계획하고 있다.

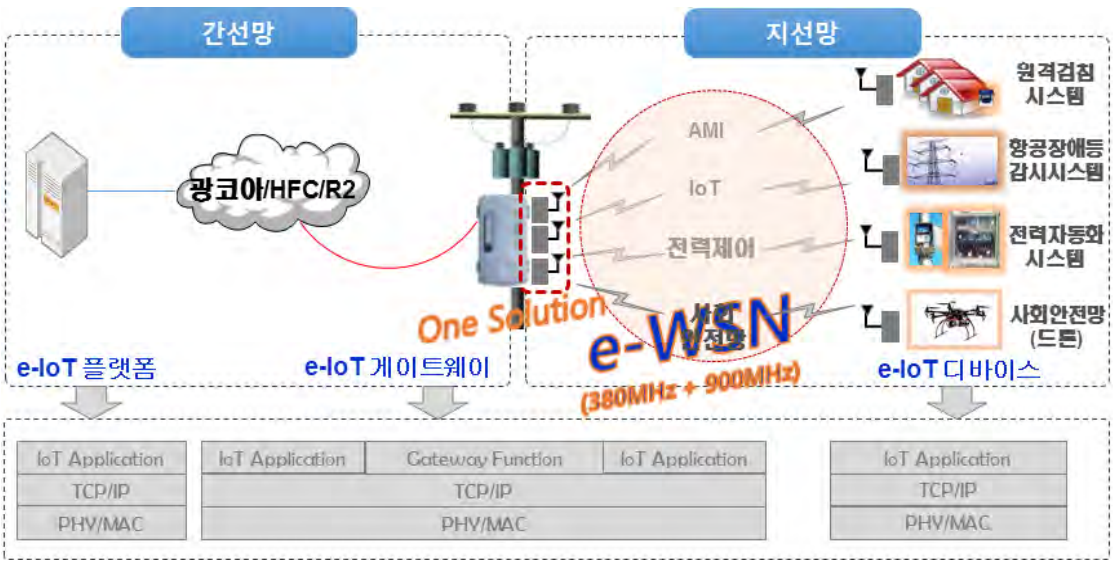
한편 실증전략은 국제표준 기반의 에너지 IoT 플랫폼 체계(e-IoT 플랫폼 ↔ 게이트웨이 ↔ 디바이스)로 무선센서네트워크 e-WSN을 구축하되, 개발 편의성 및 활용 극대화를 위한 One Chip Solution(모뎀+프로토콜+SDK개발환경)을 제공하는 것을 목표로 하고 있다.

2.1 전력서비스용 무선통신시스템 설계 연구

한전에서 보유하고 있는 380MHz 전용 대역 및 900MHz ISM 대역을 활용하며, 100kbps@25kHz, 500kbps@125kHz 이상의 전송속도를 지원하는 무선 송수신 모뎀 칩과 Protocol Stack 개발을 목표로 하고 있다.

한전 전용 주파수 대역과 ISM대역을 이용하는 무선통신기술을 개발하고 『RF+Baseband+Networking+Application』 하나의 칩으로 구현하여 다양한 전력서비스를 제공하기 위한 시스템을 설계하고, 크게 3대 분야를 중심으로 개발 및 기술확보를 추진하고 있다.

- 물리계층 기술개발 : 100kbps 속도/-120dBm 수신감도를 갖는 전송기술 개발
- 네트워킹 기술개발 : 1,000개 단말 수용/D2D 환경을 제공하는 망구성기술 개발
- SoC 및 운영기술 : 『RF+Baseband+Networking +Application』 One Chip 개발



(그림 1) 전력망 센서네트워크 e-WSN 실증 시스템 구성도

하드웨어 플랫폼 개발을 위해 모뎀 기능 검증을 위한 FPGA HW 플랫폼 제작, 저전력 CPU 코어를 내장한 MCU 시스템 IP 개발, 저전력 동작 지원 Power Gating IP 구현, 모뎀 기능검증을 위한 FPGA 하드웨어 플랫폼 제작, Gateway emulation/Signal capture 기능의 디버깅 환경 구축, 송수신 데이터를 캡처할 수 있는 대용량 메모리 장착, 송수신 데이터의 업로딩 및 다운로딩, 하드웨어 플랫폼을 이용한 모뎀 IP의 기능검증 등을 진행할 계획이다.

전력서비스용 Networking Protocol Stack 개발 측면에서 전력서비스 특성에 따른 Protocol Stack 규격과 Protocol Stack 및 NAS 개발, 전력서비스 위한 핵심기술로서 D2D(Device to Device) 릴레이 통신 기능 개발, 무선 자원 스케줄러 개발 등이 포함되어있다.

2.2 네트워크 설계 및 모델링 연구

신뢰성 있는 무선망 설계 및 분석을 위해서 공

<표 1> 전파모델 종류

전파모델		비고
Fresnel	Fresnel Propagation model	기본적인 자유 공간 모델에 추가적인 감쇄 식을 포함하는 모델이며, UHF와 SHF에서 좋은 성능을 보이며 VHF에서 약간의 마진을 가지고 전계 강도 계산에 적용
ITU-R P.525	CALCULATION OF FREE-SPACE ATTENUATION	프레넬에 반하여 추가적인 감쇄 식을 포함하지 않고 자유 공간 감쇄만을 적용한 모델
ITU-R P.370	VHF AND UHF PROPAGATION CURVES FOR THE FREQUENCY RANGE FROM 30 MHz TO 1000 MHz	방송 망을 계획하는데 사용될 VHF와 UHF 주파수대의 예측 방법이다. 이것의 기본적인방식에서는 지형 고도 지식이 거의 필요하지 않으며, 주로 다른 상황에서 얻은 전계 강도 측정 데이터에 기초
ITU-R P.1546	Method for point-to-area predictions f의r terrestrial services in the frequency range 30 MHz to 3000 MHz	일대다중 시스템을 이용하고 있는 방송국, 육상통시, 해상통신 및 임의의 고정서비스에서 전계강도 예측 방법, 예측은 거리경로(1~1000km), 시간 백분율(1~50%), 여러 가지 송신안테나 높이와 같은 파라미터 범위에 따라서 주파수 계획의 범위 내에서 이루어진다.
Okumura	OKUMURA Model	도심지에서의 신호를 예측할 때 가장 광범위하게 사용되는 모델이다. 150MHz에서 1920MHz 범위의 주파수와 1km 에서 100km범위의 거리에 대해 적용할 수 있으며, 30m 에서 1000m범위의 기지국 안테나 높이에 대해서 사용될 수 있다
HATA	HATA Model	150MH에서 2000MHz까지 적용 가능하며, 도심지역 전파경로손실 표준화공식으로써 만들어짐, 다른 환경에 대한 수정공식도 있음. 이 모델은 OKUMURA 모델에 의해 제공된 그래픽 경로손실 데이터의 경험적 공식화 과정에서 나온 결과입니다.
ITU-R P.368	Ground-wave propagation curves for the frequency between 10KHz and 30MHz	LF, MF, HF(AM) 대역 지표파
ITU-R P. 533	HF propagation prediction method	2~30MHz 주파수대역에서 원거리, 전리층 통신의 예측에 사용되며, P2P와 P2A 분석에 사용되며, 7000km 까지 광선경로 분석기법 사용, 9000km 이상은 측정된 실험데이터에서 적절한 실험공식 적용.
ITU-R P.452	Prediction procedure for the evaluation of microwave interference between stations on the surface of the Earth at frequencies above about 0.7GHz	700MHz에서 30GHz까지의 지상망의 간섭 분석을 위해 만들어진 것이다. P2P 분석으로 인접국가간 외래 간섭 발생 시 유입되는 간섭량이나 파라미터들을 예측하기 위한 것.

간상에서 전파 환경에 큰 영향을 주는 지형 및 장애물의 고려가 필수적으로 필요하다. 이를 위한 지형 및 3D 장애물, 경계 지도 등에 대한 GIS DB 데이터의 확보 및 전파전파 분석기술의 발달에 따른 다양한 방식으로 제작된 디지털 지도의 모델링이 필요하다. 모델링의 방법으로 Raster/Vector 방식이 있으며, 일반적으로 무선망 설계에서 가장 중요하게 사용하는 지형 모델의 경우 Rasterizing을 통한 정규격자(pixel)방식으로 모델링하게 된다.

• 전파 모델링

전파의 경로 손실에 대한 예측 모델을 선택하는 것을 전파 모델링이라고 하며, 이는 송신 장비로부터 일정한 거리에 위치한 점에서의 신호의 평균 수신 값을 예측하는 것으로 어느 위치를 중심으로 짧은 거리 범위 내에서 신호 세기의 변화를 예측하는 것이 신호의 전파 전달의 성질을 이해하는데 중요하게 작용된다.

특히 전파의 전달/전송 방법에 있어 반사(Reflection), 회절(Diffraction), 산란(Scattering), 감쇄(Attenuation), 페이딩을 기본으로 이것들을 모델링한 전파 모델과 회절 모델 및 날씨(안개/스모그, 비 등)의 영향이나 지형지물의 영향을 고려한 기법들이 적용되어야 한다.

무선망 설계 및 분석 S/W에는 사용자가 사용하는 기술 및 용도, 사용하는 디지털 지도의 유형에 따라 ITU에서 권고하는 모델들(Deterministic 모델)뿐만 아니라 오쿠무라-하타, 하타-코스트 231, 코스트 231 등의 실측에 의한 경험적인 전파모델들(Empirical)과, 불링톤, Deygout-94 등의 회절 감쇄 모델, 날씨에 대한 모델 등 다양한 전파모델들을 선택할 수 있어야 하며, 실측에 의해 수정된 모델 등 사용자가 임의 자신의 모델도 만들어 적용할 수 있어야 한다. 이를 사용하여 디지털 지도와 함께 다양한 조건 및 환경에서 전파의 영향을 분석하고 비교해볼 수 있으며, 또한 클러터와 연계하여 최적의 모델을 도출하는 것이 필요하다.

• GIS DB – 브이월드

국토교통부에서 제공하는 공간정보 오픈플랫폼 지도 서비스. '한국형 구글어스'로 고품질 3차원(3D)을 기반으로 국가, 지자체 등 공공 기관이 보유한 다양한 공간 정보와 행정 정보를 웹을 통해 제공한다. 국민 누구나 브이월드에 접속하면 오픈 플랫폼의 정보를 열람할 수 있으며, 정보를 활용하여 새로운 서비스를 개발하려는 사람은 제공된 오픈 API(Open-API)를 통해 자유롭게 활용할 수 있다. 디지털 지도를 활용한 무선망 설계를 위하여 국토교통부에서 제공하는 브이월드 지도데이터 중 필요한 자료를 확보하고 이를 변환하여 사용하고자 한다.

• 지형지도(DTM/DEM) & 3D 건물 & 시설물 DB 모델링

무선망 설계에서 가장 중요하게 고려되는 지도가 디지털 지형지도이다. 이것은 공간상에 나타나는 지형기복의 변화를 2차원 평면상에 연속적으로 표현하는 모델이다. DTM은 Digital Terrain Model의 약자이며, DEM은 Digital Elevation Model의 약자이다. 보통 지형만 고려될 때는 DTM을 사용하며, DEM은 지형과 건물(장애물)이 같이 고려되었을 때 사용한다.

• 시나리오 망 모델 시험 및 분석

다양한 요구사항에 맞추어 적절한 무선망 설계 및 분석을 위한 방향을 설정한다. 이에 따른

분석 방법 및 절차를 선정하고 최종 시스템에 부합하는지와 요구된 성능에 따른 분석 결과를 도출한다. 이러한 분석 방법 및 절차는 S/W를 통해 이루어지며, 각 설계 방향과 분석 방법 및 절차에 따라 시나리오를 모델링하고 그에 따른 결과를 시험 및 분석한다.

설계 및 분석방향은 설계 또는 분석하고자 하는 사용자의 요구사항에 따라 방향을 설정하고, 분석 방법 및 절차에서는 망 설계 대상에 대한 세부 요구사항을 파악하고, 분석 방법 및 절차에 반영, 장비와 기술에 대한 식별 및 제원에 따른 망(커버리지, 링크)의 요구사항이 부 합하는 지에 대해 분석 방법 및 절차에 반영, 트래픽 또는 품질 등을 목표로 하는 요구사항에 대한 분석 방법 및 절차 반영, 망 운용 방식을 고려한 분석 방법 및 절차 반영 등의 과정을 거친다.

2.3 Critical Communication 적용기술연구

무선 통신 기술의 단점으로 지적되는 time critical 이슈를 정의하고 해결 방안을 제시해 신뢰성 있는 전력 서비스 제공을 목표로 한다.

2015년 Motorola사에서는 critical communication을 위한 새로운 기술인 WAVE (Wide Area Voice Environment)를 발표했다. 이는 공공 안전 및 정부 서비스의 라디오 시스템을 위한 목적으로 구축된 라디오, 최적화된 광대역 통신망에 대한 전문화된 스마트폰, 광대역 캐리어의 소비자 등급 광대역 기기 등 어느 통신망이나 어느 기기에서든 모두 활용이 가능하다.

공공 안전과 LTE를 공공 안전 통신을 위한 차세대 플랫폼으로 확보하려는 공공 안전 및 중요 통신 분야에 대한 관심이 증가함에 따라, Project 25 및 TETRA (Terrestrial Truked Radio) 시스템과 같은 전통적인 협대역 기술에 대해, 3GPP는 새로운 그룹과 Release 13에 상응하는 아이템 (MCPTT, Mission Critical Push To Talk)을 출시하였다. 이번 3GPP의 작업에서 주된 목표는 통신 산업의 전 세계 커뮤니티의 요구를 충족하는 단일 공통 표준을 만드는 것이다. PS-LTE (Public Safety over LTE) 표준이 이미 3GPP Release 12 때 부터 ProSe (Proximity Services)와 GCSE (Group Communication Services Enabler) 주도하에 개발 중에 있으며 MCPTT는 미션 크리티컬 애플리케이션의 전반적인 애플리케이션 및 서비스 계층 측면을 개발하는 업무를

<표 2> 전력정보서비스 주요 요구사항

Mode	DAS	AMI
Frame length	300 Byte	100 Byte ~ 500 Byte
Transmission period	특정 event 발생 시	15 min.
Coverage	1,000 m 이내	도심지 : 200 m 이내 준도심지 : 400 m 이내 농어촌 : 500 m 이내
Maximum transmission power	TBD	2 W
Receiver Sensitivity	TBD	−120 dBm
UE capacity (수용단말수)	10대 이내	1,000가구
Data rate	TBD	9.6 kpbs
Error rate	TBD	PER 0.1
Latency	수 ms 이내	

담당한다. 그러나 MCPTT는 IMS, LTE Device to Decive Proximity Services (ProSe), LTE용 그룹 통신 시스템 enabler 등과 같은 기본 기술을 활용하여, 필요한 MCPTT의 요구사항을 실현할 것으로 기대된다.

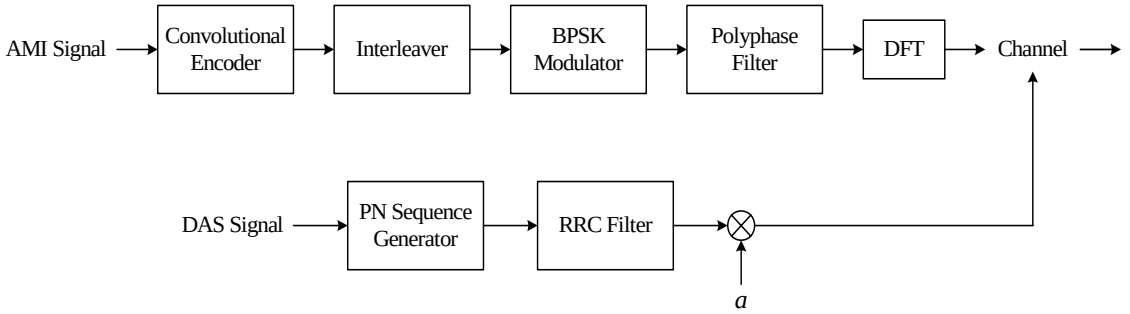
배전 자동화 시스템 (DAS, distributed automation system)은 주기적으로 전송되는 UE (user equipment) 신호와 emergency 신호가 동시에 전송될 때, UE 신호가 손실되지 않고 적절한 성능을 내기 위해 필요한 시스템이다. DAS의 요구사항에 부합하면서 최적의 성능을 얻을 수 있는 시스템 구조를 연구하고 최적화된 파라미터들을 도출하고자 한다. 본 연구에서 대상으로 하고 있는 DAS와 AMI의 요구사항은 다음 표와 같다.

AMI 시스템에서 권장되는 수신 감도는 -120 dBm으로 설정하였으며 이에 따라 25 kHz 채널 하나를 사용할 때를 기준으로 수신 신호의 최소 CNR (carrier-to-noise ratio)를 도출할 수 있다. 실제 구현에 사용되는 RF (radio frequency)부의 NF (noise figure) 값에 따라 차이가 있으나 대략 3 dB 이상의 CNR을 확보할 수 있을 것으로 예상된다. 따라서 최악의 경우 3 dB CNR에서 요구되는 에러율(error rate)을 달성할 수 있는 시스템을 설계하기 위하여 변조 방식, 채널 부호화방식 및 부호율 등을 설정해야한다. 특히, 신호 검출 (signal detection), 프레임 동기 (frame synchronization), 반송파 주파수 (carrier frequency) 및 심볼 타이밍 (symbol timing) 동기 등은 일반적인 동작 SNR (signal-to-noise ratio) 영역보다 낮은 영역에서도 동작하여야하므로 동기를 위한 프레임 구조 그리고 이에 부합하는 수신 동기 알고리듬 설계 시 CNR 3 dB 이하에서도 동작할 수 있도록 설계하여야 한다.

Emergency 신호는 PN sequence에 실려 전송되며 채널에서 spreading spectrum의 형태로 UE 신호와 더해진다. 이때, emergency 신호는 채널로 전송되기 전에 특정 상수 a가 곱해지며 이로 인해 특정 삽입레벨 (bury ratio)을 갖는 형태로 전송된다. 이를 도식화하면 아래 그림과 같다.

3. 결 론

앞에서 언급한 바와 같이 2020년 2,100만호 AMI 구축, '30년 전력망 지능화사업 등 국가차원으로 추진 중인 전력망 고도화사업으로 인해 통신회선은 급속히 증가하고 있으며, 임차비 증가에 따른 해결책 강구가 필요한 실정이다. 최근들어 개발 되고 있는 WiSUN, LoRA 등의 무선통신기술은 비면허 주파수 대역을 활용하고, 많은 데이터 전송을 필요로 하지 않는 응용에 접목



(그림 2) Block diagram of emergency signal and UE signal

되고 있고, 전력산업분야의 독자적인 보안 체계를 적용하기에 용이하지 않다. 표준화된 프로토콜 기반으로 지능화되고 있는 전력망에 고도의 보안기술과 무선통신기술을 융합한 전력서비스용 Device Solution 개발이 필요하며, 저주파 대역인 특히 한전의 380MHz 대역은 면허 대역이고, 송신 및 수신 주파수가 나누어져 있어 전파 특성이 우수하여 전력망 인프라 구축에 핵심 자원으로 활용 가능하기에 지능화되고 고도화되는 전력망 네트워크 요구사항에 적합한 중·고속의 속도를 지원할 수 있는 시스템 개발이 필요하다.

한전에서는 스마트그리드 확대에 따른 무선분야 솔루션 확보(AMI통신방식 기술검증사업(대상기술 : Zigbee), 900㎒ AMI 무선통신망 시범사업(대상기술 : SUN) 등), 무선통신 송수신기 설계 기초기술 확보(380㎒ 주파수 대역에서의 디지털 TRS기술을 활용한 중고속 데이터통신 송수신기 설계) 및 한전 IoT 표준기술인 e-IoT 구현기술이 확보된 상태이다.

따라서 전력망 사업 및 사물인터넷 활성화 사업 전략 측면에서 모뎀 및 관련 시스템 개발을 추진함으로써, 지능형 전력망 사업 및 사물인터넷 활성화를 위한 위해 수요가 크게 증가할 것으로 예상되는 통신망 수요를 해결하는데 확보된 무선통신기술의 역할이 기대된다.

참 고 문 헌

[1] AMI 근거리 통신기술분석, 한국통신학회논문지, 2013년 10월
[2] 전력망에서의 이더넷 활용기술, 한국통신학회논문지, 2015년 1월
[3] 에너지 IoT플랫폼에 관한 연구, 정보처리학회논문지, 2016년 6월.

저 자 약 력

김 영 현
이메일 : younghyun.kim@kepco.co.kr

- 2002년 한국항공대학교 정보통신공학 (학사)
- 2004년 광주과학기술원 정보통신공학 (석사)
- 2004년~현재 한전 전력연구원 선임연구원
- 관심분야 : 유무선 통신시스템 설계, 사물인터넷, 가상현실 및 증강현실, 시각지능

강 수 경
이메일 : sk.kang@kepco.co.kr

- 2008년 한양대학교 전자공학(학사)
- 2008년~현재 한전 전력연구원 연구원
- 관심분야 : 유무선 통신시스템 설계, AMI, 사물인터넷, 시각지능

박 명 혜
이메일 : myunghye.park@kepco.co.kr

- 1993년 경북대학교 전자공학과(학사)
- 1995년 경북대학교 전자공학과(석사)
- 1995년~현재 한전 전력연구원 책임연구원
- 관심분야 : 유무선 통신시스템 설계, 사물인터넷, 가상현실 및 증강현실, 시각지능

특집 03

NIST 양자내성암호 표준공모전 제출물 분석 및 향후 연구전망

박태환 (부산대학교), 서화정 (한성대학교), 김호원 (부산대학교)

목 차

1. 서 론

최근 양자컴퓨터 기술의 발전으로 인해, 2017년 17 Q-bit 기반의 양자컴퓨터가 개발된 상황이며, 양자컴퓨터와 관련된 Shor 알고리즘 및 Grover 알고리즘의 특성으로 인해 기존 공개키 기반 암호와 대칭키 기반 암호의 보안 안전성 문제가 발생할 것으로 예상되고 있다. 이러한 문제점을 해결하고자 전 세계적으로 많은 암호학자 및 수학자들에 의해, 양자컴퓨터 환경에서도 안전성과 보안성을 제공할 수 있는 양자내성암호(Post-Quantum Cryptography) 분야의 연구가 활발히 이루어지고 있다. 이러한 연구와 더불어 미국 국립 표준 기술원(NIST, National Institute Standard Technology)에서는 2012년부터 격주로 양자내성암호 세미나를 개최하였으며, 2015년부터는 NIST PQC Workshop으로 확대하여 개최하고 있다. 이를 통해 양자내성암호에 대한 표준 공모전을 준비하여 2016년 PQCrypto 2016에서 양자내성암호 표준 공모전에 대한 발표가 있었으며, 2017년 11월 30일자로 양자내성암호 표준공모전 후보군 제출을 마감한 상태이며, 올해 4월 후보군 제출자들과 NIST 간의 워크숍이 열릴 예정이며, 최종 표준 확정은 2023년에서 2025년 사이로 예상되고 있다.

미국 NIST의 양자내성암호 표준공모전은 기존의 AES, SHA-2/SHA-3 표준 공모전과 달리 하나의 표준 암호 제정이 아닌 다양한 환경에서 다양한 유형의 안전성과 효율성을 갖춘 양자내성암호 표준 후보군 제정에 그 목적을 두고 있으며, 양자내성암호 표준 확정 이후, 응용 및 활용성 강화 측면에서 각 후보군들의 응용 및 활용성 또한 고려될 것으로 보인다. 이에 따라 미국 NIST 양자내성암호 표준 공모전 제출물들에 대한 분석과 분석 결과를 바탕으로 향후 연구 진행을 통해 연구 및 기술 경쟁력 확보가 필요할 것으로 보인다. 본 논문에서는 미국 NIST 양자내성암호 표준 공모전에 제출된 제출물들에 대한

동향 분석과 양자내성암호 유형별 대표 제출물 특성 분석 결과를 제시하며, 분석 결과를 바탕으로 향후 연구 전망을 제시하고자 한다.

