

PROGRAMME BOOK AND ABSTRACT

The 2nd International Conference on Computing and Applied Informatics (ICCAI) 2017

November 29th - 30th, 2017 Hotel GranDhika Setiabudi Medan, Indonesia

Scopus' I Inspec Compendex SPIRES INIS

NASA Astrophysics Data System VINITI Abstract Journal Chemical Abstracts Service



Contents

Introduction from the Chair **Conference Information** 1 Committee 2 Venue Map Floor Plan 5 Keynote Speaker Schedule of ICCAI 2017 Schedule of ICCAI 2017 Parallel Session 11 Abstracts of Paper 25 Artificial Intelligence 25 Vi-DA: Vitiligo Diagnostic Assistance Mobile Application (G A Nugraha, A Nurhudatiana and R Bahana) 25 Performance test for prototype game for children with ADHD (R Bahana, F L Gaol, T Wiguna, S W H L Hendric, B Soewito, E Nugroho, B P Dirgantoroand E 25 The Development of Indonesian Traditional Bekel Game in Android Platform (R FRahmat, O R Fahrani, S Purnamawati, and M F Pasha) Control Of Motion Stability Of The Line Tracer Robot Using Fuzzy Logic And Kalman Filter (M S Novelan, Tulusand E M Zamzami) Improved Hybridization Of Fuzzy Analytic Hierarchy Process (FAHP) Algorithm With Fuzzy Multiple Attribute Decision Making - Simple Additive Weighting (FMADM-SAW) (B E Zaiwani, M Zarlisand S Efendi) Implementation of Chaotic Gaussian Particle Swarm Optimization for Optimize Learning-to-Rank Software Defect Prediction Model Construction (M A Buchari, S Mardiyanto, B Hendradjaya) Analysis Backpropagation Methods with Neural Network for Prediction of Children's Ability In Psychomotoric (F Izhari, H W Dhany, M Zarlisand Sutar-Rangku Alu - A Traditional East Nusa Tenggara Game in Android Platform (R F Rahmat, R Ramadhan, D Arisandi and O S Sitompul)

	W.a.W (We are Watching) Smart App: Accommodating Social Perception Towards	
	Public Officers Performance (S A Widhoyoko, Sasmoko, L A Nasir, S R	
	Manaluand Y Indrianti)	28
	Nearby Search Indekos Based Android Using A Star (A*) Algorithm (B Siregar, E	
	B Nababan, J A Rumahorbo, U Andayaniand F Fahmi)	29
	The Implementation of A^* Algorithm on Courier Application Development (D Gu-	
	nawan, I Marzuki and A Candra)	29
	Advertisement scheduling on commercial radio station using genetics algorithm (S $$	
	Purnamawati, E B Nababan, B Tsani, R Taqyuddin, R F Rahmat)	30
	Skipping Strategy (SS) for Initial Population of Job-Shop Scheduling Problem (M	
	Abdolrazzagh-Nezhad, E B Nababan, Iryanto and H M Sarim)	30
Aug	gmented Reality	31
	Augmented Reality Social Story for Autism Spectrum Disorder ($M F Syahputra, D$	
	Arisandi, A F Lumbanbatu, L F Kemit, E B Nababan and O Sheta)	31
	An Interactive Augmented Reality Implementation on Hijaiyah Alphabet for Chil-	
	dren Education (R F Rahmat, F Akbar, M F Syahputra, M A Budiman)	31
	Implementation of Augmented Reality to Models Sultan Deli ($M \ F \ Syahputra, \ N \ P$	
	Lumbantobing, B Siregar and Rahmat $R(F)$	32
	Implementation Of Augmented Reality To Train Focus On Children With Special	
	Needs (M F Syahputra, P P Sari, D Arisandi, D Abdullah, D Napitupulu,	
	M I Setiawan, W Albra, Asnawi)	32
Dat	a Science	33
	Supply Chain Management using FP-Growth Algorithm for Medicine Distribution	
	$(A Wahana, D S Maylawati, M Irfan and H Effendy) \ldots \ldots \ldots$	33
	The implementation of two stages clustering (k-means clustering and adaptive neuro	
	fuzzy inference system) for prediction of medicine need based on medical data	
	(A M Husein, M Harahap, S Aisyah, W Purbaand A Muhazir)	33
	Improving Data Quality in the Linked Open Data: A Survey (A Hadhiatma) \ldots	34
	Mapping of Medicine Data with K-Means and Apriori Combinations Based on Pa-	
	tient Diagnosis (N P Dharshinni, H Mawengkangand M K M Nasution)	34
	Feature Weighting Using Particle Swarm Optimization for Learning Vector Quanti-	
	zation Classifier (A Dongoran, S Rahmadani, M Zarlis and Zakarias) \ldots	35
	Social network extraction based on Web: 3. The integrated superficial method (M	
	K M Nasution, O S Sitompul, S A Noah)	35
	An Optimal Generic Model for Multi-Parameters and Big Data Optimizing: A Lab-	
	oratory Experimental Study (D N Utama, N Aniand M M Iqbal)	35
	Improving the Accuracy of k-Nearest Neighbor Using Local Mean Based and Dis-	
	tance Weight (K U Syaliman, E B Nababanand O S Sitompul) $\ldots \ldots$	36
	Multi-documents Summarization based on Clustering of Learning Object using Hi-	
	erarchical Clustering (M Mustamiin, I Budiand H B Santoso)	36
	Application of the fuzzy topsis multi-attribute decision making method to determine	
	scholarship recipients (I Irvanizam)	37
	Decision Support Model for Mosque Renovation and Rehabilitation (Case Study:	
	Ten Mosques in Jakarta Barat, Indonesia) (D N Utama, Y S Triana, M M	
	Iqbal, M Iksal, I Fikriand T Dharmawan)	37