2. NIST 양자내성암호 표준공모전 제출물 분석

본 장에서는 NIST 양자내성암호 표준공모전 제출물에 대해 통계적 분석과 양자내성암호 유형별 대표 제출물에 대한 분석 결과를 제시하고자 한다. 기존에 알려진 양자내성암호의 유형은 격자 기반(Lattice Based), 코드 기반(Code Based), 다변수 기반(Multivariate Based), Isogeny 기반(Isogeny Based), 해시 기반(Hash Based)이 있다. 하지만 실제 NIST 양자내성암호 표준공모전 제출물 유형에 있어서 기존에 알려진 양식이 아닌 다른 유형과 기존 공개키 암호 방식의 개선안들이 포함되어있다.

2018년 2월 기준으로 NIST 양자내성암호 표준 공모전에 총 66건이 제출되었으며, 이 중 3건은 Withdraw가 된 상태이다. 제출된 66건에 대해 양자내성암호 유형별로 분석한 경과, 격자 기반(Lattice Based)이 가장 많은 26건이 있었으며, 코드 기반(Code Based)이 20건, 다변수 기반(Multi-variate Based) 9건, 해시 기반(Hash Based) 3건, Isogeny 1건, 기타 유형 7건으로 확인되었다. 이를 통해, 격자 기반(Lattice Based)과 코드 기반(Code Based) 가장 많은 유형을 차지하고 있다는 것을 확인할 수 있다.

양자내성암호의 방식의 경우, 전자 서명 기법이 21건, KEM (Key Encapsulation Mechanism), 키 교환 및 암/복호화 유형이 45건으로 확인되었다. 이를 통해, 전자서명과 KEM/키 교환 방식이 유형의 주를 이루는 것으로 확인되었다.

NIST 양자내성암호 표준 공모전 제출 건에 대해 참여한 국가별 분포를 분석한 경과, 미국이 총 22건에 참여하였으며, 프랑스가 15건, 네덜란드가 9건에 참여한 것으로 확인되었으며, 한국의 경우, 다른 국가와의 협업 방식이 아닌 독자 제안 방식으로 5건이 제출된 것으로 확인되었으며, 해당 수치는 일본, 캐나다, 벨기에와 동일한 수치이며, 4번째로 많은 제출 건에 기여한 국가인 것으로 확인되었다. 한국에서 제출한 5건에 대해 분석한 결과, 격자 기반(Lattice Based) 2건(KEM, 암/복호화 유형), 코드 기반(Code Based) 2건(전자서명 1건, 암/복호화 1건), 다변수 기반(Multi-variate Based) 1건(전자서명)으로 확인되었다.

다음으로는 제출물의 유형별 대표 제출물에 대해 분석한 결과를 설명한다.

2.1 격자 기반(Lattice Based) 양자내성암호 대표 제출물 분석

격자 기반(Lattice Based) 양자내성암호는 격자(Lattice) 상의 문제를 해결하는 것이 NP-hard 문제임에 기반으로 보안성을 제공하는 암호시스템 유형을 말한다.

격자 기반(Lattice Based) 양자내성암호의 대표적인 제출물인 CRYSTALS-Dilithium [1]은 독일 보훔(Bochum)대와 미국 SRI international, 스위스의 IBM Research, 네덜란드 Radbound 대학, 프랑스 ENS de Lyon이 같이 제출한 격자 기반 (Lattice-Based) 전자서명 방식으로써, 격자 상에서의 short vector를 찾기 어려운 문제에 기반하고 있다. 제안 기법은 “Fiat-Shamir with Aborts” 접근 방식을 기반으로 설계되었으며, 효율성을 위해, SHAKE-128 (암/복호화 시 사용), SHAKE-256(서명 기법 시 사용)을 사용하였으

	I weak	II medium	III recommended	IV very high
q	8380417	8380417	8380417	8380417
d	14	14	14	14
weight of c	60	60	60	60
$\gamma_1 = (q-1)/16$	523776	523776	523776	523776
$\gamma_2 = \gamma_1/2$	261888	261888	261888	261888
(k, ℓ)	(3, 2)	(4, 3)	(5, 4)	(6, 5)
η	7	6	5	3
β	375	325	275	175
ω	64	80	96	120
pk size (bytes)	896	1184	1472	1760
sig size (bytes)	1487	2044	2701	3366
Exp. reps (from Eq. (5))	4.3	5.9	6.6	4.3

(그림 1) Dilithium 파라미터

며, 제안 기법의 권고 수준의 보안강도를 가질 경우, 서명의 크기는 2.7KB, 공개키는 1.5KB의 크기를 가지는 것으로 확인되었다. 제안 기법의 파라미터 및 파라미터 별 공개키/서명 크기는 아래의 그림과 같다.

Dilithium의 보안강도별 성능 평가 결과는 아래와 같으며, 서명 생성 과정이 서명 검증 과정보다 오래 걸린다는 것을 확인 할 수 있었다. Dilithium의 가장 높은 보안강도의 경우, 키 생성에 512,116 cycles(ANSI C), 292,404 cycles (AVX2)가 걸리며, 서명 생성과정의 경우, 1,677,782 cycles(ANSI C), 711,018 cycles (AVX2)가 소요되며, 검증 과정은 548,558 cycles, 288,398 cycles가 소요되는 것으로 확인되었다.

2.2 코드 기반(Code Based) 양자내성암호 대표 제출물 분석

코드 기반 (Code Based) 양자내성암호는 일반적인 Linear Code를 Decoding하는 것이 NP-hard 문제임에 기반으로 보안성을 제공하는 암호시스템의 유형을 의미한다.

대표적인 코드 기반(Code Based) 양자내성암호 제출물에는 Classic McEliece가 있다. Classic McEliece [2]는 고 보안강도를 제공함과 동시에 IND-CCA2 보안성 제공을 위해 설계된 KEM 방식이며, Binary Goppa code를 사용하는 McEliece의 Niederreiter's dual version 기반으로 OW-CPA 보안성을 위해 설계된 PKE 기반 방식을 제공한다. 제안 방식에서는 2가지의 파라미터가 있으며, 관련 파라미터는 아래의 표과 같다.

NIST Security Level	-	1	2	3
Gen cycles (Haswell)	169,972	269,844	382,756	512,116
Sign cycles (Haswell)	765,442	1,285,476	1,817,902	1,677,782
Verify cycles (Haswell)	196,048	296,920	395,936	548,558
Gen cycles (AVX2, Haswell)	104,128	156,432	225,432	292,404
Sign cycles (AVX2, Haswell)	338,922	493,332	673,144	711,018
Verify cycles (AVX2, Haswell)	105,584	150,228	207,164	288,398

(그림 2) Dilithium 성능 평가 결과 (AVX2 SIMD 미적용/적용, Haswell 환경)

<표 1> Classic McEliece 파라미터

제안방식 유형	m	n	t	l	해시함수
kem/mceliece6960119	13	6960	119	256	SHAKE256
kem/mceliece8192128	13	8192	128	256	SHAKE256

Classic McEliece의 성능 평가는 소프트웨어와 하드웨어 2종으로 제시되고 있다. 소프트웨어 성능 평가의 경우, GCC 컴파일러를 활용하여 -march=native-mtune=native-O3 -fomit-frame-pointer-fwrapv 옵션으로 컴파일된 소스에 대한 성능을 평가하였으며, 각 수행에서 31 timing의 중간 값을 성능치로 평가가 진행되었다. mceliece8192128의 경우, Encapsulation 과정에 첫 번째 수행에서는 296036 cycles, 두 번째에서는 295392cycles, 세 번째에서는 295932 cycles가 소요되는 것으로 확인되었으며, De-capsulation의 경우, 3회의 수행에 대해 각각 458556cycles, 458476 cycles, 458340 cycles가 소요되며, 키 생성 과정은 수십억 cycles가 소요되는 것으로 확인되었으며, 중간치로 각각 4010278828 cycles, 6008245724 cycles(약 2초), 4005886024 cycles가 소요되는 것으로 확인됨. 각 키 생성과정은 약 20억 cycles 정도 소요되는 것으로 확인되었다.

하드웨어 성능 평가의 경우, 중간 크기의 Altera Straix V FPGA (5SGXEA7N) 상에서 synthesize 및 성능 평가가 이루어졌다. mceliece8192128의 경우, 231MHz 동작 주파수 상에서 키 생성 과정은 1173750 cycles (5.08ms), Decoding 과정은 17140 cycles (0.074ms)가 소요되는 것으로 확인되었으며, mceliece6960119의 경우, 248MHz 동작 주파수 상에서 키 생성 과정은 966400 cycles (3.58ms), Decoding 과정은 17055 cycles (0.060ms)가 소요되는 것으로 확인 되었다. 하드웨어 면적의 경우, mceliece8192128이 227,750 레지스터(flip-flops), 129,059 ALMs (가능한 로직 자원의 55%), 1,126 RAM blocks (가능한 on-chip RAM의 44%), 4개의 DSP 블록(가능한 DSP의 1.6%)이 필요한 것으로 확인되었고, mceliece6960119의 경우, 223,232 registers (flip-flops), 121,806 ALMs (가능한 로직 자원의 52%), 961 RAM blocks (가능한 on-chip RAM의 38%), 6 DSP blocks (가능한 DSP의 2.3%)가 필요한 것으로 확인되었다(키 생성부분과 decoding부분만 포함된 면적).

제안 기법에서의 입/출력의 크기는 아래의 표와 같다.

2.3 다변수 기반(Multi-variate Based) 양자내성암호 대표 제출물 분석

다변수 기반(Multi-variate-Based) 양자내성암호는 유한체에서 다변수 함수를 푸는 것이 NP-hard문제인 것에 기반으로 보안성을 제공하는 암호시스템 유형을 말하며, 대표적인 제출물

<표 2> Classic McEliece의 유형별 공개키/비밀키/암호문/세션키 크기 비교

제안기법 유형	공개키 크기(byte)	비밀키 크기(byte)	암호문 크기(byte)	세션키 크기(byte)
mceliece8192128	1357824	14080	240	32
mceliece6960119	1047319	13908	226	32

은 Rainbow가 있다. 표준 공모전에 제출된 Rainbow [3]는 기존 Rainbow 전자 서명 기법을 수정 변경한 방식이다. 제안 기법의 파라미터와 파라미터 별 공개키, 개인키, 해시 크기, 서명 크기는 아래의 그림과 같으며, 제안 기법의 파라미터 중 가장 높은 보안강도를 제공하는 VIb 파라미터를 사용하는 경우, 공개키는 1,321KB, 비밀키는 922.4KB, 서명 크기는 128bit salt값을 포함하여 1,176bit가 소모되는 것으로 확인되었다.

제안 기법의 소프트웨어 성능 평가에서 가장 높은 보안강도를 제공하는 VIb 파라미터를 사용하는 경우, 키 생성과정에 49,906ms (ANSI C), 1,066ms (AVX2)이 소요되며, 서명 생성 과정은 5.077ms (ANSI C), 1.108ms (AVX2)가 걸리며, 서명 검증 과정의 경우, 3.401ms(ANSI C), 1.421ms (AVX2) 가 걸리는 것으로 확인되었다.

2.4 Isogeny 기반(Isogeny Based) 양자내성암호 대표 제출물 분석

Isogeny 기반 양자내성암호는 Order가 같은 두 타원곡선 사이에 존재하는 Isogeny를 구하는 것이 NP-hard 문제임에 기반으로 보안성을 제공하는 암호시스템 유형을 의미한다. 이번 NIST 양자내성암호 표준 공모전에는 SIKE (Supersingular Isogeny Key Encapsulation) 1건이 제출되었다.

SIKE [4]는 미국 마이크로소프트(MS)사를 중심으로 제안된 Supersingular Isogeny Key Encapsulation(SIKE) 기법을 의미하며, Supersingular Isogeny Diffie-Hellman(SIDH)를 기반으로 한 키 교환 기법에 해당된다. 제공 방식은 IND-CPA KEM과 IND-CCA KEM 방식이 있다. 제안 기법의 성능 평가의 경우, 제안 기법에 대한 성능 평가를 위해 제안자들은 GMP 라이브러리를 활용한 레퍼런스 코드, portable C 기반의 최적화 구현, x64 assembly 기반의 최적화 구현, ARM64환경에 대해 ARMv8 assembly 기반의 최적화, FPGA와 ASIC을 위한 VHDL모델(속도 최적화)을 제시하고 있다. 제안 기법에 대한 최적화 구현의 경우, F_{p^2} 상에서의 효율적 연산을 위해 Karatsuba and lazy reduction을 사용하였고, fully roled 버전의 Comba, Montgomery reduction을 사용하였음. x64 환경 상에서는 MULX, ADX 명령어 이용 가능성으로 인해 Comba 곱셈보다 Schoolbook 곱셈이 더 좋은 성능을 보이는 것으로 확인되었으며, 제안 기

parameter set	parameters $(\mathbb{F}, v_1, o_1, o_2)$	public key size (kB)	private key size (kB)	hash size (bit)	signature size (bit) [1]
Ia	(GF(16),32,32,32)	148.5	97.9	256	512
Ib	(GF(31),36,28,28)	148.3	103.7	268	624
Ic	(GF(256),40,24,24)	187.7	140.0	384	832
IIIb	(GF(31),64,32,48)	512.1	371.4	384	896
IIIc	(GF(256),68,36,36)	703.9	525.2	576	1,248
IVa	(GF(16),56,48,48)	552.2	367.3	384	736
Vc	(GF(256), 92,48,48)	1,683.3	1,244.4	768	1,632
VIa	(GF(16), 76,64,64)	1,319.7	871.2	512	944
VIb	GF(31), 84,56,56)	1,321.0	922.4	536	1,176

[1] 128 bit salt included

(그림 3) Rainbow 파라미터 별 키/서명 크기

Scheme	KeyGen (stack)	Encaps (stack)	Decaps (stack)	static library	
				speed (-03)	size (-0s)
Reference Implementation					
SIKEp503	512	762	1528	107,450	96,386
SIKEp751	2880	1332	2280	107,450	96,386
SIKEp964	3744	2262	2936	107,450	96,386
Optimized Implementation					
SIKEp503	8,040	8,632	9,464	122,612	60,020
SIKEp751	13,864	14,024	14,680	167,508	61,404
Additional implementation using x64 assembly					
SIKEp503	8,120	8,520	8,952	132,688	62,488
SIKEp751	14,032	14,176	14,944	188,720	67,080

(그림 4) SIKE S/W 속도 메모리 사용량 평가 (단위: 1,000 cycles, bytes)

법에서 사용하는 소수 $p = 2^{e_2}3^{e_3} - 1$에 대해 최적화된 Montgomery reduction을 구현하여 사용하였다. x64 Assembly로 최적화 구현된 SIKEp751의 경우, 키 생성과정에 30,919(1000 cycles)이 소요되며, En-capsulation과 De-capsulation 과정은 총 103,852(1000 cycles)가 소요되는 것으로 확인되었다. 제안 기법에 대한 레퍼런스, 최적화 및 x64 assembly 구현물의 메모리 사용량은 아래의 그림과 같음. SIKE의 메모리 사용량에서 stack 사용량은 레퍼런스 코드가 가장 적게 소모되는 것으로 확인되었고, static library 크기의 경우, 최적화 구현 결과물이 가장 적게 소모되는 것(-Os 컴파일 옵션)으로 확인되었다.

2.5 해시 기반(Hash Based) 양자내성암호 대표 제출물 분석

해시 기반 양자내성암호는 해시 함수의 안전성에 기반으로 보안성을 제공하는 전자서명 시스템 유형을 의미한다. 대표적인 제출물로는 SPHINCS+ [5]가 있다. SPHINCS+는 기존에 연구된 SPHINCS와 유사한 과정을 수행하지만, 기존 대비 Multi-target 공격에 대한 방어가 가능하며, Tree-less WOTS+ 수행 및 FORS key pair를 사용함으로써 $k2^a$ bit message digest에 대한 서명이 가능하며, Verifiable index selection 기

	n	h	d	$\log(t)$	k	w	bitsec	sec level	sig bytes
SPHINCS$^+$-128s	16	64	8	15	10	16	133	**1**	8 080
SPHINCS$^+$-128f	16	60	20	9	30	16	128	**1**	16 976
SPHINCS$^+$-192s	24	64	8	16	14	16	196	**3**	17 064
SPHINCS$^+$-192f	24	66	22	8	33	16	194	**3**	35 664
SPHINCS$^+$-256s	32	64	8	14	22	16	255	**5**	29 792
SPHINCS$^+$-256f	32	68	17	10	30	16	254	**5**	49 216

(그림 5) SPHINCS+ 파라미터

	public key size	secret key size	signature size
SPHINCS$^+$-128s	32	64	8 080
SPHINCS$^+$-128f	32	64	16 976
SPHINCS$^+$-192s	48	96	17 064
SPHINCS$^+$-192f	48	96	35 664
SPHINCS$^+$-256s	64	128	29 792
SPHINCS$^+$-256f	64	128	49 216

(그림 6) SPHINCS+ 키, 서명 크기(단위:byte)

능을 제공한다. 제안 기법의 파라미터 값 및 파라미터별 키, 서명크기는 아래의 그림과 같다.

SPHINCS+의 성능평가는 Intel x86-64환경 상에서 수행되었다(-O3 옵션). 성능 평가는 아래의 그림과 같으며, 다양한 해시함수를 사용하여 성능 측정하였다. 특히 Haraka의 경우, AES 암호 활용이 필요한 구조로써, Intel AES-NI 기반의 하드웨어 가속기 활용 성능 또한 제시하고 있다.

2.6 기타 유형의 양자내성암호 대표 제출물 분석

기타 유형의 양자내성암호로는 메르센 소수를 활용한 Mersenne-756839 기법 [6]과 기존의 RSA 공개키 암호에 대해 양자컴퓨터 환경에 따른 소수 및 파라미터 크기 확장을 통한 암/복호화 및 서명 기법 [7, 8]들을 제시하고 있다. 하지만 이러한 새로운 유형의 경우, 안전성 관점에서 많은 연구가 되어 있지 않기 때문에 양자컴퓨터 환경 상에서의 안전성에 대한 연구가 필요할 것

	key generation	signature generation	verification
SPHINCS$^+$-SHAKE256-128s	617 619 732	8 610 599 004	10 222 936
SPHINCS$^+$-SHAKE256-128f	19 348 784	580 904 788	24 826 884
SPHINCS$^+$-SHAKE256-192s	907 587 276	17 586 416 344	15 036 680
SPHINCS$^+$-SHAKE256-192f	28 200 752	757 001 640	40 338 224
SPHINCS$^+$-SHAKE256-256s	1 210 939 356	13 842 403 104	20 889 204
SPHINCS$^+$-SHAKE256-256f	75 031 996	1 664 510 764	41 469 276
SPHINCS$^+$-SHA-256-128s	307 425 484	4 606 958 168	5 514 124
SPHINCS$^+$-SHA-256-128f	9 625 644	302 359 220	12 901 012
SPHINCS$^+$-SHA-256-192s	576 727 832	12 239 247 980	10 740 192
SPHINCS$^+$-SHA-256-192f	17 902 436	487 388 724	26 456 352
SPHINCS$^+$-SHA-256-256s	1 095 050 628	12 893 347 756	19 141 296
SPHINCS$^+$-SHA-256-256f	68 819 608	1 558 148 364	38 316 192
SPHINCS$^+$-Haraka-128s	917 405 356	16 992 635 344	19 360 272
SPHINCS$^+$-Haraka-128f	28 814 020	1 056 761 824	45 964 624
SPHINCS$^+$-Haraka-192s	1 244 530 184	38 062 259 596	27 243 200
SPHINCS$^+$-Haraka-192f	42 782 840	1 276 694 620	69 760 728
SPHINCS$^+$-Haraka-256s	1 817 324 180	28 860 355 888	42 380 420
SPHINCS$^+$-Haraka-256f	113 876 252	3 172 247 452	76 203 004

(그림 7) SPHINCS + 성능 평가 결과 (단위: cycles)

으로 보인다.

3. 양자내성암호 향후 연구전망

앞선 장에서 살펴본 미국 NIST 양자내성암호 표준 공모전에 제출한 유형별 대표적인 제출물 분석 결과를 바탕으로 향후 양자내성암호 연구는 다양한 사물인터넷용 디바이스 환경 상에서의 최적화 구현 연구 및 하드웨어 최적화 구현 연구가 필요할 것으로 보이며, 유형별 부채널 공격 관점 상에서의 안전도와 대응방안 연구 또한 동시에 필요할 것으로 보인다. 이러한 구현 및 공격 관점에서의 연구 이후에는 연구결과물들에 대해 각종 응용 단에서의 적용 및 적용 시 발생할 수 있는 문제 해결을 위한 연구가 필요할 것으로 보인다.

4. 결 론

본 논문에서는 최근 미국 NIST 양자내성암호 표준 공모전 1차 라운드 제출물에 대한 유형/방식 등 통계적 분석 결과와 양자내성암호 유형별 대표적인 제출물에 대한 분석 결과를 제시하고 있다. 이러한 분석 결과를 바탕으로 향후 양자내성암호 연구에 대한 연구전망을 제시하였다. 본 논문의 결과는 향후 양자내성암호 연구 분야에서의 연구 기술력 및 국가 경쟁력 확보에 있어서 기초자료로써, 많은 도움이 될 것으로 기대된다.

참 고 문 헌

[1] V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler, D. Stehle, Crystals-dilithium, Tech. rep., National Institute of Stan- dards and Technology, available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions (2017).

[2] D. J. Bernstein, T. Chou, T. Lange, I. von Maurich, R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Sze- fer, W. Wang, Classic mceliece, Tech. rep., National Institute of Standards and Technology, available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions (2017).

[3] J. Ding, M.-S. Chen, A. Petzoldt, D. Schmidt, B.-Y. Yang, Rainbow, Tech. rep., National Institute of Standards and Technology, available at https://csrc.nist.gov/projects/post-quantum-cryptography/ round-1-submissions (2017).

[4] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. D. Feo, B. H. A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, D. Urbanik, Sike, Tech. rep., National Institute of Standards and Technology, available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions (2017).

[5] A. Hulsing, D. J. Bernstein, C. Dobraunig, M. Eichlseder, S. Fluhrer, S.-L. Gazdag, P. Kampanakis, S. Kolbl, T. Lange, M. M. Lauridsen, F. Mendel, R. Niederhagen, C. Rechberger, J. Rijneveld, P. Schwabe, Sphincs+, Tech. rep., National Institute of Standards and Technology, available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions (2017).

[6] D. Aggarwal, A. Joux, A. Prakash, M. Santha, Mersenne-756839, Tech. rep., National Institute of Standards and Technology, available at https://csrc.nist.gov/projects/post-quantum-cryptography/ round-1-submissions (2017).

[7] D. J. Bernstein, J. Fried, N. Heninger, P. Lou,

L. Valenta, Post-quantum rsa-encryption, Tech. rep., National Institute of Stan- dards and Technology, available at https://csrc.nist.gov/projects/ post-quantum-cryptography/round-1-submissions (2017).

[8] D. J. Bernstein, J. Fried, N. Heninger, P. Lou, L. Valenta, Post-quantum rsa-signature, Tech. rep., National Institute of Stan- dards and Technology, available at https://csrc.nist.gov/projects/ post-quantum-cryptography/round-1-submissions (2017).

저 자 약 력

박 태 환

이메일 : pth5804@pusan.ac.kr

- 2013년 부산대학교 정보컴퓨터공학부 (학사)
- 2013년~현재 부산대학교 전기전자컴퓨터공학과 (석, 박사 통합과정)
- 관심분야 : 암호화 S/W 구현, IoT 디바이스 보안, 양자 내성 암호

서 화 정

이메일 : hwajeong84@gmail.com

- 2010년 부산대학교 컴퓨터공학과 (학사)
- 2012년 부산대학교 컴퓨터공학과 (석사)
- 2016년 부산대학교 컴퓨터공학과 (박사)
- 2015년 4월~5월 싱가포르 난양공대 인턴쉽
- 2016년 1월~2017년 3월 싱가포르 과학기술청 연구원
- 2017년 4월~현재 한성대학교 조교수
- 관심분야 : 정보보호, 암호화 구현, IoT

김 호 원

이메일 : howonkim@pusan.ac.kr

- 1993년 경북대학교 전자공학과 학사 졸업
- 1995년 포항공과대학교 전기전자공학과 석사 졸업
- 1999년 포항공과대학교 전기전자공학과 박사 졸업
- 2008년 한국전자통신연구원 정보보호연구단 선임연구원/팀장
- 2008년 3월~현재 부산대학교 전기컴퓨터공학부 정교수
- 관심분야 : 스마트그리드 보안, RFID/USN 정보보호 기술, PKC 암호, VLSI 설계, Embedded system 보안, IoT 보안

KIPS 취임사

한국정보처리학회 2018년도 회장 취임사

안녕하십니까! 한국정보처리학회의 2018년도 제23대 회장을 맡게 된 콤텍시스템 남석우 대표입니다.