PCA Based Feature Reduction to Improve the Accuracy of Decision Tree C4.5 Clas-	
sification (M Z F Nasution, O S Sitompuland M Ramli)	38
The Gap Values In The Profile Matching Method By Fuzzy Logic (S A Sitepu, S	
Efendiand Z Situmorang)	38
Comparison of Naive Bayes and Decision Tree on Feature Selection Using Genetic	
Algorithm for Classification Problem (S Rahmadani, A Dongoran, M Zarlis,	
Zakarias)	39
Data Matching Approach to Find the Same Company from Multiple Databases $(D$	
Gunawan, M S Lubis and B Azzahry)	39
Bioinformatics and Socio Informatics	40
Bioinformatics approach of three partial polyprenol reductase genes in Kandelia	
obovata (M Basyuni, R Watiand H Sagami)	40
Bioinformatics analysis of the predicted polyprenol reductase genes in higher plants	
$(M Basyuni and R Wati) \ldots \ldots$	40
Investigation of the ripeness of oil palm fresh fruit bunches using bio-speckle imaging	
(R Salambue, A Adnanand M Shiddiq)	41
General Computing	42
Comparative Analysis of Gameplay and Players Emotion in The Most Popular	
Games From Play Store (Riwinoto, N Mahfud and L Lumombo)	42
Indonesia Knowledge Dissemination: A Snapshot $(M \ K \ M \ Nasution)$	42
Assessing ERP SAP Implementation in the Small and Medium Enterprises (SMEs)	
in Indonesia (Yohanes, W Gunawan, R B Ikhsanand Aries)	43
Metacognitive Components in Smart Learning Environment (M Sumadyo, H B San-	
tosoand D I Sensuse)	43
Study to the Current Protection of Personal Data in the Educational Sector in	
Indonesia (E Rosmaini, T F Kusumasari, M Lubisand A R Lubis)	44
Analysis of Factors that Inhibiting Implementation of Information Security Man-	
agement System (ISMS) Based On ISO 27001 (R Tatiara, A N Fajar, B	
Siregarand W Gunawan)	44
Insights to Develop Privacy Policy for Organization in Indonesia ($E Rosmaini$, $T F$	
Kusumasari, M Lubis and Arif Ridho Lubis)	45
Readiness Factors for Information System Strategic Planning among Universities in	
Developing Countries: A Systematic Review (M Irfan, S J Putra, C N Alam,	
A Subiyaktoand A Wahana)	45
Mobile technology for expansion of service range Medan Public Library (A R Siregar	
and H Dewiyana)	46
No research without publication: Early mining $(M K M Nasution)$	46
Design and Architecture of RetailApp: An Application to Support Conventional	
Retailers (I Jaya, J T Tarigan, S M Hardi, E M Zamzami)	46
Molybdenum-99 Production Calculation Analysis of SAMOP Reactor Based on Tho-	
rium Nitrate Fuel (Syarip, E Togatoropand F Yassar)	47
Predicted cycloartenol synthase protein from Kandelia obovata and Rhizophora sty-	
losa using online software of phyre2 and Swiss-Model (M Basyuni, N Sulis-	
tiyono, R Wati1, Sumardi, H Oku, S Baba, H Sagami)	47