2018년 무술년 새해를 맞이해서 회원 여러분 모두 새해 복 많이 받으시고 항상 건강하시기를 기원드립니다. 아울러 지난 한해동안 학회 발전과 우리나라 ICT 학문 발전을 위해 노력해 주신 학회 회원님들을 비롯한 임직원들의 노고에 깊이 감사의 말씀을 드립니다.

존경하는 한국정보처리학회 회원 여러분!!

우리 학회가 창립한지 25년이 지난 청년기에 접어들어 제2의 도약을 해야하는 한국정보처리학회는 그동안 수많은 학술 활동을 통해 명실공히 국내 최고의 학회로 성장했습니다. 이러한 발전은 1대 성기중 회장님을 비롯한 역대 전임 회장님들과 임원 여러분들의 열정과 노력으로 오늘의 한국정보처리학회를 만들었다고 생각합니다.

이제 저는 이러한 선배님들이 이룩해 놓으신 현재의 한국정보처리학회를 발판으로 더욱 도약하는 학회를 만들기 위해 최선의 노력을 다하겠습니다.

특히, 다음의 중요한 몇가지의 역점 사업을 통해 내년도 학회 발전에 일조하고자 합니다.

첫째, 회원과의 소통 강화 및 공동 이익 실현의 기반을 마련하겠습니다.

둘째, 산·학·연의 동반 성장을 실현하겠습니다.

셋째, 학회의 글로벌화를 적극 추진하겠습니다.

마지막으로, 학회 재정 확보 방안도 적극 마련하겠습니다.

현재의 한국정보처리학회를 발판으로 더욱 도약하는 학회를 만들기 위해 학회 설립 목적을 충실히 실천하는 회장으로서 역할을 다할 것을 약속드립니다..

더불어 유관기관과의 긴밀한 협력을 통하여 명실상부한 산학협력 학회로 성장할 수 있는 발판과 역대 회장님들의 노고와 회원들의 기대에 어긋나지 않도록 국내 제일의 학회가 되기 위해 최선의 노력을 다하겠습니다.

끝으로 금년 한해에도 임원 여러분 모두의 가정과 직장에 발전과 영광이 같이 하시길 기원합니다.

감사합니다.

2018년 1월

한국정보처리학회 회장 남석우

KIPS

권두언

2018년, 새로운 희망과 함께 학회지 발간 횟수를 조정하며...

몇 년 전부터, 컴퓨터 과학기술 중 인공지능이 두각을 나타고 있으며 음악, 영화 등을 사용자의 기호에 따라 검색 및 추첨하면서 우리의 실생활에 적용되고 있습니다. 우리학회에 제출되는 연구 논문들도 인공지능 기술과 응용에 대한 것으로 집중되고 있으며 이는 우리 학회의 연구 방향과도 일맥상통하는 것으로 향후에 학회의 사업 분야에 대한 확장에도 많은 도움이 될 것입니다.

한국정보처리학회의 학회지에서는 기술에 대한 새로운 통찰력을 확보하는데 도움이 되고자 회원님들께 매년 새롭고 주요한 연구 및 기술적인 이슈들을 제공해 왔습니다. 특히, 우리 학회만의 특징인 산/학/연 형태의 회원 구성은 새로운 기술에 대한 심도 있는 연구, 응용 및 산업화가 가능하여 대한민국의 ICT 기술발전에 이바지하고 있다고 자부하며 더욱 높은 사명감을 갖고 있습니다.

그동안 우리 학회지는 격월 발간으로 많은 독자들에게 다양한 기술에 대한 정보를 제공하였습니다. 그러나 우리가 이미 경험했던 빅데이터나 인공지능과 같은 주요기술들의 현상은 페레토 법칙(Pareto principle)과 같이 20%의 주요기술들이 연구와 산업현장에서 기술 발전의 80%를 견인하고 있습니다. 우리학회에서는 이와 같은 현상을 반영하고 핵심 기술에 대한 보다 알찬 정보를 제공하고자 기술의 분석과 원고모집기간을 고려하여 학회지 발간 횟수를 연 2회(1월, 7월)로 조정하였습니다.

올해에 첫 번째로 발간되는 학회지는 과도기적인 성격이 강하여 세 개의 주제 - '4차 산업혁명 (양순옥 교수)', 'ICT융합 (김호원 교수)' 그리고 '병렬 프로그래밍 기법 (김종완 교수)' - 을 묶어서 출간하게 되었습니다. 각 주제에 대한 원고를 모으고 출판에 수고를 아끼지 않으신 편집 위원님들께 감사를 드리며 특히, 병렬 프로그래밍 기법에 대한 원고를 제출해주신 저자 분들께도 감사의 인사를 드립니다.

우리 학회지는 주요 기술에 대한 연구현황과 기술의 응용에 대한 지속적인 정보제공을 통해 회원님들의 궁금증을 해소하는 ICT 기술 정보지로서의 역할을 충실하게 수행할 것입니다. 향후에도 학회지에 대한 많은 관심을 부탁드립니다.

2018년 1월

한국정보처리학회 학회지편집위원장 김 종 완

특집 01

AVX-512를 활용한 인텔 차세대 프로세서에서의 효과적인 프로그래밍 방법

최재영 · 김래현 · 임록택 (숭실대학교)

목 차

1. 서 론

마이크로프로세서의 클럭 증가에 따른 전력 소모와 그에 따른 발열에 대한 제약으로 인해 고성능 컴퓨팅 아키텍처는 점차 낮은 클럭의 다수 코어로 이루어진 칩 병렬화 구조로 변화되고 있다. 이런 추세에 발맞춰 인텔은 2001년 DP (Dual processor) 및 MP (Multi processor, 4개 이상) 구조의 서버용 Intel Xeon 프로세서를 시작으로 2017년 현재 최대 24개 코어 프로세서까지 출시하였다. 뿐만 아니라 2012년 Many Integrated Core (MIC) 구조의 Xeon Phi Knights Corner (KNC)를 시작으로 2016년 Xeon Phi Knights Landing (KNL)을 출시하였다. 인텔 Xeon Phi 프로세서는 최대 72개의 코어로 구성되어 있으며, Vector Processing Unit (VPU)을 통해 최대 512-bit 길이의 강력한 벡터 연산 기능을 지원한다. 2017년에 출시된 Intel Xeon Skylake Scalable Processors (Skylake-SP)도 Advanced Vector Extensions 512 (AVX-512) 명령어를 지원한다.

인텔 차세대 아키텍처의 성능을 최대한 이끌어내기 위해서는 대상 프로세서의 구조를 정확히 파악하고, 이를 바탕으로 효과적인 알고리즘을 구현해야 한다. 벡터 연산 기능을 효과적으로 활용하기 위해 벡터화가 용이한 형태로 알고리즘을 수정함과 동시에 Single Instruction Multiple Data (SIMD) 명령어를 적극적으로 사용해야 한다. 또한 다중 레벨 캐시 구조에 맞게 캐시 재활용을 최대화하여 주된 성능 저하 요인인 대역폭을 최소화하여야 한다. 뿐만 아니라 환경 변수와 컴파일 옵션 등 추가적으로 고려해야 할 요소가 다수 존재한다. 일반 사용자에게 있어 이러한 요소들을 모두 고려하여 프로그램을 작성하고 최적화하는 것은 매우 어려울 뿐 아니라 많은 시간을 소요하게 된다.

본 논문에서는 일반 행렬 곱셈 알고리즘의 구현 결과를 바탕으로 인텔 차세대 아키텍처를 효

과적으로 사용하는 방법을 제시하고자 한다. 2장에서는 인텔 Xeon Phi Knights Landing (KNL) 프로세서의 하드웨어, 소프트웨어적 특성에 대해 설명한다. 3장에서는 인텔 차세대 아키텍처를 효과적으로 활용하기 위한 Advanced Vector Extensions 512 (AVX-512) 명령어 집합을 소개하고, 배정밀도 행렬곱셈루틴인 DGEMM (Double precision GEneral Matrix Multiply) 알고리즘 구현 결과를 바탕으로 최적의 캐시 활용법과 병렬화에 관련된 환경 변수 설정에 대해 설명한다. 마지막 4장에서는 연구 내용을 종합한 결론으로 마무리한다.

2. 인텔 차세대 매니코어 프로세서의 구조

인텔 Xeon Phi Knights Landing (KNL) 프로세서 7250은 68개의 1.4GHz 코어들로 이루어져 있는 매니코어 프로세서 아키텍처이다. 총 34개의 타일이 2D 매쉬 구조로 연결되어 있는 형태이며, 각 타일은 2개의 코어와 4개의 VPU들로 구성되어 있다. 타일 내부의 2개 코어는 개별적으로 32KB 크기의 L1 캐시를 가지고 있으며, 1MB 크기의 L2 캐시를 공유한다. 각 코어에는 2개의 VPU가 있어 32개의 512-bit 벡터 레지스터를 제어하며 각 VPU는 사이클마다 16개의 단정밀도 연산 혹은 8개의 배정밀도 연산을 수행한다.

KNL의 가장 중요한 특징 중 하나는 DDR4 SDRAM과 Multi-Channel DRAM (MCDRAM)으로 구성된 계층적 메모리 구조이다. KNL은 on-package 메모리로 최대 450GB/s의 대역폭을 가지는 16GB 크기의 MCDRAM를 제공하며, platform 메모리로 최대 90GB/s의 대역폭을 가지는 DDR4 SDRAM 6개 슬롯을 제공한다. MCDRAM은 용도에 따라 캐시 모드, 플랫 모드, 하이브리드 모드의 세 가지 메모리 모드로 활용할 수 있다. 본 연구에서는 MCDRAM을 직접적으로 제어하기 위해 플랫 모드로 구동하였다.

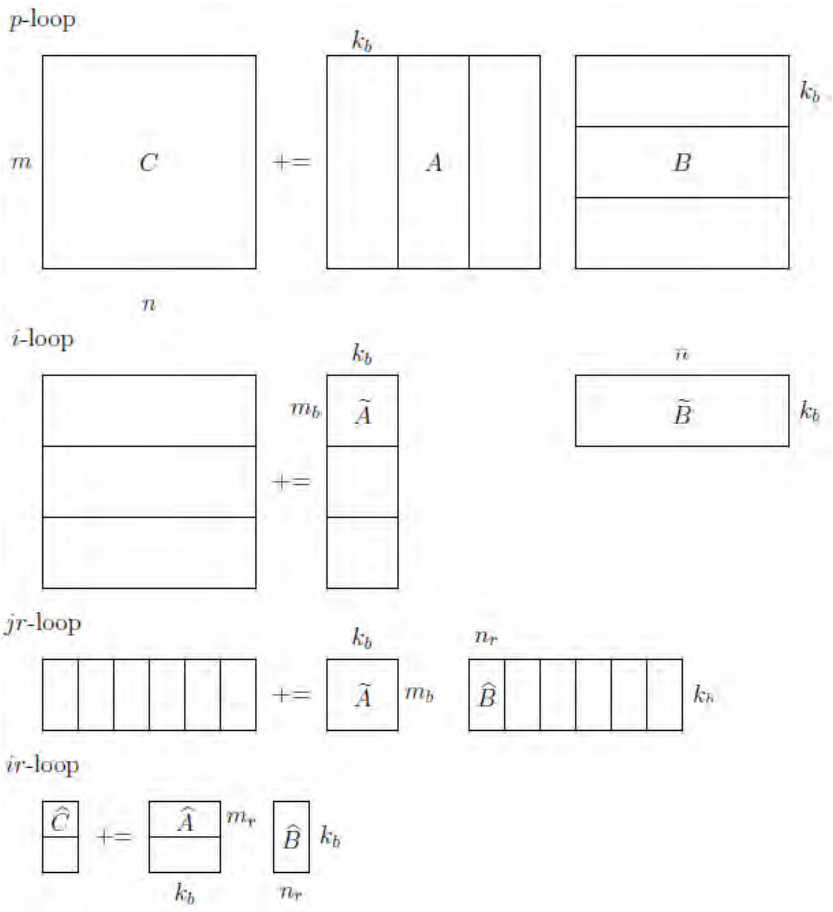
KNL은 독립적으로 부팅가능한 첫 제온 파이 시리즈 프로세서로 CentOS 계열 OS를 지원한다. 본 연구는 CentOS 버전 7.2.1511 (커널 3.10.0-327.13.1)의 OS에서 진행되었다. GEMM 알고리즘의 성능을 비교하기 위해 Intel Math Kernel Library (MKL)과 BLAS-like Library Instantiation Software(BLIS)[8]의 두 BLAS 라이브러리를 활용하였다. MKL 버전은 Intel Parallel Studio XE 2017 Update 1, BLIS 버전은 0.2.2이다.

3. 최적화 방법

본 논문에서는 인텔 차세대 매니코어 프로세서 KNL에서 DGEMM 알고리즘을 구현하고 그 결과를 바탕으로 최적 변수 탐색에 대한 기준을 제시하고 환경 변수 설정과 병렬화 효율성에 대해 설명한다. 분석을 위해 구현한 DGEMM 알고리즘은 배정밀도 밀집행렬간 곱셈 알고리즘으로 바깥 부분의 블록화된 행렬 곱셈 영역와 실제 연산을 수행하는 고효율 내부 커널로 이루어져 있다. 내부 커널은 AVX-512 명령어 집합을 사용

<표 1> Blocked GEMM 알고리즘의 매개변수 설명

매개변수	설명
m	행렬 A, C 의 행 개수
n	행렬 B, C 의 열 개수
k	행렬 A의 열과 행렬 B의 행 개수
k_b	p-loop의 블록킹 매개변수
m_b	i-loop의 블록킹 매개변수
n_r	jr-loop의 블록킹 매개변수
m_r	ir-loop의 블록킹 매개변수



(그림 1) Blocked GEMM 알고리즘

하여 구축하였으며, C 언어를 사용해 블록화된 행렬 곱셈 영역을 구현하였다.

블록화된 행렬 곱셈은 그림 1과 같은 형태로 진행되며, 그림 1에 사용된 매개 변수들은 표 1에 설명되어 있다. 내부 커널은 그림 1의 ir-loop에서 $\hat{C}+=\hat{A}\times\hat{B}$ 연산 부분을 담당한다.

3.1 AVX-512 명령어 집합

KNL은 각 코어의 벡터 레지스터를 조작하기 위해 SSE, AVX 등 여러 명령어 집합를 지원한다. 그 중 Advanced Vector Extensions 512 (AVX-512) 명령어 집합은 가장 강력한 벡터 기반 연산 명령어 집합으로 인텔 Xeon Phi 시리즈와 인텔 Xeon Scalable 프로세서를 포함한 인텔 차세대 아키텍처에서 지원된다. AVX-512 명령어는 어셈블리로 구성된 약간 더 높은 수준의 매크로로, 레지스터 주소를 통한 명시적 할당이 필요한 어셈블리 언어와는 달리 일반적인 변수를 활용할 수 있다. 즉, 일반적인 사용자의 경우 일반적인 함수와 같은 형태로 제공되는 AVX-512 명령어 집합을 활용함으로써 쉽고 빠르게 어셈블리 언어 만큼의 계산 효율을 가져갈 수 있다.

AVX-512 명령어의 기본 연산 단위는 512-bit

길이의 캐시 라인으로 8개의 배정밀도 혹은 16개의 단정밀도 연산이 한 번에 이루어진다. 따라서 AVX-512 명령어를 효과적으로 활용하려면 대상 알고리즘을 512-bit 캐시 라인에 맞게 수정할 필요가 있다. OMP SIMD directive을 통해 컴파일 과정에서 자동으로 SIMD 명령어를 사용할 수 있지만 직접적인 명령어 활용에 비해 그 성능이 떨어지는 모습을 보인다.

AVX-512 명령어 집합에는 단일 곱셈-누산기(Fused multiply-add)를 포함한 일반적인 산술 명령어와 로드, 스토어, 프리패치와 같은 레지스터 조작 명령어가 포함되어 있다. 사용 가능한 명령어와 작동 기작은 인텔 Intrinsic Guide[4]에서 확인할 수 있다. 그림 2는 AVX-512 명령어를 활용한 단일 곱셈-누산 알고리즘이다. 일반적인 C 코드와 같이 벡터 레지스터 변수를 선언하고 AVX-512 명령어를 활용하여 연산을 수행한다. 그림 3은 그림 2의 코드에 의해 실제로 생성되는 어셈블리 코드이다. AVX-512 명령어와 어셈블리 명령어가 일대일로 대응되는 모습을 확인할 수 있다.

AVX-512 명령어를 활용하여 내부 커널을 구성하여 실험한 결과 [6], 어셈블리어로 구현된 인텔 MKL DGEMM 커널에 버금가는 계산 성능을 보일 수 있다.

3.2 레지스터 및 캐시 사용 기준

KNL의 각 코어에는 32개의 512-bit 벡터 레지스터가 존재한다. 레지스터 사용량은 내부 커널의 구조가 결정하는데, $\hat{C} += \hat{A} \times \hat{B}$ 연산에서 레지스터에 $m_r \times n_r$ 크기의 $\hat{C}$와 n_r 길이의 $\hat{B}$의 한 행이 저장된다. 한 벡터 레지스터에는 8개의 배정밀도 수가 저장되므로 레지스터 사용량 num_r은 다음과 같은 식으로 계산할 수 있다.

```
register __m512d a, b, c;
a = _mm512_load_pd(A);
b = _mm512_load_pd(B);
c = _mm512_load_pd(C);
c = _mm512_fmadd_pd(a, b, c);   // c += a * b
_mm512_store_pd(C, c);
```

(그림 2) AVX-512 명령어를 활용한 단일 곱셈-누산 알고리즘

```
vmovaps          256(%rsp), %zmm1
vmovaps          320(%rsp), %zmm2
vmovaps          384(%rsp), %zmm3
vfmadd231pd      %zmm1, %zmm2, %zmm3
vmovaps          %zmm3, 384(%rsp)
```

(그림 3) 그림 2의 코드로 생성된 어셈블리 코드

$$num_r = (m_r + 1) \times \left\lceil \frac{n_r}{8} \right\rceil$$

최적의 레지스터 사용량에 대해서는 전체를 사용해야 한다는 주장과 50%만 사용해야 한다는 주장이 있다. Goto와 van de Geijn[1]은 프리패치시킨 데이터를 저장할 공간을 확보해야 한다는 이유로 50%의 사용을 주장하였다. 반면에 Jaffers et al.[5]은 전체 벡터 레지스터를 활용해야 높은 성능을 얻을 수 있다고 주장하였다. 뿐만 아니라 Heinecke et al.[3]은 이전 세대의 인텔 매니코어 아키텍처 나이츠 코너(KNC)에서 모든 벡터 레지스터를 활용해 내부 커널을 구성하였으며, 그 결과 이론적 최대 성능의 약 90%까지 얻었다. 우리는 KNL에서 위의 모든 경우를 적용하여 커널을 구성하여 실험하였으며, 모두 사용하는 경우에 50%만 사용하는 경우보다 더 좋은 결과를 얻었다[6]. 뿐만 아니라 언롤링을 적용하여 레지스터 사용량을 높일수록 성능이 향상되는 것을 확인하였다.

다음으로 캐시 사용량은 각 캐시에 들어가는 블록의 크기가 결정하는데 L2 캐시의 경우 i-loop의 $\widetilde{A}, \hat{B}, \hat{C}$ 블록들이 들어가며, L1 캐시의 경우 jr-loop의 $\hat{A}, \hat{B}, \hat{C}$ 블록들이 들어간다. 다만 L1 캐시의 경우 캐시 만료가 가능하다는 전제 하에 $\hat{B}$ 블록의 크기만 고려할 수 있으나 KNL의 경우 캐시 만료 명령어를 지원하지 않기 때문에 $\hat{A}, \hat{B}, \hat{C}$ 블록들 모두의 크기를 고려하였다. 즉 L1, L2 캐시 사용량 $usage_{L1}, usage_{L2}$은 다음과 같은 식으로 나타낼 수 있다.

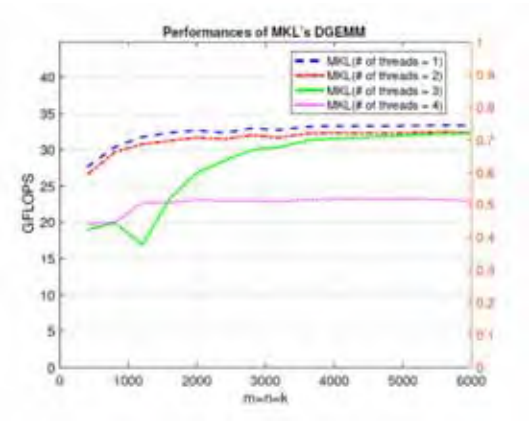
$$usage_{L1} = (m_r \times k_b + n_r \times k_b + m_r \times n_r) \times (8bytes)$$
$$usage_{L2} = (m_b \times k_b + n_r \times k_b + m_r \times n_r) \times (8bytes)$$

캐시 활용 관련 논의의 핵심 쟁점은 크게 두 가지로 좁힐 수 있다. 첫째는 각 레벨 캐시의 최적 사용량 문제이다. Gunnels et al.[2]은 각 캐시 레벨에서 이루어지는 행렬 곱셈의 구성요소 중에서 가장 큰 블록의 크기가 해당 캐시 크기의 대부분을 차지해야 한다고 주장하였다. 반면 Goto와 van de Gejin[1]은 캐시 방출(cache eviction)를 방지하기 위해 가장 큰 블록의 크기가 캐시 크기의 절반 이하가 되어야 한다고 주장하였다. 우리는 실험을 통해 최적의 L2 캐시 사용량을 탐색하였다[6].

다음으로 L1 캐시 블록킹의 효용성에 대한 논의이다. 종래의 블록킹 기법의 경우 모든 캐시 레벨에 대해 블록킹이 이루어지는 것을 기본 전제로 캐시 사용량, 블록의 형태에 대해 논의하였다. 하지만 최근 KNC[3, 7]나 Loongson 프로세서[9]에 대한 연구에 따르면 계산 성능을 충분히 이끌어내기엔 L1 캐시의 크기가 너무 작기 때문에 L1 캐시 블록킹의 효용이 떨어진다고 한다. 실험을 통해 확인한 결과 L2 캐시의 절반정도를 사용하는 것이 가장 효과적임을 확인할 수 있었으며 그 기준은 다음 식과 같다.

$$(m_b \times k_b + n_r \times k_b + m_r \times n_r) \times (8bytes) \approx 512KB$$

싱글 코어 기준 모든 경우 50%(512KB)를 조금 넘어가는 선에서 가장 높은 결과를 얻을 수 있었고, 650KB를 넘어가는 순간 큰 성능 저하가 나타났다. 즉 L2 캐시의 경우 512KB 기준 그 상하범위에서 최적 매개변수를 탐색하는 것이 효과적임을 확인할 수 있었다. 또한 KNL의 경우 L1 캐시 블록킹의 효용성이 떨어지는 모습을 보였다. 매개 변수 조정을 통해 L1 캐시 재활용 횟수를 늘려가며 성능을 측정한 결과 성능이 감소하는 모습을 확인할 수 있었다.



(그림 4) 코어당 쓰레드 생성량에 따른 MKL 성능 테스트

3.3 환경 변수 설정

KNL의 각 코어는 Hyperthreading을 통해 최대 4개의 쓰레드를 생성할 수 있다. 모든 성능을 이끌어내기 위해선 2개 이상의 쓰레드 생성이 필수였던 이전 프로세서 KNC와는 달리 KNL은 코어당 1개, 2개, 4개의 쓰레드만으로도 최대 성능을 이끌어낼 수 있다[5]. 최적의 쓰레드 생성량은 구현하는 알고리즘마다 차이를 보이므로, 구현 과정 중에 최적의 쓰레드 생성량을 확인하는 것이 중요하다. 그림 4는 쓰레드 생성량을 바꿔가며 MKL DGEMM 커널을 테스트한 결과이고, 다음과 같은 환경 변수를 이용하여 쓰레드 생성을 조절하였다.

```
$ export KMP_AFFINITY = COMPACT
$ export KMP_HW_SUBSET =
‘1C,nT’ with n=1,2,3,4
```

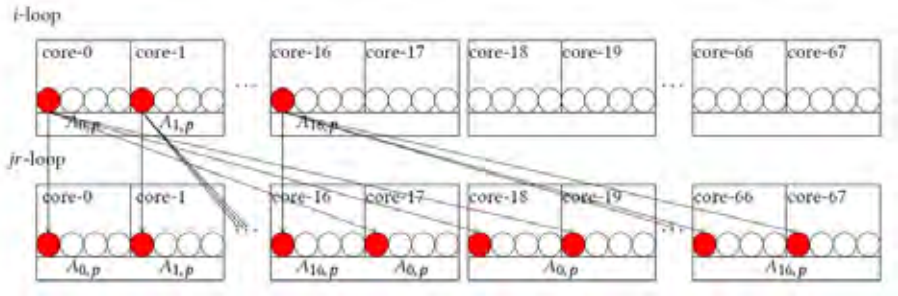
그 결과 MKL DGEMM 커널의 경우 쓰레드 1개만으로도 가장 높은 성능을 얻었다. 이러한 결과를 바탕으로 쓰레드 생성량 기준을 코어당 1개로 하고 DGEMM 알고리즘을 구현하였으며, 최적화 과정 단계마다 최적의 쓰레드 생성량을 확인하였다.

본 연구에서 구현한 DGEMM 알고리즘의 주된 병렬 구간은 i-loop와 jr-loop으로 구성된 nested loop이다. Nested 병렬 구간의 경우 쓰레드를 물리적 코어에 할당하는 방식에 따라 그 병렬화 성능이 크게 변한다. 특히 KNL의 경우 타일 기반 구조로 1MB 크기의 L2 캐시를 한 타일의 두 코어가 공유하는 형태이므로 환경 변수 설정에 보다 민감하다.

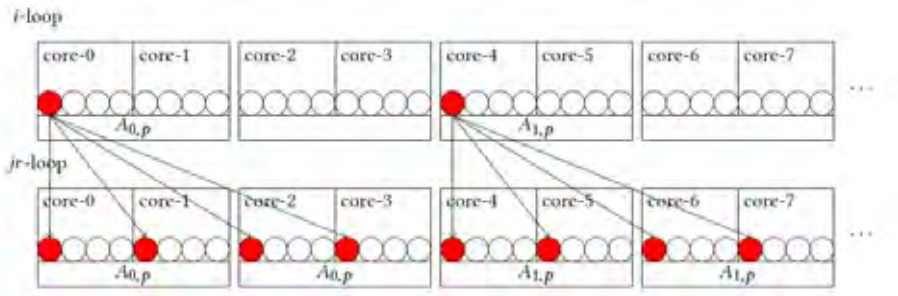
```
$ export KMP_AFFINITY = SCATTER
$ export OMP_PLACES = CORES
```

KNL에서는 다음의 두 환경 변수를 이용하여 쓰레드를 할당한다. KMP_AFFINITY 환경 변수는 OMP_PLACES 환경 변수에 우선하여 적용된다. 만약 두 환경 변수가 동시에 선언될 경우 KMP_AFFINITY 환경 변수 설정에 따라가게 된다. 먼저 KMP_AFFINITY는 인텔 OpenMP 런타임 라이브러리에서 제공하는 환경 변수로 쓰레드를 물리적 코어에 할당하는 부분을 제어한다. 일반적으로 KMP_AFFINITY=SCATTER로 설정하며, 이 경우 각 쓰레드는 최대한 떨어져서 할당되며 모든 코어에 할당되기 전에는 한 코어에 다중으로 할당되지 않는다. 즉 68개의 쓰레드를 생성하면 68개의 코어에 각각 1개씩의 쓰레드가 할당되며, 이후 추가로 생성하는 쓰레드는 앞서 68개의 코어에 할당된 순서를 따라 할당된다.

다음으로 OMP_PLACES는 OpenMP Affinity에서 제공하는 환경변수로 마찬가지로 쓰레드 할당을 담당한다. OMP_PLACES=“{0:8:1}”과



(그림 5) KMP_AFFINITY=SCATTER 환경에서의 작업 분배



(그림 6) OMP_PLACES=CORES 환경에서의 작업 분배

같이 명시적으로 할당하거나 OMP_PLACES=CORES와 같이 미리 정의된 규칙을 활용할 수 있다. OMP_PLACES=CORES로 설정할 경우에는 쓰레드를 코어마다 할당하게 된다. 즉 KMP_AFFINITY=SCATTER 설정과 마찬가지로 68개의 쓰레드를 생성하면 68개의 코어에 각각 1개씩의 쓰레드가 할당되게 된다.

68개의 쓰레드를 생성할 경우 KMP_AFFINITY=SCATTER와 OMP_PLACES=CORES가 동일한 CPU map을 갖는 것처럼 보이지만 내포 병렬 구간의 작업 분배에 있어 이 둘은 큰 차이가 있다. 그림 5는 KMP_AFFINITY=SCATTER 환경에서 작업 분배 형태를, 그림 6은 OMP_PLACES=CORES 환경에서 task 분배 형태를 각각 도식화한 그림이다.

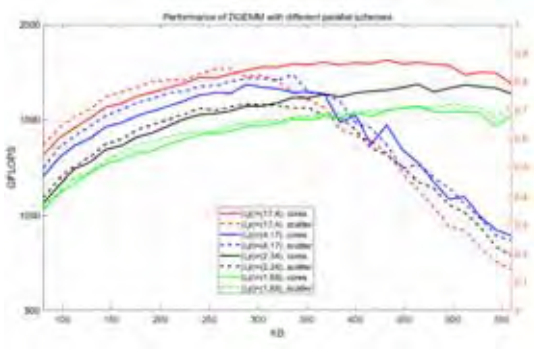
KMP_AFFINITY=SCATTER의 경우 내포 병렬 구간의 바깥 루프인 i-loop에 할당한 쓰레드 개수만큼의 타일에서 작업 수행에 서로 다른 $\widetilde{A}$ 블록을 요구하게 된다. 이러한 작업 분배 방식은 L2 캐시를 비효율적으로 활용하게 하며, 성능 저하를 일으키는 원인이 된다. 반면 OMP_PLACES=CORES의 경우 모든 타일에서 그 내부의 두 코어는 같은 $\widetilde{A}$ 블록을 공유하여 작업을 수행한다. 이 경우 두 코어가 같은 $\widetilde{A}$ 블록을 공유함으로써 타일 내부의 L2 캐시를 보다 효율적으로 활용할 수 있게 된다. 다만 jr-loop에 홀수 개의 쓰레드를 할당한다면 적어도 2개의 타일에서 서로 다른 $\widetilde{A}$ 블록을 요구하게 되어 L2 캐시의 공유 환경을 깨트리게 된다.

본 실험에서는 병렬화 조합 $(i, jr) = (17,4)$, $(4,17)$, $(2,34)$, $(1,68)$에 대해 KMP_AFFINITY=SCATTER, OMP_PLACES=CORES 환경

에서 실험하였으며 고정된 크기의 행렬 곱셈에서 매개변수 k_b만을 변경시키면서 DGEMM 커널의 병렬화 성능을 테스트하였다. 앞서 언급한 바와 같이 다른 변수들이 고정되어 있을 경우 k_b가 L2 캐시 사용량을 결정하게 된다. 따라서 k_b에 따른 성능 변화를 관찰함으로써 각 환경 설정에 따른 L2 캐시 사용 양상을 확인하였다. 실험 결과는 그림 7과 같다. 실선은 OMP_PLACES=CORES 환경에서의 결과이며 점선은 KMP_AFFINITY=SCATTER 환경에서의 결과이다.

먼저 병렬 조합 $(i,jr)=(17,4),\ (2,34)$의 경우 앞서 설명한 바와 같이 OMP_PLACES=CORES 환경에서 L2 캐시를 보다 효율적으로 활용하는 모습을 확인할 수 있다. KMP_AFFINITY=SCATTER 환경에서는 $k_b=256$ 근처에서 가장 좋은 성능을 보이고 이후 성능이 크게 감소하였으나 OMP_PLACES=CORES 환경에서는 $k_b=432$ 근처에서 가장 좋은 결과를 얻었으며 피크 이후 성능 감소도 완만한 모습을 보인다.

반면 병렬 조합 $(i,jr)=(4,17),\ (1,68)$의 경우 두 환경에서의 결과가 크게 차이나지 않다는 것을 확인하였다. 먼저 $(i,jr)=(4,17)$의 경우 jr-loop에 홀수 개의 쓰레드가 할당된 상황이다. 앞서 언급한 바와 같이 이러한 경우 2개의 타일에서 서로 다른 $\widetilde{A}$블록을 요구하게 되며, 이는 L2 공유 환경을 해치게 된다. 이 경우 $\widetilde{A}$ 블록 공유 문제가 전체 34개의 타일 중 단 2개에서만 일어났음에도 불구하고 전체 성능에 큰 영향을 끼쳤다. 따라서 내포 구간 병렬화에 있어 쓰레드 할당에 주의하여야 한다. 다음으로 $(i,jr)=(1,68)$로 쓰레드를 할당할 경우 내포 구조가 아니므로 동일한 CPU map을 바탕으로 작업이 분배된다. 따라서 두 환경 사이의 양상이 동일한 모습을 보인다.



(그림 7) 병렬 조합 및 환경 설정에 따른 병렬 성능 비교

4. 결 론

본 논문에서는 AVX-512를 활용하여 구현한 배정밀도 밀집행렬곱셈 알고리즘(DGEMM)을 통해 인텔 차세대 매니코어 프로세서인 나이츠 랜딩(KNL)의 특성을 파악하였다. 그리고 이를 바탕으로 레지스터 및 캐시 활용과 환경 변수 설정에 관한 최적화 방법을 제시하였다. 내부 커널 실험 및 캐시 블록킹 테스트를 통해 KNL에 알맞은 레지스터 및 캐시 활용의 기준을 유도하였다. 이러한 기준을 바탕으로 알고리즘의 설계 및 최적화 과정에서 보다 효율적으로 매개변수를 탐색하고 결정할 수 있을 것이다. 또한 여러 환경 변수에 대한 분석과 테스트를 통해 내포 병렬 구간을 보다 효과적으로 병렬화하기 위한 환경을 제시하였다. 대부분의 과학 계산 알고리즘에 내포 병렬 구간이 존재하는 만큼 보다 효과적인 병렬화가 가능하게 된다. 2017년 3분기에 출시된 Intel Xeon Skylake Scalable Processors도 AVX-512 명령어를 지원하기 시작하였고, 앞으로 출시되는 인텔 프로세서들에서도 이를 활용하여 보다 효과적인 프로그래밍이 가능할 것이다.

감사의 글

본 연구는 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행되었습니다(No. R0117-17-0001).

참 고 문 헌

[1] Goto, K., van de Geijn, R.A. “Anatomy of high-performance matrix multiplication”, ACM Transactions on Mathematical Software (TOMS) 34(3), 12 (2008)

[2] Gunnels, J.A., Henry, G.M., Van De Geijn, R.A. “A family of highperformance matrix multiplication algorithms.”, In: International Conference on Computational Science, pp. 51-60. Springer (2001)

[3] Heinecke, A., Vaidyanathan, K., Smelyanskiy, M., Kobotov, A., Dubtsov, R., Henry, G., Shet, A.G., Chrysos, G., Dubey, P. “Design and implementation of the linpack benchmark for single and multi-node systems based on Intel Xeon Phi Coprocessor” In: Parallel & Distributed Processing (IPDPS), 2013 IEEE 27th International Symposium on, pp.126-137. IEEE (2013)

[4] “Intel Intrinsics Guide.” Software.intel.com. (2018). [online] Available at: https://software.intel.com/sites/landingpage/IntrinsicsGuide/ [Accessed 22 Mar. 2018].

[5] Jeffers, J., Reinders, J., Sodani, A.: Intel Xeon Phi Processor High Performance Programming: Knights Landing Edition. Morgan Kaufmann (2016)

[6] Lim, R., Lee, Y., Kim, R., Choi, J. “An Implementation of matrix-matrix multiplication on the Intel KNL processor with AVX-512.” In: Cluster Computing (Submitted)

[7] Peyton, J.L. “Programming dense linear algebra kernels on vectorized architectures.” Master's thesis, The University of Tennessee, Knoxville (2013)

[8] Van Zee, F. G., van de Geijn, R. A. “BLIS: A Framework for Rapidly Instantiating BLAS Functionality” In: ACM Trans. Math. Softw., 41(3), pp.1-33. ACM (2015)

[9] Xianyi, Z., Qian, W., Yunquan, Z. “Model-driven level 3 BLAS performance optimization on Loongson 3A processor” In: Parallel and Distributed Systems, 2012 IEEE 18th International Conference, pp. 684-691. IEEE (2012)

저 자 약 력

최 재 영

이메일 : choi@ssu.ac.kr

- 1984년 서울대학교 제어계측공학과 (공학사)
- 1986년 미국 남가주대학교 전기공학과 (석사)
- 1991년 미국 코넬대학교 전기공학부 (박사)
- 1992년 1월~1994년 2월 미국 국립 오크리지연구소 연구원
- 1994년 3월~1995년 2월 미국 테네시 주립대학교 연구교수
- 1995년 3월~현재 숭실대학교 컴퓨터학부 교수
- 관심분야 : HPC 컴퓨팅, 시스템 소프트웨어, 로봇 미들웨어

김 래 현

이메일 : Kim.rh3169@gmail.com

- 2016년 서울대학교 수학교육과 (학사)
- 2016년 서울대학교 계산과학 연합전공 (학사)
- 2018년 서울대학교 수리과학과 (석사)
- 2018년~현재 숭실대학교 연구원
- 관심분야 : 계산 과학, 수치 해석, 수치 선형대수, 알고리즘

임 록 택

이메일 : rokt.lim@gmail.com

- 2007년 서울대학교 물리천문학부 천문학전공 (학사)
- 2014년 서울대학교 협동과정 계산과학전공 (박사)
- 2014년~2015년 서울대학교 박사 후 연구원
- 2015년~2016년 Nanyang Technological University, 연구원
- 2016년~현재 숭실대학교 연구원
- 관심분야 : 수치해석, 유한요소해법, 고성능계산

특집 02

매니코어 시스템에서의 병렬 프로그래밍 최적화를 위한 분석 도구 및 벤치마크 성능 실험

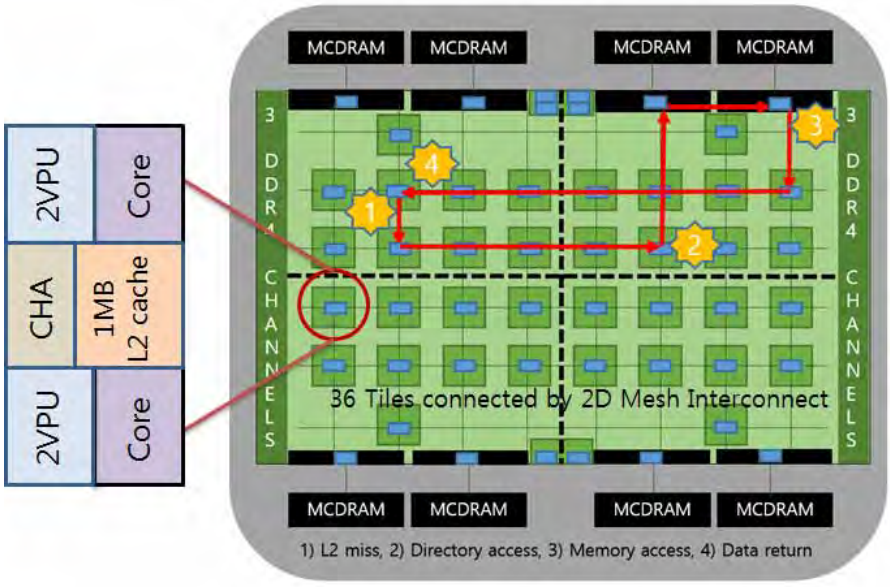
노승우 · 최지은 · 남덕윤 · 박근철 · 박찬열 (한국과학기술정보연구원)

목 차

1. 서 론

슈퍼컴퓨터는 하드웨어적으로 크게 컴퓨팅, 스토리지, 인터커넥트 부분으로 구분하여, 해당 성능을 높이는 데에 집중한다. 슈퍼컴퓨터를 구축하는 데에 있어서 클러스터 형태가 주류가 된 이후, 스토리지 및 인터커넥트의 성능 향상에 비해 컴퓨팅 부분의 성능 향상은 발전이 더딘 상황이었다. 이는 컴퓨팅 성능이 프로세서 성능 발전과 함께 이루어져 왔기 때문이다. 프로세서의 성능, 즉 반도체 집적회로 성능의 발전은 무어의 법칙으로 이야기하듯이 18개월에서 24개월마다 두 배씩 증가해 왔으나, 몇 년 전부터 무어의 법칙이 더 이상 지켜지기 힘들 것이라는 소식이 들려왔다. 이러한 이유는 고집적을 위한 비용의 증가, 고밀도에 따른 발열, 선로 선폭 및 회로 간격의 감소로 인한 데이터 간섭 현상 발생 가능성 등 다양한 현상들 때문이었다. 또한 멀티코어 성능 향상의 한계는 몇 해 전부터 단일 CPU의 클럭 속도가 3GHz에서 더 이상 향상되지 않고 있는 점에서 어느 정도 예상되던 부분이었다. 이러한 상황에서 컴퓨팅 성능은 프로세서의 클럭 속도 향상이 아닌, 인텔 제온파이나 NVIDIA GPU와 같이 별도 카드 타입의 가속기 형태가 나옴으로서 향상을 꾀할 수 있었다.

최근의 프로세서 성능 향상 방법은 멀티코어에서도 그렇게 해 왔지만 매니코어의 방식으로 (비록 클럭 속도가 낮은 코어이기는 하지만) CPU 내 코어 수를 늘리고, 프로세서 패키지 내에 추가적인 메모리를 부착하는 형태로 이루어지고 있다. 인텔에서는 2016년에 매니코어 프로세서인 나이츠랜딩 (Knights Landing; KNL)을 가속기 타입이 아닌 호스트 프로세서 타입으로 출시했다. 여기에서 우리는 앞으로 고속 메모리를 프로세서 패키지 안에 포함한 형태의 프로세서를 자주 보게 될 것으로 예상된다. 이는 '레지



(그림 1) KNL 프로세서의 하드웨어 구조 및 Quadrant 모드 캐시 미스 라우팅[2]

스터-캐시-메모리-디스크'의 저장 매체 계층이 캐시와 메모리 사이에 위치하는 온-패키지 메모리 또는 고대역폭 메모리라 불리는 고속 메모리가 위치하여 '레지스터-캐시-고대역폭 메모리-기존 메모리'의 계층 구조가 된다는 의미이다. 결국 슈퍼컴퓨터와 같이 컴퓨팅 요소의 모든 부분을 최적화하고 고속화하고자 하는 분야에서는 고속 메모리가 추가로 들어간 프로세서를 제대로 분석하고, 활용할 수 있어야 한다.

이에 본고에서는 고속 메모리가 추가된 인텔 KNL을 간략히 소개한 후, 병렬 프로그래밍을 위한 최적화된 환경을 분석하기 위해 활용하는 성능 모니터링 방법과 주요 분석 도구에 대해서 설명한다. 그리고 KNL 기반의 시스템 테스트베드를 활용하여 주요 벤치마크 실험을 실행하고 성능을 측정한다. 이를 통해 KNL 고속 메모리 크기와 코어 수, 스레드와 MPI 프로세스 수의 조합 등이 병렬 프로그램 성능에 끼치는 영향을 살펴보고 분석한다.

2. 매니코어 시스템

대표적인 매니코어 시스템인 인텔 제온파이 시스템은 매우 많은 수의 코어와 하드웨어 스레드 구조 때문에 기존의 프로세서와는 다른 특징을 가진다. 즉, 지금까지는 적은 수의 크고 정교한 코어를 만드는 방식이었다면, 반대로 제온파이는 더 많은 수의 단순한 코어를 만드는 접근 방식을 채용했다. 이러한 아이디어는 트랜지스터의 대부분이 산술 연산에 사용될 수 있다는 점에 착안했다. 이 접근법으로 제 1세대인 나이츠 코너(Knights Corner, KNC)를 시작으로, 2016년 제2세대인 나이츠 랜딩(Knights Landing, KNL)이 공식 출시되었다. KNL CPU는 KNC와 달리 AVX2 명령어 셋 확장을 통해 완전히 인텔 제온 ISA(Instruction Set Architecture)와 호환이 가능해졌기 때문에, 독립적으로 운영체제를 실행할 수 있다[1,2].

2.1 시스템 구조

KNL 플랫폼은 코프로세서, 호스트프로세서, 전용 통합 네트워크(옴니패스)를 가진 호스트프로세서의 총 3가지 유형을 가진다. 프로세서 구조는 1개의 타일 당 1MB의 L2 캐시를 공유하는 2개의 코어와 캐시 동기화를 위한 Cache/Home Agent(CHA)로 구성되며, 각 타일은 2D 메시 구조로 최대 36개 타일을 이룬다. 한 코어는 1.3~1.4GHz의 클럭 속도로, 최대 동시 4개의 멀티쓰레딩(4 SMT)을 지원하며 2개의 AVX-512 벡터 처리 장치(Vector Processing Unit)를 가지고 있다. 메모리 구조는 8개의 고속 메모리 컨트롤러에 의해 접근되는 16GB 고대역폭 메모리(High Bandwidth Memory, HBM)와 2개의 3채널 메모리 컨트롤러에 의해 접근되는 최대 384GB의 DDR4 메모리로 구성된다. I/O 구조는 36개의 PCIe 선로와 추가적인 옴니패스(omnipath) 컨트롤러로 구성된다. 옴니패스는 인텔 전용 고속 네트워크 구조로 최대 100 Gb/s의 속도를 보장한다.

2.2 메모리 구조

KNL의 고대역폭 메모리(HBM)인 MCDRAM (Multi-Channel Dram)은 flat, cache, hybrid 형태의 3가지의 다른 모드로 사용할 수 있다. flat 모드는 MCDRAM이 별도의 물리적 공간을 가지도록 하며, DDR4와는 별도로 원하는 데이터를 저장할 수 있다. 이 모드는 가장 높은 대역폭과 가장 작은 지연시간을 제공하는 반면, 효과적으로 사용하기 위해 응용 프로그램의 수정이 필요할 수 있다. cache 모드는 MCDRAM을 L3 캐시로 사용할 수 있어, 응용프로그램의 수정이 필요 없다. 단점은 캐시 미스가 발생했을 때 데이터가 크면 클수록 지연이 커진다. hybrid 모드는 cache 모드와 flat 모드를 혼합하여 사용한다. 적합한 설정방법은 전체 응용프로그램의 크기와 데이터의 수정, 분리 유무에 따라 적절하게 설정한다.

2.3 캐시 클러스터링 모드

KNL의 각 타일 내의 모든 L2 캐시는 MESIF 프로토콜을 사용하는 메시에 의해 일관성있게 유지된다. 메시의 수직 및 수평 링크는 양방향 링크이며, 각 타일은 캐시 동기화를 위해 캐시 라인의 칩 상태와 위치를 식별하는 분산된 태그 디렉토리(Tag Directory, TD)를 가지고 있다. 이러한 캐시 동기화의 복잡성을 관리하고 주어진 계산 응용 프로그램에 대해 최적의 작동 모드를 설정하기 위해 KNL은 물리 메모리 주소 매핑 방법에 따라서 All2All, Quadrant/Hemisphere, SNC(Sub-NUMA-Clustering)의 3가지 클러스터링 모드를 제공하며, 이중 하나에서 작동한다. 이러한 모드는 바이오스나 인텔에서 제공해주는 명령어를 통해 콘솔에서 변경 가능하지만, 적용을 위해서는 시스템 재시작이 필요하다.

All2All 모드는 타일, TD, 메모리 채널 사이에 의존성이 없어, 메모리 주소가 칩의 모든 TD에 균일하게 분산되기 때문에 가장 지연이 크다. Quadrant/hemisphere 모드는 가상의 4개 또는 2개 부분으로 나뉘어지고, 메모리 주소가 같은 부분의 TD로 해시된다. 즉, 같은 위치에 TD와 메모리 채널이 위치하기 때문에 All2All 모드에 비해 더 높은 성능을 가진다. SNC 모드는 2개(SNC2) 또는 4개(SNC4)의 사분면을 모두 가상 NUMA 클러스터로 나타내어, 2 또는 4 소켓 제온 서버처럼 보이게 한다. 이 모드는 타일, TD, 메모리 채널이 모두 같은 소켓에 위치하므로 가장 좋은 성능을 보인다. 하지만 캐시 트래픽이

NUMA 경계를 넘는 경우에는 Quadrant /Hemisphere 모드를 사용하는 것보다 효율적이지 않다. (그림 1)은 가장 많이 사용되는 Quadrant 모드에서의 캐시 미스 라우팅 상황을 보여준다.