Modeling of Sedimentation Process in Water (Tulus, IZ Sefnides, Sawaluddin, Suri-	
atiand M Dwiastuti)	48
Protein modelling of triterpene synthase genes from mangrove plants using phyre2	
and Swiss model (M Basyuni, N Sulistiyono, R Wati, R Hayati, Sumardi, H	
Oku, S Babaand H Sagami)	48
Fluid flow and heat transfer characteristics of enclosure with fin of a double glasses	12
top cover solar collector (H Ambarita, A D Ronowikartoand E Y Setyawan)	49
Effects of the inclination angle on the performance of flat plate solar collector (H	
Ambarita, R E T Siregar, E Y Setyawan)	49
The optimum intermediate pressure of two-stages vapor compression refrigeration	
cycle for Air-Conditioning unit (H Ambarita, H V Sihombing)	50
Numerical study on the effects of absorptivity on performance of flat plate solar	
collector of a water heater (D R S Tambunan, H Ambarita, F H Napitupulu,	
$H Kawai) \ldots \ldots$	50
Simulation evaluation of capacitor bank impact on increasing supply current for	-
alumunium production (S Hasan, K Badra, Suherman, and R Dinzi) \ldots	51
Simulation comparison of proportional integral derivative and fuzzy logic in con-	
trolling AC-DC buck boost converter (A Faisal, S Hasan, and Suherman	2.5
)	51
Measuring the power consumption of social media applications on a mobile device	
(A I Max Dunia, Suherman, A H Rambe and R Fauzi)	51
Geographic Information System	52
Analysis of urban flood vulnerability of Deli River overflow (I Indrawan, R I Siregar	50
and $A P Mulia$)	52
Human Computer Interaction	53
Usability Testing of Indonesia Tourism Promotion Website (U Yunus, Anindito, E	
Tanuar, Maryani)	53
Usability Evaluation of User Interface of Thesis Title Review System (T Yuliati, E	50
Alimudin, GellysaUrva)	93
Implementation and Evaluation of LMS Mobile Application: SCELE Mobile Based	51
on User-Centered Design (<i>R D Banimahendra and H B Santoso</i>)	34
Development of Excavator Training Simulator using Leap Motion Controller (F	54
Fahmi, F Nainggolan, U Andayaniand B Siregar)	55
Image Vision and Computer Graphics	99
Automated Color Classification of Urine Dipstick Image in Urine Examination (R F	
Rahmat, Royananda, M A Muchtar, K Taqiudain, S Adnan, K Ahugranwaiy	55
and R Budiarto) CVD(C - Lineity in Verieur Page Orientation	00
Real-time Detection with Adaboost-SVM Combination in various Face Orientation	55
(<i>R P Fhonna</i> , <i>M K M Nasutionana Tutus</i>)	00
Identification Of Hand Motion Using Background Subtraction Method And Extrac-	
tion Of Image Binary with Backpropagation Neural Network On Skeleton	56
Model (Fauzian, E.F. Wildow, S. Maaenaaana Husinawaii)	00
Facial Expression System On Video Using Widrow Holl (M Junnan, M Zartis and	56
$H Maweng (ang) \dots \dots$	50

v

A Real Time Mohile-based Face Recognition with Fisherface Methods (D. Arisondi	
M F Subputra I L Putri S Purnamawati R F Rahmat P P Sari)	57
Identification Tibia and Fibula Bone Fracture Location using Scapline Algorithm	
(M A Muchtar S E Simaniuntak B F Rahmat H Mawenakana M Zarlis	
O S Sitompul, I D Winanto, II Andayani, M.F. Syahputra, I Sireagrand T.H.	
Nasution)	57
Image Processing Analysis of Geospatial UAV Orthophotos for Palm Oil Plantation	04
Monitoring (F Fahmi D Trianda II Andayani B Sireaar Sawaluddin)	58
Graph-Connected Polygons in a 3D Object to Simulate Deformation (IT Tariagn	00
L Java S M Hardi E M Zamzami)	58
Feature Detection of Curve Traffic Sign Image on The Bandung - Jakarta Highway	90
(M Naseer I Suprindiand S H Supanakat)	50
Classification of Stroke Disease Using Convolutional Neural Network (Seniman U	22
Andouaniand I T Marhun)	50
Virtual Reality Interactive Media for Universitas Sumatera Utara, a campus Intro	03
duction and Simulation (R F Rahmat Anthoniaus M A Machtar A Hisriadi	
and M F Supportra)	60
Hypertensive Retinonethy Identification Through Retinal Fundus Image Using Reak	00
M_{F} propagation Neural Network (M F Suphrutra C Amplia B F Rahmat D	
Abdullah D Nanitunulu M I Setiawan W Albra Nurdin)	60
Identification Male Fertility Through Abnormalities Sperm Based Morphology (Ter-	00
atospermia) using Invariant Moment Method (M.F. Suchnutra, R. Chairani	
Seniman R F Rahmat D Abdullah D Nanitunulu M I Setiawan W Albra	
C I Erliana)	61
An Analysis of Absorbing Image on the Indonesian Text by Using Color Matching	0
(G A Hutagalung, Tulus, Irugato, Y F A Lubis, M Khairani, and Surjati)	61
Real-time monitoring system for elderly people in detecting falling movement using	0.
accelerometer and gyroscope (B Sireaar, U Andayani, R P Babri, Seniman	
and F Fahmi)	62
Korean letter handwritten recognition using deep convolutional neural network on	
android platform (S Purnamawati, D Rachmawati, G Lumanauw, R F Rah-	
mat, and R Tagyuddin)	62
Information Security and Networking	63
Designing Indonesian Teacher Engagement Index (ITEI) Applications Based on An-	
droid (S R Manalu, Sasmoko, S D Permai, S A Widhoyoko, Y Indrianti).	63
Delay and Cost Performance Analysis of the Diffie-Hellman Key Exchange Protocol	
in Opportunistic Mobile Networks (B Soelistijanto and V Muliadi)	63
Developing Cloud-Based Business Process Management (BPM): A Survey (Mercia,	
W Gunawan, A N Fajar, H Alianto, Inayatulloh)	64
Hybrid Cryptosystem RSA-CRT Optimization and VMPC (R Rahmadani, H Mawengk	an-
gand Sutarman)	64
Implemeting Hybrid Cryptography Using Elgamal and Double Playfair Cipher on	
Image Files (S M Hardi, J T Tarigan, N Safrina, I Jaya)	65
Architecture and Design of a NonDedicated Game Lobby (E M Zamzami, I Jaya,	
S M Hardi, J T Tarigan)	65