3. 성능 분석 도구

3.1 성능 모니터링

제온파이 프로세서의 성능 모니터링은 하드웨어 퍼포먼스 유닛(Hardware Performance Units)을 사용하여 많은 정보를 얻을 수 있다. 하드웨어 퍼포먼스 카운터(Hardware Performance Counter)는 하드웨어 관련 이벤트를 수집하는 레지스터로 프로세서의 성능 모니터링 시 사용된다. 하드웨어 퍼포먼스 카운터에서 수집 가능한 성능 관련 이벤트들은 크게 타일(Tile) 이벤트와 언타일(Untile) 이벤트로 나누어진다. 타일 모니터링은 타일 내의 Core, VPU, 캐시 관련된 이벤트를 집계(Counting)하고, 언타일 모니터링은 타일 밖의 요소들과의 통신 및 메모리, 캐시 관련 이벤트를 대상으로 진행된다. <표 1>은 KNL 프로세서의 하드웨어 퍼포먼스 카운터(HPC) 주요 이벤트를 보여준다.

3.2 분석 도구

리눅스 커널 2.6 이상에서는 하드웨어 퍼포먼스 카운터를 이용한 성능 분석을 위해 Perf[5]를 제공한다. Perf를 이용하면 성능 관련 이벤트에 대한 추적(tracing)과 집계가 가능하다. PAPI (Performance Application Programming Interface)[6]는 주로 사용자가 직접 실행 프로그램을 최적화를 할 때 코드 삽입(Instrumentation)의 형태로 하드웨어 퍼포먼스 카운터를 프로파일링 한다. 이외에도 Intel Vtune[7], ARM HPC tools(과거 Allinea)[8], Oregon 대학에서 개발한 TAU[9] 등이 하드웨어 퍼포먼스 카운터를 이용하는 주요 성능 분석 도구이다. 이들은 사용자를 위해 응용 프로그램 실행부터 결과 분석까지 하나의 그래픽 인터페이스를 제공하고 분석 결과 시각화 툴을 포함하기도 한다.

인텔의 Vtune은 고성능 분석(HPC analysis)을 위해 CPU Utilization, memory access, FPU Utilization의 3가지 주요 지표의 분석 결과를 제공한다. Vtune은 대부분의 최신 프로세서까지 지원하기 때문에 단일 인터페이스로 다양한 프

<표 1> KNL 프로세서의 HPC 이벤트[3,4]

HPC 이벤트 유형		주요 이벤트
Tile		Unhalted reference clock cycles, Retired Instructions, L1 and L2 Hit/Miss Loads, Branch−*, DTLB / UTLB−*, L2Q−*
Untile	EDC	EDC Hit/Miss, MCDRAM Clock(ECLK), All read/wire request in MCDRAM cache (RPQ, WPQ),
	MC	DDR4 clock(DCLK), Memory controller −*: Column Access Strobe(CAS)
	CHA	IPQ−*, IRQ−*, ISMQ−*, RxR−*, TOR−*, Transgress−*, TxR−*
	CMS	Agent0−*, Agent1−*
	M2PCIe	RxR−*, TxC−*
	IRP	Outbound request queue−*, Write cache occupancy, Coherent Ops.

로세서의 성능 분석을 진행할 수 있다는 점이 장점이다.

ARM의 HPC tools은 성능 분석을 통해 실행 프로그램의 병목지점 추적을 돕는다. 또한 시스템에서 실행된 프로그램의 계산, 통신, I/O 연산 결과를 분석하여 보고서(Arm Performance Reports[10]) 형태로 제공하는 것이 특징이다.

TAU의 경우 routines, loops과 메모리 관련하여 소스 코드에 삽입하여 성능 분석하기에 유용하고, 하드웨어 성능 카운터를 프로파일링하여 각 routine들의 소요 시간을 분석한다. TAU의 수많은 시각화 툴은 사용자들이 다양한 성능 분석 결과를 얻을 수 있도록 한다.

4. 주요 벤치마크 성능 실험 및 분석

슈퍼컴퓨터의 성능을 측정하기 위한 다양한 시스템 벤치마크 프로그램들이 존재한다. 본 장에서는 대표적으로 가장 널리 사용되는 벤치마크 프로그램인 STREAM, HPLinpack, HPCG를 대상으로 KNL 기반 테스베드 성능 측정 결과를 비교하고 분석해 본다.

4.1 테스트베드 구성

사용한 테스트베드는 1대의 로그인 노드와 총 14대의 계산 노드로 구성되어 있다. 이중 10대의 계산 노드는 인텔 제온파이 프로세서 7250 기반으로 관련 상세 스펙 및 소프트웨어, 환경설정, 및 사용한 벤치마크는 <표 2>와 같다.

4.2 STREAM 벤치마크

가장 기본적으로 널리 사용되고 있는 메모리 성능 벤치마크 프로그램으로, 초기 버전은 1991년 Texas Advanced Computing Center(TACC)의 John D. McCalpin에 의해 개발되었다[11]. 그는 STREAM 벤치마크를 “지속가능한 메모리 대역폭(MB/s)과 단순한 벡터 커널(Copy, Scale, Add, Triad) 계산을 수행하고 측정하기 위한 단순한 종합 벤치마크 도구”라고 정의한다[12]. 인텔 STREAM 최적화 공식 문서에 따르면 KNL 7250의 Quadrant, Flat 모드에서 STREAM Triad 기대 성능은 MCDRAM 최대 475 ~ 490 GB/s, DDR4 최대 90 GB/s 이다. 본 절에서는 인텔 최적화 문서[13]에 따른 기대 성능과 실제

<표 2> 제온파이 기반 테스트베드 환경설정

하드웨어	
플랫폼	Intel S7200AP
프로세서	Intel XeonPhi 7250 1.40GHz, 68C
가용 메모리	13 of 16 GB (MCDRAM), 90 of 96 GB (DDR4)
네트워크	Intel Omni-Path 100GB/s

소프트웨어	
운영체제	CentOS 7.3
커널	3.10.0-514.26.2.el7.x86_64
스케줄러	PBS v14.2
파일시스템	Lustre v2.7

환경설정	
메모리 모드	Flat Mode
클러스터 모드	Quadrant

벤치마크	
STREAM	v5.10
HPLinpack	Intel Optimized HPL v2.1 Netlib HPL v2.2
HPCG	Intel MKL 2018(HPCG v3.0)

성능을 검증 해보고 CPU와 메모리 크기의 변화에 따른 성능 결과를 비교하고 분석한다.

본 벤치마크는 메모리 대역폭 점수 결과 인용을 위해 개발자가 정의한 실행규칙을 따르는 표준 버전과 사용자 또는 공급 업체가 수정 된 소스 코드를 기반으로 결과를 제출하는 비표준(튜닝) 버전의 두 가지 범주로 나뉜다. 표준 버전에서 STREAM의 배열 요소 크기는 일반적으로 사용가능한 마지막 레벨 캐시(Last Level Cache, LLC) 메모리 크기의 4배 이상이거나 10 MB 중 큰 값이어야 한다[13]. STREAM 표준에 따라 L2 캐시를 LLC로 고려하였을 때, KNL 7250의 각 배열 크기 요소를 계산해보면, 배열이 더블 타입(8byte) 이므로, 34MB * 4 / 8 = 17,000,000 이 되며, 각 배열 당 메모리 크기는 136 MB로 A,B,C 세 배열 전체가 차지하는 메모리 크기는 408 MB 이다. 그리고 MCDRAM을 LLC로 사용한다면, 각 배열 크기 요소는 16GB * 4 / 8 = 8,000,000,000, 각 배열당 메모리 크기는 64 GB, 전체 메모리 크기는 192 GB가 된다.

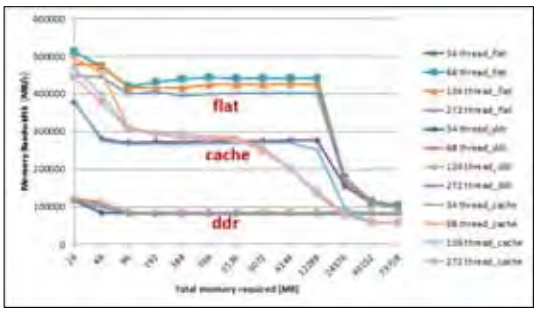
본 실험에서는 STREAM의 최신 표준 공식 버전인 5.10을 이용하였으며, 4가지 벡터 커널 중 가장 복잡한 시나리오인 Triad 커널 계산을 이용하여 실험을 진행하였다. Triad는 복사(Copy, a=b), 곱셈(Scale, a*SCALAR), 덧셈(Add, a+b)가 모두 적용된 벡터 커널로 위의 <표 3>과 같다.

STREAM 벤치마크의 구현 버전은 일반적으로 C와 Fortran의 2가지 버전이 존재하며, 여기서는 C 버전과 인텔 버전의 컴파일러(ICC)를 사용하였다. 인텔에서 권고되는 STREAM 최적화 문서를 기준으로, 정적 메모리 할당, 2MB의 메모리 정렬, 그리고 컴파일러 옵션을 사용한다[12]. 그리고 메모리 모드(cache, ddr, mcdram), STREAM 배열 크기(STREAM_ARRAY_SIZE)와 스레드 개수(OMP_NUM_THREADS)가 성능에 미치는 영향을 살펴보기 위해 각 요소의 변화에 따른 성능 결과를 측정하였다. 이 때, 이용가능한 모든 코어 위에서 스레드가 실행되도록 OpenMP 환경변수인 KMP_AFFINITY를 scatter로 설정한다. 실험 결과는 (그림 2)와 같다.

<표 3> STREAM Triad 벡터 커널

```
#pragma parallel for
    for (i =0; i<N; i++) {
    a[i] = b[i] + c[i] * SCALAR;
 }
```

본 실험에서 벡터의 배열 크기를 최소 1,000,000 부터 최대 3.072,000,000 까지 제곱하여 증가시켰을 때, 전체 할당 메모리 크기는 약 24 MiB 부터 73,728 MiB 이다. 이때 소모되는 전체 메모리 크기가 34 MiB 와 16 GiB 일 때 큰 폭으로 성능이 두 단계 떨어짐을 확인할 수 있다. 그 이유는 모든 코어의 L2 캐시 합의 크기가 34 MiB 이기 때문에 모든 백터 크기가 L2 캐시의 크기보다 클 때 성능이 한번 떨어지며 이후에 MCDRAM의 크기인 16 GiB 보다 클 때 또 한번 성능이 떨어진다. 실험 결과를 살펴보면 먼저 각 메모리 모드는 ddr < cache < flat, 스레드 개수는 34 < 272 < 136 < 68 순으로 성능이 높



(그림 2) STREAM(Triad) 벤치마크를 사용한 메모리 대역폭 비교 실험

아짐을 확인할 수 있다. 즉, flat 모드 68 스레드의 경우 표준 성능이 약 450,000 MB/s로 가장 높고, cache 모드 68 스레드의 표준 성능은 약 260,000 MB/s, ddr 모드 68 스레드의 표준 성능은 약 85,000 MB/s로 위에서 언급한 기대 성능치와 거의 비슷하다.

4.3 Linpack 벤치마크

Linpack 벤치마크는 분산 메모리 컴퓨터에서 무작위 계수를 갖는 선형 대수 방정식의 대규모 시스템을 생성하고 해결하기 위해 1980년대 초 Jack Dongrra 등에 의해 개발되었다[14]. 즉, 선형 방정식 Ax * b의 조밀한 n * n 시스템을 풀고, 시스템을 분석하고 해결하는데 걸리는 시간을 측정하고, 그 시간을 성능 속도로 변환하고 결과의 정확성을 테스트한다. 이때 시스템의 성능은 초당 부동소수점 연산(FLOP/s)으로 표현된다.

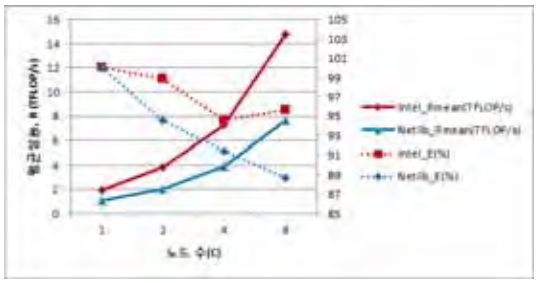
본 벤치마크의 최신버전인 HPLinpack은 결과를 표준화하기 위해 이식 가능한 구현체로서의 소프트웨어 패키지인 HPL 코드가 사용된다[15]. 본 코드는 실제 병렬 고성능 컴퓨팅 시스템(HPC)의 부동 소수점 연산의 성능 측정을 위한 산업 표준 테스트로, 세계에서 가장 강력한 컴퓨터 시스템의 목록을 정기적으로 업데이트하는 TOP 500 프로젝트의 기준으로 활용되고 있다. 본 절에서는 제온파이 테스트베드를 기반으로 인텔에서 소스 최적화한 HPLinpack 벤치마크와 기존 Netlib의 HPLinpack를 이용하여 단일 노드 및 클러스터 환경에서의 성능을 측정하고 비교 분석한다.

HPL은 HPL.dat라는 입력 텍스트 파일을 통해서 사용자가 벤치마크 매개변수를 조정하고, 인수분해 알고리즘을 선택할 수 있다. 이 중 성능에 가장 크게 영향을 미치며 중요한 매개변수인 N, NB, P와 Q에 초점을 맞추고 나머지 매개변수는 기본 값을 유지한다. 여기서 N은 문제크기이며, HPL에 의해 사용되는 메모리 크기를 나타낸다. 이 값은 최대한 메모리 크기에 맞추는 것이 적절하나, 시스템 프로그램 등의 필수 사용 메모리를 제외하고, 일반적으로 전체 사용가능한 메모리의 약 80% 정도로 할당하는 것을 추천하며, NB는 분배되는 데이터의 블록 크기로 인텔에서는 제온파이 프로세서에 최적화된 값으로 336을 제시한다[16]. P와 Q는 분산되어지는 격자의 프로세스 행과 열의 수를 나타내며, P와 Q의 곱은 MPI 프로세스의 수와 같아야 한다. P와 Q값은 서로 같거나 Q값이 크고, 보통 두 값의 차이가 적을수록 성능이 좋다.

본 실험은 인텔에서 최적화한 정적 메모리 HPL 코드와 코드 수정을 하지 않은 기존 Netlib HPL 소스에 인텔 컴파일러 최적화만을 실시하였다. 두 코드는 단일 노드에서는 공유 메모리 형태의 272개의 스레드 방식을 사용하고 다중 노드 간에는 MPI 통신 모델을 사용한다. 실험 노드의 개수(C)를 1, 2, 4, 8로 증가시켰을 때, 인

<표 4> 인텔 최적화 HPLinpack 성능 및 병렬 확장성 효율 비교

노드(사용 코어)	n	P(#)	Q(#)	Memory(%)	Rmean(TFLOP/s)	E(%)
1(68)	100000	1	1	75%	1.93	100%
2(136)	140000	1	2	74%	3.81	98.9
4(272)	210000	2	2	84%	7.30	94.6
8(544)	290000	2	4	81%	14.75	95.6



(그림 3) HPLinpack 소스 최적화에 따른 성능 비교

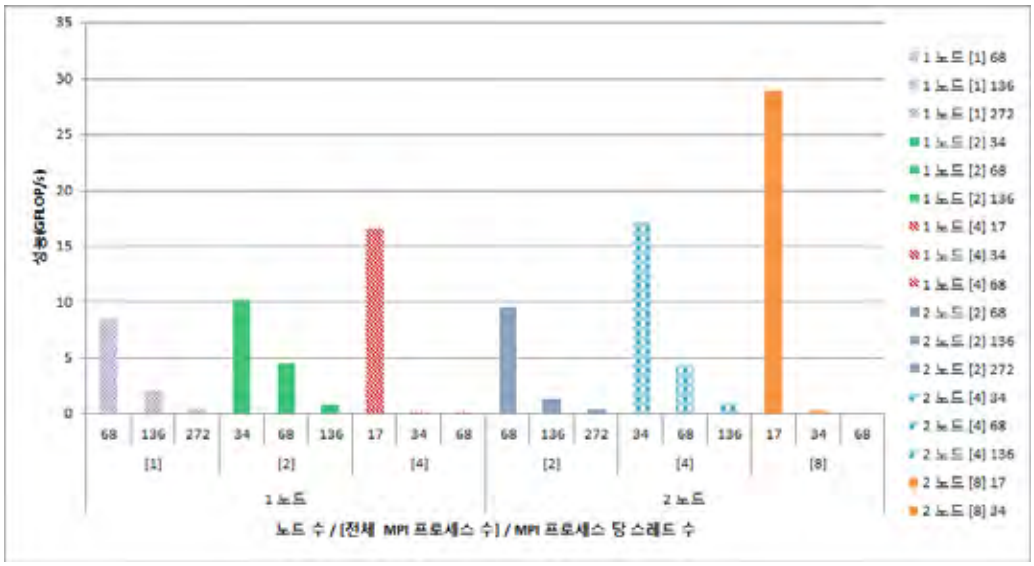
텔 코드에서의 최대 성능 값은 <표 4>와 같다. 각 실험에서 블록 크기는 최소 10,000 부터 최대 메모리로 할당이 될 때까지 10,000씩 증가시키며, 그 중에서 가장 성능이 높은 블록 크기를 선택하였다. 실험 결과, 10대 노드 미만까지는 확장 성능 효율이 약 95% 이상으로 유지된다. 또한 각 블록 크기가 실제적으로 전체 메모리의 약 80% 전후로 할당되었을 때 성능이 가장 높게 나온다. 본 실험 결과는 미국의 제온파이 기반 Colfax 클러스터에서 실험한 2017년 7월 벤치마크 보고서와 거의 비슷하다[17]. (그림 3)은 인텔에서 소스를 최적화한 버전과 기존 Netlib의 HPL을 비교하여 노드 수에 따른 성능을 측정한 그래프이다. 최적화에 따라서 최대 약 50%의 성능과 7%의 병렬 효율성 차이를 확인할 수 있으며, 시스템 구조에 맞는 병렬 프로그램 최적화가 중요한 요소임을 알 수 있다.

4.4 HPCG 벤치마크

HPCG(High Performance Conjugate Gradients) 벤치마크는 다양한 클러스터 응용 프로그램에 보다 잘 부합하는 기준을 제공함으로써 TOP500 시스템 순위에서 사용되는 고성능 LINPACK 벤치마크를 보완하기 위해 2013년 Michael Heroux, Jack Dongarra, Piotr Luszczek에 의해 제안되었다[18,19]. Jack Dongrra는 “기존의 LINPACK 벤치마크는 로컬 대역폭과 네트워크에 충분한 스트레스가 주어지지 않아 일반적으로 얻을 수 없는 성능레벨”이라고 한계점을 언급하였다. 반면에 HPCG는 희소행렬의 계산 같은 실세계 응용의 데이터 접근 패턴을 모델링하기 위한 것으로 슈퍼컴퓨터의 메모리 하위 시스템 및 내부 상호 연결의 한계가 컴퓨팅 성능에 미치는 영향을 테스트 한다. 따라서 HPCG 테스트는 일반적으로 컴퓨터의 최대 성능 중 극히 일부만을 수행하기 때문에 성능 측정을 위해 많은 시간을 필요로 하지 않는다. 본 절에서는 인텔에서 최적화한 버전의 HPCG[20]를 가지고, 입력 변수인 문제크기와 실행 시간에 따른 성능 차이를 확인하고 분석한다.

HPCG 방식은 3D 도메인의 각 그리드 지점(x,y,z)에서 27 포인트 스텐실을 사용하여(한 점에서의 방정식이 그 값과 주변 26 지점에 따라 달라짐) 논리적으로 전역적이며 물리적으로 분산된 희소 선형시스템을 생성한다. 세부적으로는 SPMV(Sparse Matrix-Vector Multiplication), SymGS(Symmetric Gauss-Seidel), WAXPBY (Scaled vector addition), DDOT(Dot Product)의 네가지 계산 블록과 MPI_Allreduce와 Halos Exchange의 두 통신 블록을 사용한다.

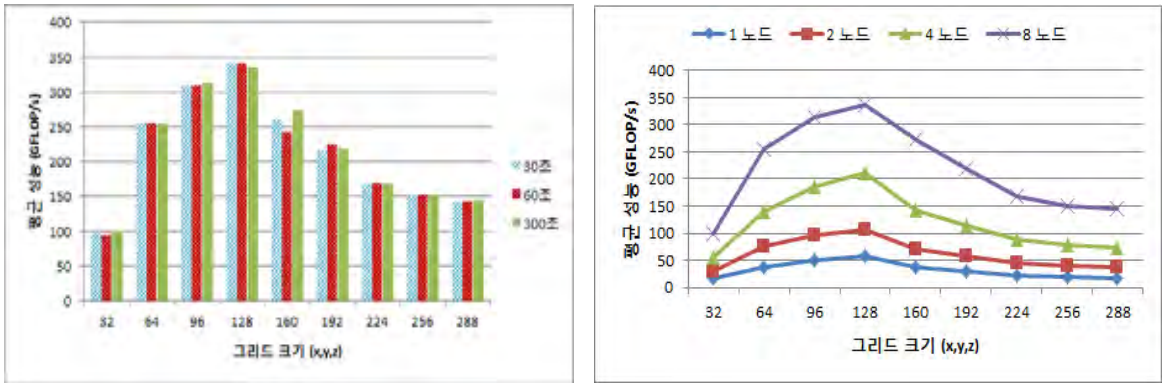
HPCG의 입력 변수는 2가지로 지역 도메인의 그리드 크기(x,y,z)와 실행시간(t)이 있다. HPCG 공식 문서에 따르면 실행에 적합한 문제 크기, 즉 그리드 크기는 CPU 캐시 보다 커야하고 총 메모리의 1/4 이상을 차지해야한다. 이때 그리드 크기는 최소 4이며, 4의 배수여야 한다. 또한 Top 500의 결과로 활용하기 위해서는 실행 시간을 최소 30분 이상 실행하도록 권고한다. HPLinpack과 마찬가지로 HPCG도 OpenMP / MPI 방식의 하이브리드 모델을 사용한다. 먼저 MPI 프로세스와 OpenMP 스레드 개수에 따른



(그림 4) 노드, MPI 프로세스, 스레드 개수의 조합에 따른 성능 비교

성능 변화를 직접 확인해 보기 위해 그리드 사이즈를 32로 작게 선택하고, 한 노드와 두 노드를 대상으로 성능을 측정한 결과는 (그림 4)와 같다. 결과에서 살펴볼 수 있듯이, 노드 당 MPI 프로세스 수는 4개 (2 노드의 경우는 8개), MPI 프로세스 당 스레드 수는 17 일 때 가장 좋은 성능을 보여준다.

본 조합의 결과를 기반으로 시간과 그리드 크기의 변화에 따른 실험 결과는 (그림 5)에 나타나 있다. 왼쪽 그림은 8 노드 OpenMP/MPI 실험으로 각 그리드 크기를 32에서 288까지 32 간격으로 증가시켰을 때, 30초, 60초, 300초별 성능을 비교한 결과로, 시간의 길이에 크게 변화가 없음을 알 수 있다. 즉, 단시간의 성능측정으로도 정확한 시스템 성능 측정이 가능하다[21]. 오른쪽 그림은 노드 수 증가에 따라 성능이 거의 선형적으로 비례하여 증가함을 확인할 수 있으며, 초기에 그리드 크기와 성능이 같이 증가하다, 그



(그림 5) 시간 및 그리드 크기의 변화에 따른 성능 결과

리드 크기가 128에 이르렀을 때 최대 성능 약 340 GFlop/s 에 이르고, 다시 서서히 떨어진다. 이는 그리드 크기가 MCDRAM의 최대 크기인 16 GB를 벗어나서, 일반 DDR 메모리를 사용하기 때문이다.