	Applying transpose matrix on advanced encryption standard (AES) for database	65
	content (E B P Manurung, O S Sitompulana Sunerman)	05
	Computer simulation and implementation of defected ground structure on a mi-	66
	crostrip antenna (H Adrian, A H Rambeana Sunerman)	00
	An Implementation of RC4 Algorithm and Zig-zag Algorithm in a Super Encryption	00
	Scheme for Text Security (M A Budiman, Amaliaand N I Chayanie)	00
	Implementation of Super-Encryption with Trithemius Algorithm and Double Trans-	
	position Cipher in Securing PDF Files on Android Platform (<i>M A Budiman</i> ,	07
	D Rachmawatiand Jessica)	67
	An Implementation of Super-Encryption using RC4A and MDTM Cipher Algo-	
	rithms for Securing PDF Files on Android (M A Budiman, D Rachmawa-	
	tiand M R Parlindungan)	67
	Auditing Albaha University Network Security using in-house Developed Penetration	10252577
	Tool $(M \ E \ Alzahrani)$	67
	A Low-Complexity Subgroup Formation with QoS-Aware for Enhancing Multicast	
	Services in LTE Networks (M Algharem, M H Omar, R F Rahmatand R	
	Budiarto)	68
	Designing a Holistic End-to-End Intelligent Network Analysis and Security Platform	
	(M Alzahrani)	68
	SSL/TLS Vulnerability Detection using Black Box Approach (D Gunawan, E H	
	Sitorus, A Hizriadi and R F Rahmat)	69
	File Text Security using Hybrid Cryptosystem with Playfair Cipher Algorithm and	
	Knapsack Naccache-Stern Algorithm (Amalia, M A Budiman and R Sitepu)	69
	PDF File Encryption on Mobile Phone using Super Encryption of Variably Modified	
	Permutation Composition (VMPC) and Two Square Cipher Algorithm (${\cal D}$	
	Rachmawati, M A Budiman and F Atika)	70
	A Comparative Study of Message Digest 5(MD5) And SHA256 Algorithm (D Rach-	
	mawati, J T Tarigan and A B Clinta)	70
	The recognition of female voice based on voice registers in singing techniques in real-	
	time using hankel transform method and macdonald function (D Abdullah,	
	R Rahim, D Apdilah, S Efendi, T Tulus and S Suwilo)	71
Int	ernet of Things	72
	Implementation of UTAUT model to understand the use of virtual classroom prin-	
	ciple in higher education (B R Adityaand A Permadi) $\ldots \ldots \ldots \ldots$	72
	Diagnostics Vehicles Condition Using OBD-II and Raspberry Pi Technology: Study	
	Literature (J V Moniaga S R Manalu, D A Hadipurnawan and F Sahidi) .	72
	Automated Hydroponics Nutrition Plants Systems using Arduino Uno Microcon-	
	troller Based On Android (P Sihombing, N A Karina, J T Tarigan and M I	
	Syarif)	73
	Application Modeling IPv6 (Internet Protocol Version 6) One-ID card for Iden-	
	tification Number for Effectiveness and Efficiency of Registration Process	
	Identification of Population (A $M H$ Pardede, Y Maulitaand R Buaton)	73
	Implementation of Supply Chain Business Application through Business Model Can-	
	vas and Waterfall Framework Collaborations for fish farmers SMEs in Ulekan	
	Market Bandung (Y Priyadi and A Prasetio)	74

Applying transpose matrix on advanced encryption standard (AES) for database	
content (E B P Manurung, O S Sitompuland Suherman)	65
Computer simulation and implementation of defected ground structure on a mi-	
crostrip antenna (H Adrian, A H Rambeand Suherman)	66
An Implementation of RC4 Algorithm and Zig-zag Algorithm in a Super Encryption	
Scheme for Text Security (M A Budiman, Amaliaand N I Chayanie)	66
Implementation of Super-Encryption with Trithemius Algorithm and Double Trans-	
position Cipher in Securing PDF Files on Android Platform ($M A Budiman$,	
D Rachmawatiand Jessica)	67
An Implementation of Super-Encryption using RC4A and MDTM Cipher Algo-	
rithms for Securing PDF Files on Android (M A Budiman, D Rachmawa-	
tiand $M R Parlindungan) \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots$	67
Auditing Albaha University Network Security using in-house Developed Penetration	
$Tool (M E Alzahrani) \dots \dots$	67
A Low-Complexity Subgroup Formation with QoS-Aware for Enhancing Multicast	
Services in LTE Networks (M Algharem, M H Omar, R F Rahmatand R	00
Budiarto)	68
Designing a Holistic End-to-End Intelligent Network Analysis and Security Platform	69
(<i>M Alzahrani</i>) Photo Device the Device of the Concerner F. H.	08
SSL/TLS Vulnerability Detection using Black Box Approach (D Gunawan, E H	60
Sitorus, A Hizriadi and R F Kanmat)	09
File Text Security using Hybrid Cryptosystem with Playian Cipner Algorithm and Keywork Newsche Stern Algorithm (Amplia, M.A. Budiman and P. Siteny)	60
DDE Eile Exemption on Mobile Phone using Super Encryption of Variably Modified	03
PDF File Encryption on Mobile Filone using Super Encryption of Variably Mounted	
Permutation Composition (VMIC) and Two Square Cipiler Algorithm (D Rachmewati, $M \neq Budiman and F \neq Atika)$	70
A Comparative Study of Message Digest 5(MD5) And SHA256 Algorithm (D Rach-	
mawati I T Tariaan and A B Clinta)	70
The recognition of female voice based on voice registers in singing techniques in real-	
time using hankel transform method and macdonald function (D Abdullah,	
R Rahim, D Apdilah, S Efendi, T Tulus and S Suwilo)	71
Internet of Things	72
Implementation of UTAUT model to understand the use of virtual classroom prin-	
ciple in higher education (B R Adityaand A Permadi)	72
Diagnostics Vehicles Condition Using OBD-II and Raspberry Pi Technology: Study	
Literature (J V Moniaga S R Manalu, D A Hadipurnawan and F Sahidi) .	72
Automated Hydroponics Nutrition Plants Systems using Arduino Uno Microcon-	
troller Based On Android (P Sihombing, N A Karina, J T Tarigan and M I	
Syarif)	73
Application Modeling IPv6 (Internet Protocol Version 6) One-ID card for Iden-	
tification Number for Effectiveness and Efficiency of Registration Process	
Identification of Population (A $M H$ Pardede, Y Maulitaand R Buaton)	73
Implementation of Supply Chain Business Application through Business Model Can-	
vas and Waterfall Framework Collaborations for fish farmers SMEs in Ulekan	
Market Bandung (Y Priyadi and A Prasetio)	74

E-Learning Process Maturity Level: A Conceptual Framework (A Rahmah, H B	
Santoso and Z A Hasibuan)	74
Develop Applications Based on Android: Teacher Engagement Control of Health	
(TECH) (Sasmoko, S R Manalu, S Anindyo Widhoyoko, Y Indriantiand	
Suparto)	75
Microcontroller Based Automatic Temperature Control for Oyster Mushroom plants	
(P Sihombing, T P Astuti, Herriyance and D Sitompul)	75
Mobile/Android Application for QRS Detection using Zero Cross Method (M I	
Rizqyawan, A I Simbolon, M A Suhendra, M F Amriand D E Kusuman-	
dari)	76
Main Factors in E-Learning for the Equivalency Education Program (E-LEEP) $(M$	
B Yeland S Sfenrianto)	76
Attendance Fingerprint Identification System using Arduino and Single Board Com-	
puter (M A Muchtar, Seniman, D Arisandi, I Aulia, S Hasanah)	76
Developing and Pilot Testing M-Health Care Application for Pregnant and Toddlers	
Based on User Experience (I D Lestantri, Putrima, A Sabigand E Suherlan)	77
Analysis Spectrum of ECG Signal and QRS Detection during Running on Treadmill	
(M A Suhendra, M Ilham R, A I Simbolon, M Faizal A and A Munandar)	77
Application of Open Garden Sensor on Hydroponic Maintenance Management (S	
Nasution, B Siregar, M Kurniawan, H Pranoto, U Andayani, F Fahmi)	78
Development of Building Security Integration System using sensors, Microcontroller	
and GPS (Global positioning system) based Android Smartphone (P Sihomb-	
ing, Y M Siregar, J T Tarigan, I Jaya)	78
Clean water billing monitoring system using flow liquid meter sensor and SMS gate-	
way (F Fahmi, A Hizriadi, F Khairani, U Andayani, and B Siregar)	79
Natural Language Processing	80
Improved Line Segmentation Framework for Sundanese Old Manuscripts (E Paulus,	
M Suryani, S Hadi)	80
Stop Words in Review Summarization Using TextRank (Willy, S R Manalu, A M	
Sundjaja, Noerlina, R Lubis and A S Gultom) $\ldots \ldots \ldots \ldots \ldots$	80
The recognition of female voice based on voice registers in singing techniques in real-	
time using hankel transform method and macdonald function (R Meiyanti,	
A Subandi, N Fuqara, M A Budimanand A P U Siahaan)	81
Hierarchical Rhetorical Sentence Categorization for Scientific Papers ($G \ H \ Rach-$	
man, M L Khodraand D H Widyantoro)	81
Specific Acoustic Models for Spontaneous and Dictated Style in Indonesian Speech	
Recognition (C B Vista, C H Satriawan, D P Land D H Widyantoro)	82
5W1H Information Extraction with CNN-Bidirectional LSTM (A Nurdinand N U	
Maulidevi)	82
Plagiarism Detection for Indonesian Language using Winnowing with Parallel Pro-	
cessing (Y Arifin, S M Isa, L A Wulandhariand E Abdurachman)	82
Determination of Quality Television Programmes Based on Sentiment Analysis on	
Twitter (A Amalia, W Oktinas, I Aulia and R F Rahmat)	83
Building Automatic Customer Complaints Filtering Application Based on Twitter	
in Bahasa Indonesia (D Gunawan, R Siregar, R F Rahmat and A Amalia).	83