5. 결 론

본고에서는 인텔 차세대 매니코어 시스템인 KNL을 활용한 성능 분석과 벤치마크 실험을 위해 먼저 KNL에 대해서 간략히 소개한 후 대표적인 분석 도구에 대해 살펴보았다. 그리고 KNL 기반 테스트베드를 활용하여 3가지 주요 벤치마크 프로그램을 통해 성능을 측정하고 분석하여 성능에 영향을 미치는 요소들을 살펴보고 시스템 구조에 맞는 병렬 프로그램 최적화가 필요함을 보였다. 첫 번째로 STREAM 벤치마크의 배열 크기를 변화 시키면서 최적의 메모리 모드와 스레드 개수를 분석하였다. STREAM 벤치마크를 사용하여 고대역폭 온칩 메모리를 포함하는 인텔 제온파이의 메모리 성능을 측정한 결과 코어당 1 스레드로 최대 사용했을 때 가장 높은 성능을 보였으며, 실제 성능이 인텔 최적화 문서에 따른 기대 성능과 거의 비슷함을 확인하였다. 또한 인텔과 Netlib의 두 가지 HPLinpack 벤치마크 버전을 이용하여 단일 노드 및 클러스터 환경에서의 실험 결과, 블록크기가 전체메모리의 약 80%정도 할당 되었을 때 최고 성능을 보였으며 노드 수 증가에 따라 거의 선형적인 성능 증가를 보였다. 또한 최적화에 따라서 약 50%의 성능과 7%의 병렬 효율성 차이를 보였다. 마지막으로 HPCG 벤치마크 실험을 통해 MPI 프로세스 및 OpenMP 스레드 개수에 따른 성능 분석 결과 노드 당 MPI 프로세스는 4, 전체 스레드 수가 68일 때 가장 좋은 성능을 보임을 확인하였다. 또한 시간의 길이에 관계없이 단시간의 성능 측정으로도 거의 정확한 시스템 성능 측정이 가능함을 보였다.

참 고 문 헌

[1] http://www.prace-ri.eu/best-practice-guide-knights-landing-january-2017/

[2] A. Sodani, “Knights landing (KNL): 2nd Generation Intel® Xeon Phi processor,” Hot Chips 27 Symposium (HCS) IEEE 2015, 2015.

[3] 최지은, 박근철, 남덕윤, “차세대 매니코어 프로세서 기반 성능 모니터링 이벤트를 활용한 응용 특성 분석 기법”, 2017년 한국소프트웨어종합학술대회 논문집, 2017년 12월.

[4] Harini R. “Intel(R) Xeon(R) Phi(TM) Processor Performance Monitoring Reference Manual” published on November 2, 2015, updated March, 2017.

[5] Arnaldo Carvalho de Melo, “The New Linux ‘Perf’ tools”, presentation from Linux Kongress, September, 2010.

[6] PAPI, http://icl.cs.utk.edu/papi/

[7] VTune, https://software.intel.com/en-us/intel-vtune-amplifier-xe

[8] HPC Tools, https://developer.arm.com/products/software-development-tools/hpc/arm-performance-reports

[9] S. Shende and A. D. Malony., “The TAU Parallel Performance System”, International Journal of High Performance Computing Applications, Volume 20 Number 2, pp 287-311, 2006.

[10] ARM Performance Reports, https://www.arm.com/products/development-tools/hpc-tools/cross-platform/performance-reports

[11] McCalpin, John D.: "STREAM: Sustainable Memory Bandwidth in High Performance Computers", a continually updated technical report (1991-2007), available at: "http://www.cs.virginia.edu/stream/"

[12] McCalpin, John D., 1995: "Memory Bandwidth and Machine Balance in Current High Performance Computers", IEEE Computer Society Technical Committee on Computer Architecture (TCCA) Newsletter, December 1995.

[13] https://software.intel.com/en-us/articles/optimizing-

memory-bandwidth-in-knights-landing-on-stream-triad
[14] J. J. Dongarra, P. Luszczek, and A. Petitet "The LINPACK Benchmark: Past, Present, and Future." Concurrency and Computation: Practice and Experience vol. 15, no. 9, pp. 803-820, August, 2003.
[15] A. Petitet, R. C. Whaley, J. Dongarra, A. Cleary "HPL-A Portable Implementation of the High-Performance Linpack Benchmark for Distributed-Memory Computers", 2016. http://www.netlib.org/benchmark/hpl/
[16] https://software.intel.com/en-us/node/725943
[17] https://colfaxresearch.com/hpl-on-xeon-phi-x200/
[18] Hemsoth, Nicole (June 26, 2014). "New HPC Benchmark Delivers Promising Results". HPCWire. Retrieved 2014-09-08.
[19] Dongarra, Jack; Heroux, Michael (June 2013). "Toward a New Metric for Ranking High Performance Computing Systems" (PDF). Sandia National Laboratory. Retrieved 2016-07-04.
[20] https://software.intel.com/en-us/mkl-linux-developer-guide-getting-started-with-intel-optimized-hpcg
[21] http://en.community.dell.com/techcenter/high-performance-computing/b/general_hpc/archive/ 2017/01/17/hpcg-performance-study-with-intel-knl

저 자 약 력

노 승 우

이메일 : seungwoo0926@kisti.re.kr

- 2009년 서울시립대학교 전자전기컴퓨터공학부 (학사)
- 2011년 서울시립대학교 전자전기컴퓨터공학과 (석사)
- 2011년~2013년 서울시립대 UGL Soft / 선임연구원
- 2011년~현재 한국과학기술정보연구원(KISTI) / 선임기술원
- 관심분야 : 고성능컴퓨팅, 분산컴퓨팅, 시스템 벤치마킹, 프로파일링

최 지 은

이메일 : jieun1205@kisti.re.kr

- 2014년 숙명여자대학교 컴퓨터과학부 (학사)
- 2016년 숙명여자대학교 컴퓨터과학과 (석사)
- 2017년~현재 한국과학기술정보연구원 / 기술원
- 관심분야 : 고성능컴퓨터, 시스템 프로파일링

남 덕 윤

이메일 : dynam@kisti.re.kr

- 1999년 포항공과대학교 컴퓨터공학과(학사)
- 2001년 한국정보통신대학교 공학부(석사)
- 2006년 한국정보통신대학교 공학부(박사)
- 2004년~현재 한국과학기술정보연구원(KISTI) / 선임연구원
- 관심분야 : 분산시스템, 슈퍼컴퓨팅, 저전력컴퓨팅

박 근 철

이메일 : gcpark@kisti.re.kr

- 1998년 중앙대학교 컴퓨터공학과 (학사)
- 2000년 중앙대학교 컴퓨터공학과 (석사)
- 1998년~2000년 (주)넥센
- 2000년~2005년 (주)창성정보시스템
- 2005년~2005년 (주)이스톰
- 2006년~현재 한국과학기술정보연구원(KISTI) / 선임연구원
- 관심분야 : 분산컴퓨팅, 프로파일링, 작업최적화

박 찬 열

이메일 : chan@kisti.re.kr

- 1993년 고려대학교 수학과 (학사)
- 1995년 고려대학교 전산학과 (석사)
- 2000년 고려대학교 전산학과 (박사)
- 2010년~2011년 누욕주립대 Visiting Scholar
- 2002년~현재 한국과학기술정보연구원 (KISTI) / 책임연구원
- 관심분야 : 분산시스템, 슈퍼컴퓨팅, 저전력컴퓨팅

정보처리학회지 2017년도 7월호 게재 목차

■ 2017년 7월 (제24권 제4호)	■ 특집명 : 드론 관련 기술과 응용

정보처리학회지 2017년도 9월호 게재 목차

■ 2017년 9월 (제24권 제5호)	■ 특집명 : 4차 산업혁명

정보처리학회지 2017년도 11월호 게재 목차

■ 2017년 11월 (제24권 제6호)	■ 특집명 : ICT 융합

JIPS(정보처리학회영문지) 2017년도 8월호 게재 목차

■ Volume 13, Number 4(Serial Number 46), August, 2017

JIPS(정보처리학회영문지) 2017년도 10월호 게재 목차

■Volume 13, Number 5(Serial Number 47), October, 2017

JIPS(정보처리학회영문지) 2017년도 12월호 게재 목차

■ Volume 13, Number 6(Serial Number 48), December, 2017

정보처리학회논문지 2017년도 7월호 게재 목차

■ 제6-CCS권 제7호(통권 제58호) 2017년 7월

■ 제6-SDE권 제7호(통권 제58호) 2017년 7월

정보처리학회논문지 2017년도 8월호 게재 목차

■ 제6-CCS권 제8호(통권 제59호) 2017년 8월

■ 제6-SDE권 제8호(통권 제59호) 2017년 8월

정보처리학회논문지 2017년도 9월호 게재 목차

■ 제6-CCS권 제9호(통권 제60호) 2017년 9월

■ 제6-SDE권 제9호(통권 제60호) 2017년 9월

정보처리학회논문지 2017년도 10월호 게재 목차

■ 제6-CCS권 제10호(통권 제61호) 2017년 10월

■ 제6-SDE권 제10호(통권 제61호) 2017년 10월

정보처리학회논문지 2017년도 11월호 게재 목차

■ 제6-CCS권 제11호(통권 제62호) 2017년 11월

■ 제6-SDE권 제11호(통권 제62호) 2017년 11월

정보처리학회논문지 2017년도 12월호 게재 목차

학회동정

[학회 주최/주관 행사]

◈ 2017년도 제3차 단기강좌 개최

1) 일 자 : 2017년 8월 18일(금)
2) 장 소 : CNN the Biz 교육연수센터 301호
3) 참석자 : 44명(일반 : 14명, 일반참가 : 30명)
4) 내 용 : Beyond 5G 이동통신 핵심 기술

[2017년도 제3차 단기강좌에서 중앙대학교
장진곤 교수의 발표 모습]

[2017년도 제3차 단기강좌 개최 모습]

◈ 2017년도 추계학술발표대회 개최

1) 일 자 : 2017년 11월 3일(금)~4일(토)
2) 장 소 : 서울과학기술대학교
3) 조 직 :
   학 회 장 : 정영식 교수(동국대학교)
   수석부회장 : 남석우 대표이사(콤텍시스템)
   조직위원장 : 박종혁 교수(서울과학기술대학교)
   학술위원장 : 김상훈 교수(한경대학교)
   홍보위원장 : 문남미 교수(호서대학교),
   한근희 교수(건국대학교)
4) 논문현황 :
   접수논문 : 411편(구두발표 163편, 포스터발표 248편/대학원생이상 144편, 학부생 267편)
   게재발표 : 385편(구두발표 155편, 포스터발표 230편/대학원생이상 136편, 학부생 249편)
   게재불가 및 취소 : 26편
   시 상 : 전체 25편 – 최우수논문상 3편, 우수논문상 22편
   학부생논문경진대회 : 전체 30편 – 대상 1편, 금상 2편, 은상 3편, 동상 9편, 장려상 15편
5) 참가자 : 498명(일반 : 136명, 학생 : 362명)
6) 튜토리얼발표 : 이종혁 교수(상명대학교),
   임희석 교수(고려대학교),
   윤덕용 교수(아주대학교)
7) 신진학자워크샵 : 조형민 교수(홍익대학교),
   이상근 교수(한양대학교),
   정영섭 교수(순천향대학교)
8) 초청강연 : 이상직 변호사(법무법인 태평양)

[2017년도 추계학술발표대회 포스터 논문 발표 모습]

[2017년도 추계학술발표대회 신진학자 워크샵 발표 모습 - 한양대학교 이상근 교수]

[2017년도 추계학술발표대회 구두 논문 발표 모습]

[2017년도 추계학술발표대회 초청강연 발표 모습 – 법무법인 태평양 이상직 변호사]

[2017년도 추계학술발표대회 튜토리얼 발표 모습 - 아주대학교 윤덕용 교수]

[2017년도 추계학술발표대회 우수논문상 시상 모습]

◈ 2017년도 제4차 단기강좌 개최

1) 일　자 : 2017년 12월 1일(금)
2) 장　소 : CNN the Biz 교육연수센터 301호
3) 참석자 : 83명(일반 30명, 학생 53명)
4) 주　제 : 블록체인 튜토리얼 및 응용 기술

◈ 2017년도 송년회 및 학술대상 시상식 개최

1) 일　시 : 2017년 12월 6일(수) 18:00
2) 장　소 : 그랜드엠버서더서울호텔
3) 참석자 : 정영식 회장 외 94명
4) 수상자 :
학술대상–박종혁 교수(서울과학기술대학교)
기술대상–남석우 대표(콤텍시스템)
논문대상–황나윤 대학원생(고려대학교)

[2017년도 송년회 및 학술대상 시상식에서
정영식 회장의 인사말 모습]

[2017년도 송년회 및 학술대상 시상식에서 학술대상 시상
모습 - 서울과학기술대학교 박종혁 교수]

[2017년도 송년회 및 학술대상 시상식에서 기술대상 시상
모습 - 콤텍시스템]

[2017년도 송년회 및 학술대상 시상식에서 논문대상 시상
모습 - 고려대학교 황나윤 학생]

[2017년도 송년회 및 학술대상 시상식에서 남석우 차기
회장의 인사말 모습]

[2017년도 송년회 및 학술대상 시상식에 참석한 임원 모습]

[CUTE 2017 논문 발표 모습]

◈ CUTE 2017(The 12th KIPS International Conference on Ubiquitious Informatiln Technologies and Applications) 개최

1) 일 자 : 2017년 12월 18일(월)~20일(수)
2) 장 소 : 대만 타이중 Providence University
3) 발 표 : 총 145편(국내 : 136편, 해외 : 9편, 총 4개국)
4) 참가자 : 83명(일반 30명, 학생 53명)
5) 일 정 :

[CUTE 2017 개회식에서 공동 조직위원장의 인사말 모습 - Prof., Hsiao-Hsi Wang, Providence University, Taiwan]

Day 1, December 18 , 2017					
Time	Min	HALL A	HALL B	HALL C	HALL D
08:40-09:00	20	Registration			
09:00-10:30	90	Session A-1 CUTE	Session B-1 SDNMC	Session C-1 CSA	Session D-1 SLLS
10:30-10:40	10	Coffee Break			
10:40-12:10	90	Session A-2 CUTE	Session B-2 HRH	Session C-2 CSA	Session D-2 SLLS
12:10-13:30	80	Lunch			
13:30-14:30	60	Keynote: Chin-Chen Chang, Ph.D. Professor at Feng Chia University Taichung, Taiwan			
14:30-14:40	10	Coffee Break			
14:40-16:10	90	Session A-3 CUTE	Session B-3 ATFC	Session C-3 CSA	Session D-3 NGFS
16:10-16:20	10	Coffee Break			
16:20-17:50	90	Session A-4 CUTE	Session B-4 SPOCCD	Session C-4 CSA	Session D-4 HRH
18:00-20:00	120	Reception			

Day 2, December 19, 2017					
Time	Min	HALL A	HALL B	HALL C	HALL D
08:40-09:00	20	Registration			
09:00-10:30	90	Session A-5 CUTE	Session B-5 IRuH	Session C-5 CSA	Session D-5 CUTE
10:30-10:40	10	Coffee Break			
10:40-12:10	90	Session A-6 CUTE	Session B-6 IRuH	Session C-6 CSA	Session D-6 CSA
12:10-13:30	80	Lunch			
13:30-15:00	90	Session A-7 CUTE	Session B-7 ISWP	Session C-7 CSA	Session D-7 SoReMo
17:00-18:00	60	Shuttle Bus to Tempus Hotel for Banquet			
18:00-20:00	120	Banquet			

Day 3, December 20, 2017					
Time	Min	HALL A	HALL B	HALL C	HALL D
10:00-12:00	120	CSA - Organizing Committee Meeting			
13:00-15:00	120	CUTE - Organizing Committee Meeting			
15:00-17:00	60	Local Arrangement Committee Meeting			

[CUTE 2017 개회식에서 공동조직위원장에게 감사패 전달 모습 - Prof., Hsiao-Hsi Wang, Providence University, Taiwan]

[CUTE 2017 감사패 전달 모습 - Prof., Chin-Chen Chang, FengChia University Taiwan]

[CUTE 2017 초청강연 발표 모습 - Prof., Chin-Chen Chang, FengChia University Taiwan]

[CUTE 2017 리셉션에 참석한 한국측 운영위원회 위원 모습]

[CUTE 2017 논문 발표 모습]

[CUTE 2017 만찬에서 감사패 수여 모습 -
Prof., Chuan-Yi Tang, Providence Univ., Taiwan]

[CUTE 2017 만찬 개최 모습]

[CUTE 2017 만찬에서 감사패 수여 모습 -
한경대학교 김상훈 교수]

[CUTE 2017 만찬에서 공동조직위원장 인사말 모습 -
서울과학기술대학교 박종혁 교수]

[CUTE 2017에 참석한 운영위원회 각 위원 모습]

[공동 주최/주관 행사]

◈ 제249회 스마트 사회 지도자 포럼 개최

1) 일 시 : 2017년 7월 7일(금) 07:00
2) 장 소 : 밀레니엄힐튼호텔 지하1층 그랜드볼룸 A
3) 주 관 : 도산아카데미 공동 주관
4) 참석자 : 정영식 회장 외 34명
5) 강연자 : 배영우 ㈜아이메디신 대표이사
6) 제 목 : 인공지능 의료IT의 혁신

[제249회 스마트 사회 지도자 포럼 개최 모습]

◈ 제250회 스마트 사회 지도자 포럼 개최

1) 일 시 : 2017년 8월 11일(금) 07:00
2) 장 소 : 밀레니엄힐튼호텔 지하1층 그랜드볼룸 A
3) 주 관 : 도산아카데미 공동 주관
4) 참석자 : 정영식 회장 외 46명
5) 강연자 : 한석수 한국교육학술정보원(KERIS) 원장
6) 제 목 : 4차 산업혁명 시대의 교육, 어디로 가야하나?

[제250회 스마트 사회 지도자 포럼 개최 모습]

◈ 제 251회 스마트 사회 지도자 포럼 개최

1) 일 시 : 2017년 9월 1일(금) 07:00
2) 장 소 : 밀레니엄힐튼호텔 B1 그랜드볼룸 A
3) 주 최 : 도산아카데미 공동 주최
4) 참석자 : 정영식 회장 외 41명
5) 강연자 : 문영준 소장(한국교통연구원 교통기술연구소)
6) 제 목 : 제4차 산업혁명과 스마트 모빌리티

[제251회 스마트 사회 지도자 포럼 개최 모습]

◈ 제252회 스마트 사회 지도자 포럼 개최

1) 일 시 : 2017년 10월 13일(금) 07:00
2) 장 소 : 밀레니엄힐튼호텔 B1 그랜드볼룸A
3) 주 최 : 도산아카데미 공동 주최
4) 참석자 : 정영식 회장 외 36명
5) 강연자 : 김창경 교수(한양대학교 과학기술정책학과)
6) 제 목 : 4차 산업혁명 시대의 뉴 노멀

[제252회 스마트 사회 지도자 포럼 개최 모습]

◈ 제253회 스마트 사회 지도자 포럼 개최

1) 일 시 : 2017년 11월 3일(금) 07:00
2) 장 소 : 밀레니엄힐튼호텔 3F 아트리움
3) 주 최 : 도산아카데미 공동 주최
4) 참석자 : 정영식 회장 외 40명
5) 강연자 : 최경일 대표이사(세틀뱅크)
6) 제 목 : 한국의 간편 결제시장의 현황 및 향후 전개 발향

[제253회 스마트 사회 지도자 포럼 개최 모습]

◈ 제254회 스마트 사회 지도자 포럼 개최

1) 일 시 : 2017년 12월 13일(금) 07:00
2) 장 소 : 밀레니엄힐튼호텔 B1 그랜드볼룸A
3) 주 최 : 도산아카데미 공동 주최
4) 참석자 : 정영식 회장 외 38명
5) 강연자 : 서병조 원장(한국정보화진흥원)
6) 제 목 : 4차 산업혁명과 지능 정보 사회

[제254회 스마트 사회 지도자 포럼 개최 모습]

[지회 및 연구회]

– 전산교육연구회

◈ 제64차 IT 관련학과 교수연수 및 논문발표 개최

1) 일 시 : 2017년 7월 5일(수) ~ 7일(금)
2) 장 소 : 전주 라마다호텔
3) 주 관 : 전산교육연구회(위원장: 김형진 교수)
4) 참석자 : 42명(발표논문 12편)
5) 내 용 :

시간	발표제목		발표/좌장	
제 1일차 – 2017. 7. 5(수)				
13:00 – 14:00	등록 및 접수			
14:00 ~ 14:30	개회식	개회사 - 위원장	정원창 진주보건대학교	
		축 사 - 한국정보처리학회 회장		
	[초청 · 기술 특강]			
14:30 ~ 14:50	4차 산업시대의 대학 교육 방안		양승원 교수 우석대학교	정우식 동서울대학교
14:50 ~ 15:00	[휴 식]			
15:00 ~ 15:50	4차 산업시대의 데이터 관리 및 효과적인 교육 지원 방안		장성우 전무 한국오라클	박정연 수성대학교
15:50 ~ 16:00	[휴 식]			
16:00 ~ 16:50	4차 산업혁명과 데이터		이화식 대표 엔코아	김수선 한양여자대학교
16:50 ~ 17:00	[휴 식]			

시간	발표제목	발표/좌장	
17:00 ~ 17:30	사물인터넷의 교통시스템 적용 사례	오재곤 대표 세인시스템	박찬호 부천대학교
17:30 ~ 17:50	기업 소개		
17:50 ~ 18:30	4차 산업혁명과 NCS	박현수 교수 백석문화대학교	선수균 동원대학교
18:00 ~ 18:30	방 배정 및 휴식		
18:30 ~ 20:30	만 찬		
20:30 ~ 21:00	운영위원회		
제 2일차 – 2017. 7. 6(목)			
07:30 ~ 08:30	조식		
09:00 ~ 09:30	MoS 운영 과정	정영진 대리 (주)와이비엠	송진희 신한대학교
09:30 ~ 10:00	혁신적인 모바일 개발 툴 Fuse Pro	김상섭 차장 (주)제이아이티	김수선 한양여자대학교
10:00 ~ 10:10	[휴 식]		
10:10 ~ 11:00	드론 체험	김상희 이사 ㈜ 바이로봇	이성은 동서울대학교
11:00 ~ 11:10	[휴 식]		
11:10 ~ 12:00	드론 소프트웨어	김상희 이사 ㈜ 바이로봇	이용관 연성대학교
12:00 ~ 13:00	중식		
13:00 ~ 13:50	(전체토의) NCS 운영 방안	조규천 교수 한림성심대학교	정우식 동서울대학교
13:50 ~ 14:10	[휴 식]		
14:10 ~ 16:00	(전체토의) NCS 교육 방안	류재천 교수 연성대학교	박승용 인천재능대학교
16:00 ~ 16:10	[휴 식]		
16:10 ~ 18:00	분과위원 및 산학협동위원 간담회	김형진 전북대학교	이준형 강동대학교
제 3일차 – 2017. 7. 7(금)			
09:00 ~ 10:00	논문발표 – Session 1	좌장-김에녹 연암공업대학교	
10:00 ~ 11:00	논문발표 – Session 2	좌장-신현정 신한대학교	
11:00 ~ 12:00	**총회**		

– IT융합/서비스연구회

◈ CAIPT 2017 국제컨퍼런스 개최

1) 일　시 : 2017년 8월 8일(화) ~ 10일(목)
2) 장　소 : Anvaya Beach Resort, Bali, Indonesia
3) 주　관 : IT융합서비스연구회
　　(위원장: 박석천 교수)
4) 참석자 : 87명(발표논문 : 98편)
5) 행사일정 :

[CAIPT 2017 개회식에서 개회사 모습 –
한경대학교 김상훈 교수]

First Day, August 8, 2017

TIME	PROGRAM	OBJECT
13:00 ~ 18:00	Participants Arrive and check in The ANVAYA Beach Resort, Bali	Committee
19:00 ~ 22:00	Welcome Dinner at The ANVAYA Beach Resort, Bali	Committee
22:00 ~	Have a nice rest	Good Night

Second Day, August 9, 2017

TIME	PROGRAM	OBJECT
07:00 ~ 08:00	Registration and Coffee Break	Committee
08:00 ~ 08:05	Conference Opening and Welcome Reception	Committee
08:05 ~ 08:10	National Anthem	Master of Ceremony, Committee
08:10 ~ 08:20	Opening Dance	Dancers
08:20 ~ 08:25	Welcoming Speech from Conference Chairperson	Master of Ceremony, Committee
08:25 ~ 08:30	Opening Speech and the Opening Statement from the President of CAIPT	Master of Ceremony, Committee
08:30 ~ 08:30	Opening Speech from KIPS	
08:30 ~ 10:00	1. Keynote Speech **Lee Kyung Oh(Sun Moon University-South Korea)** +Questions-Answers session (approx.3questions), Certificate and Souvenir session (45minutes) 2. Keynote Speech **Prof. Dr. Richardius Eko. Indrajit, M. Sc, M.B.A** (Perbanas)+Questions-Answers session (approx.3 questions), Certificate and Souvenir session (45 minutes)	Moderator Time Keeper: MC
10:30 ~ 12:30	Parallel Session 1 in 4 Rooms with 13 Presenters each Room	Time Keeper, Committee
12:30 ~ 13:30	Lunch	Committee
13:30 ~ 15:30	Parallel Session 2 in 3 Rooms with 17 Presenters each Room	Time Keeper, Committee
15:30 ~ 16:00	Coffee Break	Committee
16:00 ~ 16:30	Tour to GWK by VW	Committee
16:30 ~ 20:00	Cultural Dinner, Closing Ceremony, and Photo Session at GWK	Committee