Committee

Honorary Chair

Prof. Dr. Runtung Sitepu, S.H., M.Hum. (Rector University of Sumatera Utara, Indonesia)

International Board

Prof. Hiromi Homma (Toyohashi University of Technology, Japan)
Prof. Madya Dr. Rahmita Wirza O. K. Rahmat (Universiti Putra Malaysia, Malaysia)
Prof. Dr. Salwani Abdullah (The National University of Malaysia, Malaysia)
Prof. Dr. Masashi Daimaruya (Muroran Institute of Technology, Japan)
Prof. Dr. Rahmat Budiarto (Albaha University, Saudi Arabia)
Muhammad Fermi Pasha, B.Comp.Sc., M.Sc., Ph.D. (Monash University, Malaysia Campus)
Dr. Osama Sheta (Zagazig University, Egypt)
Dr. Mu'awya Al Dalaien, (Abu Dhabi and Khalifa City Womens Colleges, UAE)

Steering Committees

Prof. Dr. Hideki Kawai (Muroran Institute of Technology, Japan) Prof. Zainal A.Hasibuan, Ir., MLS, Ph.D. (University of Indonesia, Indonesia) Prof. Dr. Opim Salim Sitompul (Universitas Sumatera Utara, Indonesia) Prof. Dr. Herman Mawengkang (Universitas Sumatera Utara, Indonesia) Prof. Dr. Saib Suwilo (Universitas Sumatera Utara, Indonesia) Prof. Dr. Muhammad Zarlis, M.Sc. (Universitas Sumatera Utara, Indonesia) Prof. Dr. rer.nat. Dedi Rosadi, M.Sc. (University of Gadjah Mada, Indonesia) Dr. Ahmed H. Alahmadi (Albaha University/Taibah University, KSA) Dr. Mohammed Y. Alzahrani (Albaha University, KSA) Dr. Adil F. Alharthi (Albaha University, KSA) Drs. Mahyuddin K. M. Nasution, M.IT, Ph.D. (Universitas Sumatera Utara, Indonesia) Dr. Ir. Rinaldi Munir, MT (Bandung Institute of Technology, Indonesia) Dr. Fitri Arnia, M.Eng.Sc (Syiah Kuala University, Indonesia) Dr. Eng. Himsar Ambarita (Universitas Sumatera Utara, Indonesia) Benny B. Nasution, Ph.D. (Politeknik Negeri Medan, Indonesia) Tami Alwajeeh (Albaha University, KSA) Ahmed Alghamdi (Albaha University, KSA)

Chair

Dr. Erna Budhiarti Nababan, M.IT

Technical Chair

Romi Fadilah Rahmat, B.Comp.Sc., M.Sc.

Co. Chair

Dian Rachmawati, S.Si., M.Kom Jos Timanta Tarigan, S.Kom., M.Sc. Mohammad Andri Budiman, S.T., M.Comp.Sc., M.E.M. Dani Gunawan, S.T., M.T.

Members

Prof. Dr. Muhammad Zarlis Dr. Ir. Fahmi, M.Sc., IPM Emerson Sinulingga, Ph.D Dr. Elviawati Zamzami, S.T., M.T., M.M. Dr. Sawaluddin, M.IT Dr. Maya Silvi Lydia, M.Sc. Dr. Poltak Sihombing, M.Kom. Dr. Syahril Efendi, M.IT Mohammad Fadly Syah Putra, M.Sc. Muhammad Anggia Muchtar, ST, M.MIT Amalia, S.T., M.T. Indra Aulia, S.Ti., M.Kom. Ivan Jaya, S.Si., M.Kom. Sarah Purnamawati, S.T., M.Sc. Dedy Arisandi, S.T., M.Kom. Ulfi Andayani, S.Kom., M.Kom. Melvani Hardi, S.Kom., M.Kom. Marischa Elveny S.TI, M.Kom. Tigor Hamonangan Nasution, S.T., M.T. Taufiq Bin Nur, S.T., M.Eng. Baihaqi Siregar, S.Si., M.T. Amer Sharif, S.Si., M.Kom. Elviwani ST, S.Kom, M.Kom . Handrizal, S. Si, M. Comp. Sc Sajadin Sembiring S.Si, M.Comp.Sc. Ade Chandra, S.T., M.Kom. Herriyance, S.T., M.Kom.

3



CERTIFICATE



This certificate is awarded to

Bambang Soelistijanto

for the contribution as **Presenter** of

Delay and Cost Performance Analysis of the Diffie-Hellman Key Exchange Protocol in Opportunistic Mobile Networks

"Empowering the Society through Information Technology, Computational Science, and Engineering Research" International Conference on Computing and Applied Informatics (ICCAI) 2017

Organized by FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY UNIVERSITAS SUMATERA UTARA

Medan (Indonesia), 29 - 30 November 2017

Dr. Erna Budhiarti Nababan, M.IT. Chairman ICCAI 2017

PROCEEDING PUBLISHER:

IOP Conference Series conferenceseries.iop.org **IOP** Publishing

Drs. Mahyuddin K.M. Nasution, M.IT.,Ph.D. Vice Rector for Research, Community Service, and Cooperation Universitas Sumatera Utara

PAPER • OPEN ACCESS

Delay and cost performance analysis of the diffie-hellman key exchange protocol in opportunistic mobile networks

To cite this article: B Soelistijanto and V Muliadi 2018 J. Phys.: Conf. Ser. 978 012016

View the article online for updates and enhancements.



IOP ebooks[™]

Bringing you innovative digital publishing with leading voices to create your essential collection of books in STEM research.

Start exploring the collection - download the first chapter of every title for free.

Delay and cost performance analysis of the diffie-hellman key exchange protocol in opportunistic mobile networks

B Soelistijanto and V Muliadi

Department of Informatics, Sanata Dharma University, Yogyakarta, Indonesia

Email: b.soelistijanto@usd.ac.id, vmuliadi@max-metal.us

Abstract. Diffie-Hellman (DH) provides an efficient key exchange system by reducing the number of cryptographic keys distributed in the network. In this method, a node broadcasts a single public key to all nodes in the network, and in turn each peer uses this key to establish a shared secret key which then can be utilized to encrypt and decrypt traffic between the peer and the given node. In this paper, we evaluate the key transfer delay and cost performance of DH in opportunistic mobile networks, a specific scenario of MANETs where complete end-to-end paths rarely exist between sources and destinations; consequently, the end-to-end delays in these networks are much greater than typical MANETs. Simulation results, driven by a random node movement model and real human mobility traces, showed that DH outperforms a typical key distribution scheme based on the RSA algorithm in terms of key transfer delay, measured by average key convergence time; however, DH performs as well as the benchmark in terms of key transfer cost, evaluated by total key (copies) forwards.

1. Introduction

The subject of key distribution is one of the important issues in key management [1]. An obvious method of distribution of keys is simply by hand. This method was frequently used in the days of couriers. However, it is used only infrequently nowadays, since most key distribution is performed automatically. Automatic distribution is not only more convenient, but often even essential; for instance, in telephone or computer networks, which require two parties to transmit their security keys along the same communication line. In these cases often two types of keys are employed: keys which are used for the actual security of the data (so-called session keys), and keys which are used for the security of these session keys during transmission (so-called *transportation keys*).

The Diffie-Hellman (DH) protocol [2] is a method for exchanging keys in the network. In this algorithm, two parties unknown to one another can set up a private however arbitrary key for their symmetric key cryptosystem. Along these lines, there is no requirement for Alice and Bob to meet ahead of time, or utilize a safe dispatch, or utilize some other secret means, to choose a key. DH was the first practical method for setting up a "shared secret" over an unsecured communication channel. The security of this algorithm is based on the hardness of a certain computational problem. This paper discusses the delay and cost performance analysis of the DH key exchange protocol in opportunistic mobile networks (OMNs), a class of delay-tolerant networks (DTNs) [3] where nodes come into contact with each other at unpredictable intervals and the duration of each contact is also unpredictable. The area of key management in DTNs is relatively new and many research challenges remain to date [4]. Traditional key management is not suitable for DTNs due to the environment

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI. Published under licence by IOP Publishing Ltd 1

limitations and technical constraints, e.g. long round trip delays and frequent link disconnections. The author in [5] identified some requirements for key management in DTNs. The works in [6,7,8] proposed new solutions to address the security issues of key management in DTNs.

In this paper, however, we discuss the key transfer delay and cost performance analysis of DH in OMNs. To best of our knowledge, the performance evaluation of DH in OMNs in terms of key transfer delay and cost has not been discussed before. In delay-tolerant networks, such as OMNs, where end-to-end delay is very large, key transfer delay is an important aspect that directly affects the performance of DH. Indeed, a low key transfer latency is required to achieve high performance of DH. In this analysis, we consider average key convergence time to identify the key transfer delay performance of DH in OMNs. Besides transfer delay, delivery cost is an important parameter in mobile communication networks, since mobile devices typically have limited resources, e.g. storage and power. Furthermore, we use total key (copies) forwards as a metric to quantify the key transfer cost of DH in OMNs.