Third Day, August 10, 2017

TIME	PROGRAM	OBJECT
06:00 ~ 08:00	Business Meeting Between Aptikom 7 and KIPS	Committee
08:00 ~ 09:00	Individual Meetings Among Participants	Committee
12:00	Check Out Hotel Anvaya	Participants

[CAIPT 2017 개회식에서 초청강연 모습 - 선문대학교 이경오 교수]

[CAIPT 2017 논문 발표 모습 1]

[CAIPT 2017 개회식에서 초청강연 모습 - Prof. Dr. Richardius Eko. Indrajit, M. Sc, M.B.A, Indonesia]

[CAIPT 2017 논문 발표 모습 2]

[CAIPT 2017 개회식에 참석한 운영위원회 각 위원장 모습]

[CAIPT 2017 만찬에서 우수논문상 수여 모습 - 경상대학교 손영호 교수]

[CAIPT 2017의 참가자모습]

– 이브릿지연구회

◈ 2017년도 제 5차 이브릿지편집위원회 회의 개최

1) 일 시 : 2017년 8월 24일(목) 11:00
2) 장 소 : KISTI 서울분원 원장실
3) 참석자 : 안문석 위원장 외 13명
4) 내 용 : 2017년도 포럼 개최 협의 외

– 컴퓨터소프트웨어연구회

◈ BIC 2017 개최

1) 일 시 : 2017년 8월 22일(화) ~ 24일(목)
2) 장 소 : 제주 함덕호텔
3) 주 최 : 컴퓨터소프트웨어연구회 (위원장: 박두순 교수)
4) 참석자 : 124명(발표논문 : 141편)

◈ IFIT 2017 개최

1) 일 시 : 2017년 10월 12일(목) ~ 14일(토)
2) 장 소 : 동국대학교
3) 주 관 : 컴퓨터소프트웨어연구회 (위원장: 박두순 교수)
4) 참석자 : 30명(발표논문 : 25편)

– 충북지회

◈ ICW / DBMI 2017 개최

1) 일 시 : 2017년 10월 13일(금) ~ 16일(월)
2) 장 소 : 충북대학교
3) 주 관 : 컴퓨터소프트웨어연구회 (위원장: 박두순 교수)
4) 참석자 : 46명(발표논문 : 48편)

– 호남지회

◈ 2017년도 제 3차 워크샵 개최

1) 일 시 : 2017년 10월 20일(금)
2) 장 소 : 광주대학교
3) 주 관 : 호남지회(지회장: 방상원 교수)
4) 참석자 : 27명
5) 내 용 : 초청강연, 패널토론, 이사회

– 에너지그리드정보처리연구회

◈ 제6회 에너지그리드 정보처리연구회 학술대회 개최

1) 일 시 : 2017년 11월 9일(목)
2) 장 소 : 한전 전력연구원 강당
3) 주 최 : 컴퓨터소프트웨어연구회 (위원장: 송완석 원장)
4) 참석자 : 135명(발표논문 : 86편)
5) 내 용 : 에너지그리드정보처리연구회 활동 및 경과보고
에너지그리드 기술공유, 우수논문 발표 및 시상

[제회의]

◈ 2017년도 제 3차 이사회 회의 개최

- 일 시 : 2017년 10월 20일(금) 17:00
- 장 소 : 콤텍시스템 B1 회의실
- 참석자 : 정영식 회장 외 34명
- 내 용 : 2018년도 사업계획 및 예산(안) 심의 외

[2017년도 제3차 이사회에서 콤텍시스템
남석우 대표의 환영 인사 모습]

[2017년도 제3차 이사회에서 정영식 회장의 개회사 모습]

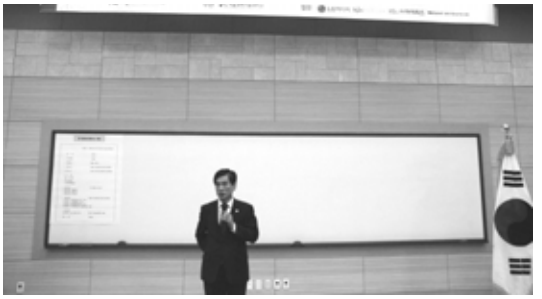
[2017년도 제3차 이사회에서 감사 보고 모습]

[2017년도 제3차 이사회 개최 모습]

◈ 2017년도 정기총회 개최

1) 일　시 : 2017년 11월 3일(금) 17:40
2) 장　소 : 서울과학기술대학교 무궁관 9층 911호
3) 참석자 : 정영식 회장 외 125명
4) 내　용 : 2018년도 사업계획 및 예산(안) 심의 외

[2017년도 정기총회에서 정영식 회장의 개회사 모습]



[2017년도 정기총회에서 서울과학기술대학교
김종호 총장의 환영사 모습]

[2017년도 정기총회에서 감사패 수여 모습 -
서울과학기술대학교 김종호 총장]

[2017년도 정기총회에서 공로상 수여 모습 - 서울과학기술대학교 박종혁 교수]

[2017년도 정기총회에서 우수 논문상 수여 모습]

[2017년도 정기총회에서 각 회무 모고 모습]

[2017년도 정기총회에서 2018년도 수석부회장 당선증 전달 모습]

[각위원회 회의]

– 선거관리위원회

◈ 제1차 선거관리위원회 회의 개최(서면결의)

1) 일 시 : 2017년 9월 18일(월)
2) 장 소 : 학회 회의실
3) 참석자 : 구원모 위원장 외 9명
4) 내 용 : 2017년도 수석부회장 선거 요강 및 일정 확정

◈ 제2차 선거관리위원회 회의 개최

1) 일 시 : 2016년 10월 28일(금) 16:00
2) 장 소 : 콤텍시스템 회의실
3) 참석자 : 박두순 위원장 외 6명
4) 내 용 : 2017년도 수석부회장 추천 서류 검토 외

– 전임회장운영위원회

◈ 2016년 제2차 전임회장운영위원회 회의 개최

1) 일 시 : 2016년 10월 6일(목) 18:00
2) 장 소 : 진진바라 강남점
3) 참석자 : 성기중 위원장 외 10명
4) 내 용 : 2017년도 수석 부회장 선거 관련 및 학회 자문 사항 외

[발간사업 추진 활동]

– 논문지(KTCCS, KTSDE) 편집위원회

◈ 논문지 제3차 SCOPUS 등재 준비회의 개최

1) 일 시 : 2016년 10월 7일(금) 12:00
2) 장 소 : 학회 회의실
3) 참석자 : 신창선 위원장 외 2명
4) 내 용 : 논문지 SCOPUS 등재 준비 협의 외

– JIPS 운영위원회

◈ 2017년도 제2차 영문논문지(JIPS) 운영위원회 개최

1) 일 시 : 2017년 8월 10일(금) 16:00
2) 장 소 : 학회 회의실
3) 참석자 : 박종혁 위원장 외 16명
4) 내 용 : JIPS 8월호 발간 준비 외

[학술사업 추진 활동]

– SQMS 2017

◈ SQMS 2017 제 1차 준비회의 개최

1) 일 시 : 2017년 7월 11일(화) 15:00
2) 장 소 : 한국소프트웨어산업협회 회의실
3) 참석자 : 진광화 학술위원장 외 4명
4) 내 용 : 제21회 소프트웨어 품질관리 심포지엄 개최 여부 협의

– 추계학술발표대회

◈ 2017년도 추계학술발표대회 제1차 학술위원장단회 개최

1) 일 시 : 2017년 8월 16일(수) 17:00
2) 장 소 : 학회 회의실
3) 참석자 : 김상훈 프로그램위원장 외 12명
4) 내 용 : 2017년도 추계학술발표대회 논문 모집 독려 방안 협의

◈ 2017년 추계학술발표대회 제2차 학술위원장단회 개최

1) 일 시 : 2017년 9월 28일(목) 14:00
2) 장 소 : 학회 회의실
3) 참석자 : 김상훈 학술위원장 외 12명
4) 내 용 : 2017년도 추계학술발표대회 논문 심사 및 우수논문상 수상자 확정 외

– CUTE 2017

◈ CUTE 2017 제 2차 준비위원회 개최

1) 일 시 : 2017년 8월 10일(목) 17:00
2) 장 소 : 학회 회의실
3) 참석자 : 이강만 조직위원장 외 17명
4) 내 용 : CUTE 2017 논문 모집 독려 및 행사 준비

[CUTE 2017 제2차 준비위원회에서
이강만 조직위원장의 인사말 모습]

[CUTE 2017 제2차 준비위원회 개최 모습]

[기타 활동]

◈ 2017년도 2/4분기 감사 시행

1) 일 시 : 2017년 7월 18일(화) 11:00
2) 장 소 : 학회 회의실
3) 참석자 : 이재일 감사외 1명
4) 내 용 : 학회 2017년도 2/4분기 회무 및 재무 감사

◈ 2016년도 3/4분기 감사 시행

1) 일 시 : 2017년 10월 12일(목) 11:00
2) 장 소 : 학회 회의실
3) 참석자 : 이재일 감사 외 1명
4) 내 용 : 학회 2016년도 3사분기 회무 및 재무 감사

신규회원 명단

회원구분	회원번호	성명	직장명
갱신된 종신회원	2004-11457-01	김명진	엠에스엘엠
종신회원	2017-21555-01	서화정	한성대학교
	2017-21567-01	정수영	서울대학교
	2017-21569-01	이종혁	상명대학교
	2017-21571-01	서영석	영남대학교
정회원	2017-21412-02	오하영	아주대학교
	2017-21418-02	황금하	한국전자통신연구원
	2017-21421-02	이영록	전남대학교
	2017-21422-02	임동진	한양대학교
	2017-21425-02	심재권	고려대학교
	2017-21472-02	어윤일	경희사이버대학교
	2017-21492-02	김경태	삼성전자
	2017-21426-02	박재용	유엔사 군사정전위원회
	2017-21427-02	이장우	디자인선
	2017-21436-02	류호성	삼성전자
	2017-21446-02	이창근	이머징큐
	2017-21453-02	이희정	평택대학교
	2017-21460-02	박영	충북도립대학
	2017-21473-02	이대호	유니텍
	2017-21474-02	전수민	유니텍
	2017-21480-02	정용환	한국과학기술정보연구원
	2017-21482-02	김중환	케이아이엔엑스
	2017-21485-02	이명수	전자부품연구원
	2017-21488-02	김봉재	선문대학교
	2017-21510-02	박상봉	세명대학교
	2017-21530-02	이은지	충북대학교
	2017-21535-02	지태현	아이엔소프트
	2017-21536-02	권혜정	고려대학교
	2017-21544-02	이필규	HCT
	2017-21546-02	김희선	안동대학교
	2017-21551-02	이상근	한국전자통신연구원

회원구분	회원번호	성명	직장명
정회원	2017-21556-02	류덕산	한국과학기술원
	2017-21561-02	곽재혁	한국과학기술정보연구원
	2017-21563-02	염희균	대전대학교
	2017-21564-02	이재철	세기정보통신
	2017-21566-02	전성신	전자부품연구원
	2017-21570-02	오현석	동서울대학교
	2017-21572-02	손현숙	대구가톨릭대학교
	2017-21573-02	노태균	성균관대학교
	2017-21574-02	유정민	한국전통문화대학교
준(학생) 회원	2017-21411-03	박상훈	가톨릭대학교
	2017-21413-03	김진배	서강대학교
	2017-21415-03	정창훈	인하대학교
	2017-21416-03	고동우	가톨릭대학교
	2017-21417-03	김미정	경동고등학교
	2017-21419-03	전재승	고려대학교
	2017-21423-03	이수진	경기대학교
	2017-21424-03	전승호	고려대학교
	2017-21519-03	이호연	충남대학교
	2017-21533-03	정원기	고려대학교
	2017-21428-03	박진호	세종대학교
	2017-21429-03	서덕원	세종대학교
	2017-21430-03	장비	한양대학교
	2017-21431-03	형효남	한양대학교
	2017-21432-03	박범준	선정고등학교
	2017-21433-03	이준희	고려대학교
	2017-21434-03	정현도	고려대학교
	2017-21435-03	Jose Angel Pineda	연세대학교
	2017-21437-03	이태열	고려대학교
	2017-21438-03	김재환	서울호서전문학교
	2017-21439-03	김한결	서울호서전문학교

회원구분	회원번호	성명	직장명
준(학생)회원	2017-21440-03	조인령	서울호서전문학교
	2017-21441-03	박성현	충북대학교
	2017-21442-03	조현석	고려대학교
	2017-21443-03	송진현	충북대학교
	2017-21444-03	채민기	충북대학교
	2017-21445-03	신동협	경기대학교
	2017-21447-03	고은혜	가톨릭대학교
	2017-21448-03	박수진	가톨릭대학교
	2017-21449-03	박인영	가톨릭대학교
	2017-21450-03	이재이	가톨릭대학교
	2017-21452-03	김상준	서울미디어대학원대학교
	2017-21454-03	박재정	인천대학교
	2017-21455-03	박승규	인천대학교
	2017-21456-03	최우영	인천대학교
	2017-21457-03	오병훈	고려대학교
	2017-21458-03	이승빈	인천대학교
	2017-21459-03	방지원	강원대학교
	2017-21461-03	김진성	인천대학교
	2017-21462-03	오성근	고려대학교
	2017-21463-03	김대연	인천대학교
	2017-21465-03	신승옥	인천대학교
	2017-21466-03	이재학	고려대학교
	2017-21467-03	이재혁	고려대학교
	2017-21468-03	장준범	서경대학교
	2017-21469-03	양찬우	서경대학교
	2017-21470-03	황지환	인천대학교
	2017-21471-03	서우덕	단국대학교
	2017-21475-03	채도원	충북대학교
	2017-21476-03	김재민	한양대학교
	2017-21477-03	박승우	고려대학교
	2017-21478-03	손호성	고려대학교
	2017-21479-03	민세원	성균관대학교
	2017-21481-03	김준한	고려대학교

회원구분	회원번호	성명	직장명
준(학생)회원	2017-21483-03	강동현	연세대학교
	2017-21484-03	정백준	서울호서직업전문학교
	2017-21486-03	조영탁	이타기술
	2017-21487-03	정은미	경북대학교
	2017-21490-03	박평우	아주대학교
	2017-21491-03	윤혜경	아주대학교
	2017-21494-03	채예은	서울여자대학교
	2017-21495-03	김주현	동국대학교
	2017-21496-03	정경석	한국기술교육대학교
	2017-21498-03	서영학	충남대학교
	2017-21500-03	박승각	인천대학교
	2017-21503-03	전수용	동의대학교
	2017-21504-03	장세운	인천대학교
	2017-21505-03	이상록	충북대학교
	2017-21506-03	박다울	한동대학교
	2017-21507-03	신재호	인천대학교
	2017-21508-03	이원준	충남대학교
	2017-21509-03	이선웅	인천대학교
	2017-21511-03	문혁은	한동대학교
	2017-21512-03	윤혜린	한동대학교
	2017-21513-03	한보경	한동대학교
	2017-21514-03	김연욱	선문대학교
	2017-21515-03	정다운	고려대학교
	2017-21516-03	김다솜	인천대학교
	2017-21517-03	김상수	서경대학교
	2017-21518-03	조장훈	충남대학교
	2017-21520-03	박선우	한양대학교
	2017-21521-03	김유정	숙명여자대학교
	2017-21522-03	오용석	서경대학교
	2017-21523-03	김민석	연세대학교
	2017-21524-03	조민수	연세대학교
	2017-21525-03	신명우	충남대학교
	2017-21526-03	박길섭	충남대학교

회원구분	회원번호	성명	직장명
준(학생) 회원	2017-21529-03	안선우	서울대학교
	2017-21531-03	김미수	성균관대학교
	2017-21532-03	김경식	성균관대학교
	2017-21534-03	이혜진	숙명여자대학교
	2017-21537-03	한재호	연세대학교
	2017-21538-03	Afarin	연세대학교
	2017-21539-03	오세라	세종대학교
	2017-21540-03	구자훈	세종대학교
	2017-21541-03	김다올	한양대학교
	2017-21542-03	한경엽	인천대학교
	2017-21543-03	김휘준	충남대학교
	2017-21545-03	김선경	한국방송통신대학교
	2017-21547-03	서유진	인천대학교

회원구분	회원번호	성명	직장명
준(학생) 회원	2017-21548-03	주화철	선문대학교
	2017-21549-03	홍보선	선문대학교
	2017-21550-03	윤종근	인천대학교
	2017-21552-03	고선재	인천대학교
	2017-21553-03	김준식	고려대학교
	2017-21554-03	권세훈	서울호서전문학교
	2017-21557-03	김민현	인천대학교
	2017-21558-03	박승현	인천대학교
	2017-21559-03	황동현	순천향대학교
	2017-21560-03	김태경	인천대학교
	2017-21562-03	방인영	서울대학교
	2017-21565-03	김도경	한밭대학교
	2017-21575-03	윤점진	전남대학교

특별 법인회원 명단

구 분	대표자	주 소
(주)경봉	윤석원 대표	경기도 안양시 만안구 예술공원로 153-32
(주)베스트케이에스	김교은 대표	서울시 금천구 범안로 1130 가산디지털엠파이어빌딩 501, 502호
(주)블루코어	이동화 대표	서울시 강남구 역삼동 682 남전빌딩 4층
삼성SDS(주)	정유성 대표	서울시 송파구 올림픽로35길 123(신천동) 삼성SDS타워
(주)영화조세통람	서동혁 대표	서울시 중구 동호로 14길 5-6 이나우스빌딩
(주)LG CNS	김영섭 대표	서울시 영등포구 여의대로 24, FKI타워
(주)자이네스	고범석 대표	서울시 구로구 디지털로33길 55 904호(E&C벤처드림타원 2차)
정보통신산업진흥원	윤종록 원장	충북 진천군 덕산면 정통로 10
정보통신정책연구원	김도환 원장	충북 진천군 덕산면 정통로 18
(주)지란지교시큐리티	윤두식 대표	서울시 강남구 역삼로 542(대치동 신사S&G 5층)
(주)G.I.G기업	이용기 대표	서울시 광진구 능동로40길8 정암빌딩 100호
KCC정보통신	이상현 대표	서울시 강서구 공항대로 665 KCC오토타워(염창동 260-4번지)
한국인터넷진흥원	백기승 원장	서울시 송파구 중대로 135 IT벤처타워 4층
한국정보화진흥원	서병조 원장	대구시 동구 첨단로 53
한국전자통신연구원	이상훈 원장	대전시 유성구 가정로 218

한국정보처리학회 기관지 원고 집필 안내

한국정보처리학회는 학회지 「정보처리학회지」와 논문지 「정보처리학회논문지A·B·C·D」를 발행하고 있습니다. 「정보처리학회지」는 새로운 기술동향을 비롯해서 각종 정보를 게재하고, 회원의 지식 향상을 목적으로 하며, 「정보처리학회논문지A·B·C·D」는 회원의 연구 결과를 발표하는 장입니다.

본 안내는 학회 기관지의 원고 집필 요령을 정리한 것으로, 집필 시 참고로 하시기 바랍니다.

『정보처리학회지』 원고 집필 안내

제 1 조 학회지에 게재할 원고의 종류는 특집, 특별기고, 기획기사, 정보 관련 기술 동향 및 편집위원회가 인정하는 것으로 한다.

제 2 조 투고자는 원칙적으로 본 학회 회원으로 한다. 단, 회원과의 공동기고자 및 초청기고자는 예외로 한다.

제 3 조 원고는 수시로 접수하며 접수일은 원고가 본학회 편집위원회에 도착한 날로 하고, 접수된 원고는 편집위원회에서 게재여부를 결정한다.

제 4 조 원고는 가장 많이 사용되는 워드프로세서로 작성한 파일을 함께 제출한다.

제 5 조 원고의 내용은 정보처리 관련자가 이해할 수 있는 정도로 작성한다.

제 6 조 투고자는 200자 이내의 약력을 제출하여야 한다. 게재가 확정된 원고에 대해서는 추후 저자의 사진을 제출해야 한다.

제 7 조 본 학회지에 게재된 내용은 본 학회의 승인없이 영리목적으로 무단 복제하여 사용할 수 없다.

제 8 조 원고 작성 방법은 다음과 같다.

(1) 1페이지 기술 분량 : A4용지 30행×40자 내외

(2) 원고분량 : 6~8페이지 내외

(3) 참고문헌 : 참고 문헌은 저자명에 의한 사전식으로 기술하되, 각 참고 문헌은 잡지의 경우 “번호저자명, 제목, 잡지명, 권, 호, 페이지, 연도”의 순으로 기술한다. 단, 참고문헌 인용시에는 대괄호를 이용할 것(예 [1], [2], [3], [4] 등)

(예) [1] 김철수, 김수철, “한국 정보 처리 산업에 관한 연구”, 한국정보처리논문지, 제 1권, 제 1호, pp.23-43, 1997.

[2] 이영희, 컴퓨터입문, pp.234, 출판사, 1997.

[3] L. Lanomt, “Synchronization Architecture and Protocols”, IEEE Trans. on Comm., Vol. 23, No. 3, pp.123-132, 1997.

[4] Steinmetz, Multimedia : Computing, Communications & Applications, PII, 1995.

(4) 내용표기에 있어서, 장, 절 등의 표시는 ‘ 1, 1.1, 1.1.1, 가, 1), 가), (1), (가)’의 순서로 한다.

(5) 원고는 ‘제목-소속-성명-목차-본문-참고문헌’의 순으로 기술하며, 첫장 하단에는 회원 구분을 명기한다.

(6) 표의 제목은 “<표1>대한민국” 과 같이 표의 상단에 기술하고, 그림의 제목은 “(그림1)서울”과 같이 그림의 하단에 기술하며, 사진판으로 사용할 수 있도로 백지에 정서해야 한다.

본 규정은 1997년 1월 1일부터 효력을 발생한다.

기타 원고 모집 안내

당 학회지 편집위원회에서는 학회지 「정보처리학회지」에 게재할 각종 원고를 회원 여러분으로부터 모집하고 있습니다. 많은 투고와 참여있으시기 바랍니다.

1. 모집내용

다음에 대한 원고를 모집합니다.

(1) 해 설 : 정보처리에 관련된 신기술 또는 이론으로서 당 학회 회원의 관심도가 높은 내용
(2) 외국기사 : 외국 잡지에 게재된 기사로서 당 학회 회원에게 유익한 내용
(3) 서 평 : 최근에 출판된 책으로서 당 학회 회원에게 유익한 도서의 소개 또는 비평
(4) 뉴 스 : 정보처리에 관한 국제규모의 회의, 대회의 보고 등 시사성이 높고 당 학회 회원에게 널리 알릴 가치가 있는 내용
(5) 기관소개 : 국내 기관 또는 외국 기관
(6) 기 타 : 당 학회 회원에게 유익한 내용

2. 응모 자격

당 학회 회원으로 한다.

3. 응모 절차

원고는 학회지 편집위원회에서 정한 투고 규정에 의거하여 다음 순서로 기술하여 주시기 바랍니다.

(1) 제 목
서평의 경우에는 저자명, 책이름, 페이지수, 출판사, 발행년도, 가격 등으로 기술한다.
어느 장르에 속하는지를 첫페이지 오른쪽 상단에 표시한다.
(2) 필자명, 소속, 필자 연락처
(3) 본 문
본문은 서평의 경우 2,000자 정도, 뉴스의 경우 1,000자 정도로 한다.
(4) 참고문헌, 부록, 그림, 표
(5) 필자 소개
이름, 경력과 학력을 기술한다.

4. 원고 취급

투고된 원고는 학회지 편집위원회에서 심사를 한 후 게재여부를 결정합니다. 게재가 결정되었을 경우에는 원고 수정을 부탁하는 경우가 있습니다. 서평의 경우에는 필자의 사진이 필요하므로 게재 결정 후 학회 사무국으로 우송해야 됩니다.

5. 원고료

학회지 규정에 의거하여 소정의 원고료를 지급합니다.

6. 보낼 곳

04376 서울특별시 용산구 한강대로 109, 1002호(한강로 2가 용성비즈텔)
한국정보처리학회 학회지 편집위원회
uskim@kips.or.kr

정보처리학회 논문지 투고 규정

1. 원고의 전자 투고

모든 원고는 전자 형태(MS Word, 아래아 한글, 혹은 PDF 형태)로 학술지 웹사이트 (http://acoms1.kisti.re.kr/kips/index.jsp?publisher_cd=kips&cid=&cid_year=2006&cid_seq=A&lang=kor)를 통해 온라인으로 투고하여야 한다. 투고 규정은 해당 웹사이트에서도 볼 수 있으며, 본 학술지에 투고하는 모든 원고들은 이 규정을 준수하여야 한다. 그렇지 않을 경우 원고가 반송되게 되며 이로 인해 출판이 지연될 수도 있다. 원고 투고에 관한 문의는 이메일(kips@kips.or.kr)이나 전화(+82-2-2077-1414), 팩스(+82-2-2077-1472)를 통해 학회 사무국으로 한다. 저자 중에 1인은 학회 회원으로 가입되어야 함을 원칙으로 한다.

2. 연구 및 출판 윤리

본 학술지는 Guidelines on Good Publication (http://publicationethics.org/static/1999/1999pdf13.pdf)에 기술된 연구 및 출판 윤리 지침을 따른다.

2.1 이해갈등관계 명시

저자는 기업으로부터의 재정적 지원 또는 연계, 이익집단으로부터의 정치적 압력 등과 같은 이해 갈등 관계가 있으면, 이에 관한 정보를 밝혀야 한다. 특히, 연구에 관계된 모든 지원금의 출처를 명백히 진술해야 한다.

2.2 저자 요건

1) 연구의 기본개념설정과 설계, 자료수집, 또는 자료분석과 해석에 지대한 공헌을 하고, 2) 원고를 작성하거나 내용의 중요 부분을 변경 또는 개선하고, 3) 최종 원고의 내용에 동의한 세 가지 조건을 모두 충족한 사람만이 논문 저자로서 원고에 나열되어야 한다. 원고의 최초 투고 후, 어떠한 저자 변경 사항(저자 추가, 저자 삭제, 혹은 저자 순서 변경)도 편집인에게 편지로 알려주고 승인을 받아야 한다. 이 편지에는 해당 논문의 모든 저자들의 서명이 포함되어야 한다.

2.3 이중게재/이중투고 금지

투고 된 모든 원고는 다른 학술지에 이미 실렸거나 또는 심사 중이어서는 안 된다. 채택된 원고의 모든 부분은 편집위원회의 허가 없이 다른 과학학술지에 이중게재 하여서는 안 된다. 본지에 실린 논문의 이중게재 발각 시에는 저자 및 소속기관에 이를 알릴 것이며, 저자에게 제재가 가해 질 것이다.

3. 상호심사 절차

모든 원고는 편집위원이 위촉한 2인 또는 3인의 심사위원들이 평가하며, 연구의 질과 독창성, 그리고 과학적 중요성을 바탕으로 심사하여 채택 여부를 결정한다. 원고투고 후 심사결과를 이메일로 통보 받게 되며 심사자의 의견이 교신저자의 이메일로 전달된다. 교신저자는 수정된 원고를 온라인으로 재투고해야 하며 심사자의 지적에 따라 변경된 내용을 각 항목별로 진술해야 한다. 편집위원회 결정 이후 8주가 경과해도 수정된 원고를 재투고하지 않을 시에는 철회로 간주한다. 저자는 학술지 웹사이트에서 투고 논문의 심사 진행 현황을 확인할 수 있다.

4. 저작권

출판된 모든 원고는 한국정보처리학회의 자산이 되며, 서면허가 없이 다른 곳에 출판되어서는 안 된다. 출판이 결정되면 저자는 저작권양도 서식을 기재하여 팩스, 우편 또는 이메일로 학회 사무국에 보내야 한다.

5. 원고 작성

5.1 언어

모든 원고는 국문 또는 영문으로 작성하여야 한다. 국문 논문의 경우, 서지 정보(제목, 저자, 소속, 교신저자의 주소와 이메일), 표, 그림, 감사의 글, 참고문헌 등은 모두 영문으로 기술하여야 한다. 심사를 위한 초기 투고 원고에는 저자 정보를 포함시키지 말아야 한다. 하지만, 논문 수락 판정을 받은 후 제출하는 최종본에는 저자 정보를 포함시켜야 한다.

5.2 일반적인 사항

1) 원고는 MS Word나 한글문서로 작성한다.

2) 원고는 A4 (21.0×29.7cm) 용지에 10point 글씨크기로 행 사이를 2행 간격(double space)으로 하여 작성하되, 상하좌우 모두 2.5cm의 여백을 둔다.

3) 모든 단위는 International System(SI) of Units 에 따라 기술하여야 한다. 퍼센트(%)와 온도(℃)를 제외한 모든 단위는 한 칸의 공백 다음에 기술해주어야 한다.

5.3 출판 유형

한국정보처리학회논문지는 연구논문(research paper), 편집인의 글(editorial), 편집인과의 서신(letters to the editor) 등을 출판한다.

1) 연구논문(research paper): 본 학술지가 다루는 범위 안에서 새로운 학술적 발견들을 상호 심사과정을 거쳐 연구논문으로 출판할 수 있다. 연구논문에는 이론이나 실험에 관한 새롭고 중요한 결과들이 기술되어야 한다. 연구논문 중 일반논문(regular paper)과 단편논문(short paper)의 길이 제한은 각각 20쪽과 4쪽 이내이다.

2) 편집인의 글(editorial): 편집인의 글은 초빙에 의해서만 원고를 투고할 수 있으며, 본 학술지 편집위원회에서 결정하는 주제들을 다룬다.

3) 편집인과의 서신(letters to the editor): 본 학술지에 이미 출판된 학술 논문에 관한 간략한 평가나 흥미로운 새로운 아이디어를 편집인과의 서신으로 투고할 수 있다. 학술지 편집위원회에서는 투고된 서신을 편집할 수 있으며, 필요한 경우 해당 논문의 저자에게 회신을 요청할 수도 있다.

5.4 연구논문

원고는 국문제목, 국문요약과 국문키워드, 영문제목, 영문요약과 영문키워드, 본문, 감사의 글(필요 시), 참고문헌을 순서대로 포함한다.

1) 영문제목
제목은 공백을 포함해 길이가 40자를 초과하지 않도록 한다.
2) 영문요약과 키워드
요약은 무슨 연구를 어떻게 수행하였는지, 주된 연구결과와 그 중요성에 관해 간결하게 기술하여야 한다. 요약은 300단어를 초과해서는 안되며, 표나 참고문헌 번호를 포함하지 않은 하나의 문단으로 기술되어야 한다. 초록의 하단부에는 연구분야와 내용을 나타낼 수 있는 3 ~ 5단어 이내의 키워드를 기재하여야 한다.
3) 본문
a) 장절 제목: 장이나 절의 제목은 1. , 1.1, 1), a) 와 같이 4 단계 레벨로 표기할 수 있다.
b) 본문 중 참고문헌 인용: 참고문헌은 본문에서 처음 인용되는 순서대로 번호를 붙인다. 그리고 본문에서 참고문헌을 인용할 때는 해당 참고문헌의 번호를 [1, 4, 7] 혹은 [6-9]와 같이 각괄호 안에 기재한다.
c) 약어: 약어는 저자의 편의성보다는 독자에게 도움을 줄 수 있는 방식으로 사용되어야 한다. 따라서 약어는 가급적 제한적으로 사용하는 것이 바람직하다. 표와 그림을 포함해 본문에서 세 번 이상 등장하지 않는 약어의 사용은 가급적 파하라. 약어는 본문에서 처음 사용될 때 축약 이전의 형태로 정의되어야 한다.
d) 표: 표는 본문에서 인용되는 순서대로 아라비아 숫자로 번호를 붙인다. 표의 제목과 설명은 영어로 작성하며, 본문 내용을 읽지 않고도 이해할 수 있도록 간결 명료하게 작성한다
e) 그림: 그림은 본문에서 인용되는 순서대로 아라비아 숫자로 번호를 붙인다. 동일한 번호에 두 개 이상의 그림이 있는 경우, Fig. 1A, Fig. 1B와 같이 아라비아 숫자 뒤에 알파벳 대문자를 기입하여 구분한다. 자신이 그린 그림이 아니면 저작권자의 허락을 받아야 하며 각주에 이를 밝혀야 한다.
4) 감사의 글
필요한 경우, 본문 뒤에 감사의 글을 포함시킬 수 있으며, 연구비 지원 또는 다른 지원에 대한 내용을 명시할 수 있다.
5) 참고문헌
모든 참고문헌은 영어로 기술하며, 제출 원고의 내용과 분명히 관련이 있는 것들이어야 한다. 참고문헌은 본문에서 처음 인용되는 순서대로 번호를 붙인다. 참고문헌들은 반드시 원저 확인을 통해 출처를 검증하는 것이 필요하다.
다음 예시들을 참고하여 참고문헌들을 작성한다.

Journal Article

[1] S. Y. Hea and E. G. Kim, "Design and implementation of the differential contents organization system based on each learner's level," *The KIPS Transactions: Part A*, vol. 18, no. 6, pp. 19-31, 2011.

[2] S. Y. Hea, E. G, Kim, and G. D. Hong, "Design and implementation of the differential contents organization system based on each learner's level," *KIPS Transactions on Software and Data Engineering*, vol. 19, no. 3, pp. 19-31, 2012.

Book & Book Chapter

[3] S. Russell, P. Norvig, *Artificial Intelligence: A Modern Approach*," 3th ed., New York: Prentice Hall, 2009.

[4]. J. L. Hennessy and D. A. Patterson, "Instruction-level parallelism and its exploitation," in *Computer Architecture: A Quantitative Approach*, 4th ed., San Francisco, CA: Morgan Kaufmann Pub., ch. 2, pp. 66-153, 2007.

[5] D. B. Lenat, " Programming articitical interlligence," in *Understanding Artificial Intelligence*, Scientific American, Ed., New York: Warner Books Inc., pp. 23-29, 2002.

Conference Proceedings

[6] A. Stoffel, D. Spretke, H. Kinnemann, and D. A. Keim, "Enhancing document structure analysis using visual analytics," in *Proceedings of the ACM Symposium on Applied Computing*, Sierre, 2010, pp. 8-12.

Dissertations

[7] J. Y. Seo, " Text driven construction of discourse structures for understanding descriptive texts," Ph.D. dissertation, University of Texas at Austin, TX, USA, 1990.

Online Source

[8] Thomas Claburn, Google Chrome 18 brings faster graphics [Internet], http://www.techweb.com/news/232800057/google-chrome-18-brings-faster-graphics.html.

6. 투고료 및 게재료

6.1 투고료

본 학술지에 원고를 투고할 때, 투고자는 1편당 일반 심사의 경우 50,000원(US $50), 급행 심사의 경우 350,000원(US $350)을 학회에 납부하여야 한다.

6.2 게재료

채택된 논문의 투고자는 논문의 게재를 위해 다음과 같은 논문 게재료를 학회 사무국에 납부하여야 한다.
- 인쇄쪽수가 1 ~ 6쪽인 경우, 100,000원
- 인쇄쪽수가 7쪽 이상인 경우, 100,000원 + 50,000원 추가 / 쪽당

6.3 은행계좌

- 한국외환은행: 232-13-01249-5 (예금주: 한국정보처리학회)
- 우체국: 012559-01-000730 (예금주: 한국정보처리학회)

7. 본 투고 규정은 2012년 9월 1일부터 효력을 발생한다.

입회 안내

국가가 지향하는 첨단 정보처리 산업과 기술혁신의 시대에 부응하여 첫째, 정보처리 학술활동의 활성화, 둘째, 정보처리 기술의 산학연 협동의 내실화, 셋째, 정보처리 기술의 국제화와 표준화 등 회원봉사 활동에 역점을 두고 정보화사회를 선도하는 명실상부한 정보처리 분야의 정통학회인 사단법인 한국정보처리학회에서는 정보처리분야에 종사하고 계시는 여러분들의 많은 입회를 바라고 있습니다.

주 요 목 적 사 업

1. 정보처리에 관한 각종 학술발표회 및 전시회 개최
2. 정보처리에 관한 지식 및 기술 보급에 관한 사업
3. 정보처리 기술의 상호 협조 및 정보 교환
4. 정보처리에 관한 표준화 사업
5. 국제적 학술 교류 및 기술 협력
6. 학회지 및 논문지 발간
7. 정보처리에 관한 문헌 발간
8. 기타 본 학회 목적 달성에 필요한 사업

(정관 제4조)

회 원 의 종 류 및 자 격

1. 특별회원 : 정보처리 분야 발전에 기여하고 본학회의 취지에 찬동하는 법인 및 단체.
2. 명예회원 : 학식과 덕망이 높고 본 학회의 발전에 크게 기여한 자.
3. 정 회 원 : 정보처리 관련 분야를 전공하여 학사학위 이상을 취득한 자 또는 정보처리 관련분야에서 2년이상 근무한 자.
4. 준 회 원 : 정보처리 관련학과 학생 또는 대학원생
5. 단체회원 : 도서관 또는 초·중·고 교육기관

(정관 제6조)

회 원 의 혜 택

1. 정보처리학회지(논설, 기술보고, 해설, 전망, 강좌, 단편정보 등 게재) 발행. 무료배포
2. 정보처리학회논문지 및 특집호(학술연구논문, 심사완료 후 게재) 발행.
3. 춘추계 학술발표회와 각종 학술행사에 참가 및 논문발표
4. 전문분과연구회의 활동자격과 각종 학술행사에 참가 및 논문발표
5. 국제 학술회의 활동 및 외국 학회에 참가 및 추천
6. 정보처리 및 기술발전에 업적이 있는 회원에게는 각종 학회상 수여

회 비

1. 특별회원 회비는 이사회의 결정에 따르면 종신회원·정회원·준회원·단체회원 회비는 다음과 같다.

구 분	종 신 회 원	정 회 원	준 회 원	단 체 회 원
연 회 비	600,000원	60,000원	40,000원	300,000원

※ 논문 구독료 각권 별도 2만원 (필요시 구독)

2. 회원가입은 학회 홈페이지를 통하여 회원정보를 입력하신후 회비를 신용카드 결제 및 아래의 은행으로 입금하여 주시기 바랍니다.
   한국외환은행 계좌번호 : 232-13-01249-5 예금주 : (사단)한국정보처리학회
   우 체 국 계좌번호 : 012559-01-000730 예금주 : 한국정보처리학회

문의처 : 04376 서울특별시 용산구 한강대로 109, 1002호(한강로 2가 용성비즈텔)
사단법인 한국정보처리학회 사무국 귀하
전 화 : (02) 2077-1414(代) 팩 스 : (02) 2077-1472
홈페이지 : www.kips.or.kr e-mail : ysyun@kips.or.kr

연구회 안내

당 학회에는 현재 다음과 같은 연구회가 구성되어 있으며, 이들 연구회는 위원장을 중심으로 하여 현재 활발한 연구 활동을 하고 있습니다. 연구회에 가입을 원하시는 회원은 연구회 가입 원서를 작성하셔서 당 학회 사무국 또는 각 위원장에게 보내주시기 바랍니다. 회원 여러분의 많은 가입을 부탁드립니다. 연구회 발족 등에 관한 의견이 있으시면 학회로 연락 주시기 바랍니다.

e-Bridge 연구회

위원장 : 이정배 부총장 (부산외국어대학교)
전 화 : 051)509-5033
e-mail : jblee1120@naver.com

우정기술연구회

위원장 : 정 훈 부장 (ETRI)
전 화 : 042)860-6470
e-mail : hoonjung@etri.re.kr

IT 융합서비스연구회

위원장 : 박석천 교수 (가천대학교)
전 화 : 031)750-5328
e-mail : scpark@gachon.ac.kr

전산교육연구회

위원장 : 김형진 교수 (전북대학교)
전 화 : 063)270-4783
e-mail : kim@chonbuk.ac.kr

IT 정책연구회

위원장 : 오길록 교수 (숭실대학교)
전 화 :
e-mail : gilrokoh@paran.com

전산수학연구회

위원장 : 박진홍 교수 (선문대학교)
전 화 : 041)530-2224
e-mail : chp@omega.sunmoon.ac.kr

빅데이터컴퓨팅연구회

위원장 : 이필규 교수 (인하대학교)
전 화 : 032)860-7448
e-mail : pkrhee@inha.ac.kr

전자정부연구회

위원장 : 이재두 수석 (NIA)
전 화 : 02)2131-0370
e-mail : leejaedu@gmail.com

소프트웨어공학연구회

위원장 : 박용범 교수 (단국대학교)
전 화 : 031)8005-3220
e-mail : ybpark@dankook.ac.kr

정보통신융용연구회

위원장 : 오진태 부장 (ETRI)
전 화 : 042)860-4977
e-mail : showme@etri.re.kr

스토리지시스템연구회

위원장 : 신범주 교수 (부산대학교)
전 화 : 055)350-5417
e-mail : bjshin@pusan.ac.kr

지식및데이터공학연구회

위원장 : 진병운 박사 (ETRI)
전 화 : 042)860-6544
e-mail : bwjin@etri.re.kr

에너지그리드정보처리연구회

위원장 : 이봉재 센터장 (전력연구원)
전 화 : 042)865-5700
e-mail : leeboja@kepco.kco.kr

컴퓨터소프트웨어연구회

위원장 : 박두순 교수 (순천향대학교)
전 화 : 041)530-1317
e-mail : parkds@sch.ac.kr

한국정보처리학회 신용카드 결제신청서

◈ **납입방법 : 신용카드**

◈ **결재내용 : 학회 회비 / 세미나 참가비 / 논문 구독료 / 논문 게재료**

학 회 회 비	종신회원 ₩600,000( ) 정회원 ₩60,000( )
	준 회 원 ₩40,000( ) 기 타 (₩)
행 사 등 록 비	(₩)
논 문 구 독 료 (각 권당 2만원)	□소프트웨어 및 데이터 공학(KTSDE) □컴퓨터 및 통신 시스템(KTCCS) (₩)
논 문 게 재 료	( )권 ( )호 (₩)
기 타	(₩)

◈ **신용카드 사용내역서**

카 드 명	□ 신한카드 □ 국민카드 □ 비씨카드		결 재	일시불( )	※ 타카드 사용 불가
카드번호	□□□□ □□□□ □□□□ □□□□				
지불금액	원	카드유효기간	년 월	전 화	
소 속		성 명		서 명	
"상기 금액을 정히 지불합니다" 사단법인 한국정보처리학회					

※ 신한카드, 국민카드 및 비씨카드만 사용이 가능합니다.

※ 반드시 팩스로 회송바랍니다.

※ 학회 연회비 및 논문 구독료는 홈페이지에서 로그인 후 모든 카드로 온라인 카드 결재가 가능합니다.

☞ 보내실곳 : **한국정보처리학회**

전화 : (02)2077-1414 팩 스 : (02)2077-1472

http://www.kips.or.kr e-mail : ysyun@kips.or.kr

04376 서울특별시 용산구 한강대로 109, 1002호(한강로 2가 용성비즈텔)

학 회 사 무 국

선임국장	송영민 (내선 5)	min@kips.or.kr	업무총괄 / 제회 / CUTE 행사 / SQMS 행사
국 장	김은순 (내선 2)	uskim@kips.or.kr	학회지 / 춘계학술대회 / 단기강좌 / 연구과제
과 장	이주연 (내선 1)	joo@kips.or.kr	JIPS(영문지) / IT21컨퍼런스 / 추계학술발표대회
과 장	윤영숙 (내선 3)	ysyun@kips.or.kr	회원 / 재무 / 국문지 / 홈페이지 및 뉴스레터

- **사무국주소** : (04376) 서울특별시 용산구 한강대로 109, 1002호(한강로2가, 용성비즈텔)
- **전 화** : 02) 2077-1414
- **팩 스** : 02) 2077-1472
- **대 표 메 일** : kips@kips.or.kr
- **홈 페 이 지** : www.kips.or.kr

정보처리학회지

제 25 권 제 1 호

등록일자 : 1994년 3월 31일
서기 2018년 1월 25일 인쇄
서기 2018년 1월 31일 발행

발 행 인 : 남 석 우

편 집 인 : 김 종 완

발 행 처 : 사단법인 한국정보처리학회 KIPS Korea Information Processing Society

(04376) 서울특별시 용산구 한강대로 109, 1002호(한강로 2가, 용성비즈텔)
전 화 : (02)2077-1414(代) 팩 스 : (02)2077-1472
홈페이지 : www.kips.or.kr 이메일 : kips@kips.or.kr

* 제작 : (주)이환디앤비 Tel : (02)2254-4301(代) <비매품>

라온이란?
'행복'이라는 뜻의 순수 우리말입니다.

LAON Intelligence

라온피플은 고객을 위한 행복 지능을 만들어갑니다.

LAON PEOPLE's Artificial Intelligence

AI

인공지능
비전 검사 솔루션
AIDi, AIPi, AIXi, AISi

인공지능
비전 검사 소프트웨어
NAVI AI Tool

인공지능
스마트 카메라
LPSC-700

인공지능
비전 검사 트레이너
NAVI AI Trainer

LAON PEOPLE

라온피플 주식회사
본사: 경기도 성남시 분당구 판교로 723, 분당테크노파크 B동 402-3호 (우)13511
대표전화: 1899-3058 팩스: 031-707-7052 전자우편: sales@laonpeople.com 홈페이지: www.laonpeople.com

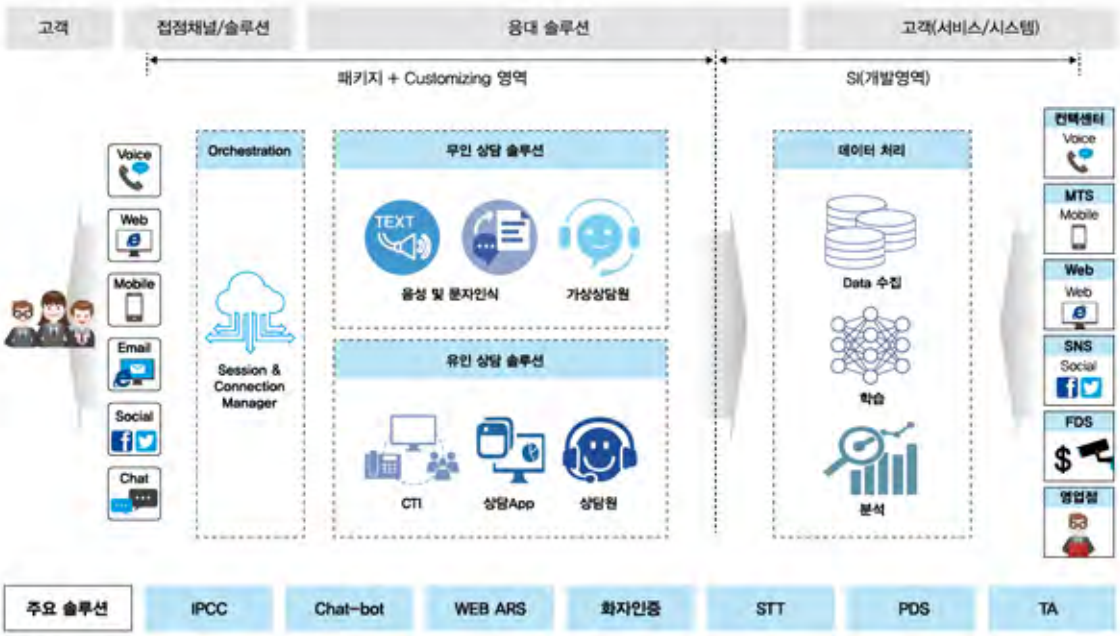
www.comtec.co.kr

AI기반 지능형 고객센터?

콤텍이 그 솔루션의 해답입니다!

4세대 지능형 고객센터

- 음성인식, 챗봇 등 가상 상담 서비스
- 지능형 응대 및 내역 관리 서비스
- AI 기반 신규 Biz 창출



comtec (주)콤텍시스템

컨설팅 문의

· 전 화 : 02-3289-0114
· 이메일 : hjlee@comtec.co.kr