The rest of the paper is structured as follows. Section 2 gives an overview of the DH key exchange algorithm. Section 3 describes our experimental setup for evaluating the key transfer delay and cost performance of DH in OMNs. A performance analysis of the protocol compared to a typical key distribution scheme based on the RSA algorithm is reported in Section 4. Finally, Section 5 concludes the paper.

2. The Diffie-Hellman Key Exchange Protocol

The Diffie-Hellman (DH) protocol offers an efficient method for exchanging keys in the network. Consider a network of n nodes (parties) who communicate bilaterally in an enciphered form, controlled by a key. In the network, the total number of keys is n(n-1) in which two nodes are involved during each communication. Each node must therefore have (n-1) keys available to be able to communicate with the other (n-1) nodes. This kind of communication will require a large number of keys and managing these keys correctly can be very complicated.



Figure 1. The Diffie-Hellman key exchange protocol

Diffie and Hellman (1976) have devised a method with which the number of keys can be reduced drastically. Their system is based on the exponential and logarithmic functions. Given that all nodes in the network select the same prime number p and a base g. Each node N_i may now choose a secret key x_i and calculates y_i according to $y_i = g^{x_i} \pmod{p}$; the value of y_i is then made public. Suppose a node N_i wishes to communicate with a node N_j . This will require a mutual session key K_{ij} , with which the message can be enciphered and deciphered. Node N_i must first calculate $K_{ij} = y_j^{x_i} \pmod{p}$. N_i can perform this calculation since p is published, x_i is N_i 's own key, and y_j was disclosed to N_i by N_j . On the other hand, node N_j can calculate the session key $K_{ji} = y_i^{x_j} \pmod{p}$. This will result in exactly

the same session key for both nodes ($K_{ij} = K_{ji}$), due to symmetry of the power function. In figure 1, we illustrate the DH key exchange protocol between two parties, Alice and Bob.

3. Simulation Setup for Evaluating the Diffie-Hellman Protocol in OMNs

In this section, we discuss the choice of simulation scenarios, evaluation metrics, and benchmark protocols to evaluate the delay and cost performance of DH in OMNS. We implement DH using the ONE simulator [9], an event-driven simulator for mobile opportunistic networks. In our simulations, the number of nodes and the length of simulation time vary depending on the node mobility scenarios. The node buffer size and the message size are set to 10 MB and 4 kB, respectively. Moreover, we assume that a message can only carry a single key. The simulations were run 10 times for both DH and its protocol benchmark with different random number seeds.

For the simulation's node mobility scenario, we use a random movement model and real human mobility traces. For the latter case, we exploit the Infocomm [10], Reality [11] and Sassy [12] human contact datasets. In Infocomm, 41 iMote Bluetooth-enabled devices were distributed to attendees at the IEEE Infocomm conference in Miami in 2005. These devices recorded the human contacts occurred during the 3-day seminar. In Reality, on the other hand, 100 smart phones were deployed among the students and staffs of MIT over period of 9 months. These phones were running software that logged contacts with other phones, capturing academic activities in the campus over an academic year. The Sassy trace, in contrast, was collected using a mobile sensor network with TMote invent devices carried by 25 participants from the University of St. Andrews for period of 74 days.

For performance analysis, we use two evaluation metrics as follows:

- 1. Average key convergence time: the mean of the times required before all the nodes in the network can reach knowledge regarding the latest updated of the key of a particular node.
- 2. Total key (copies) forwards: the total number of key (copies) forwarded during node contacts throughout the simulation time.



Figure 2. A key distribution scheme based on the RSA algorithm

In order to benchmark the performance of DH, we consider a typical key distribution scheme based on the RSA algorithm (hereafter called RSA) as follows. In figure 2, consider two parties, Alice and Bob, whose public keys P_A and P_B , respectively, are made available in the network, and secret keys are denoted by S_A and S_B . Suppose that Alice wishes to transfer a (session) key K to Bob. Alice may do this by first enciphering the key K with her own secret key and subsequently enciphering this result with Bob's public key. The total result can be written as $(K^{S_A})^{P_B}$. Then, Bob can find the original key K by decrypting the received message with his own secret key followed by a second decipherment with Alice's public key.

In our simulations, a new public key is generated at a randomly selected node at a rate of one key per hour for both DH and RSA. Moreover, in RSA, we assume that after a node broadcast its new public key to all nodes in the network, the node promptly sends an individual encrypted session key *K*

to each the network node. Therefore, the average key convergence time in RSA is calculated as the mean of the times when all the network nodes are able to find the original key K of a node by decrypting the received messages minus the time when K is created in the original node. Furthermore, the peer node is able to disclose the encrypted session key K whenever it has knowledge of the latest updated public key of the original node. This is however not the case in DH since K is never transported over the network but is calculated autonomously on both communicating end nodes, providing that each end node has information of the public key of the other end node (as shown in figure 1). As a result, the key convergence time in DH can be calculated as the average of times when all nodes in the network receive a particular node' public key minus the time when the key is created in the original node.

Finally, to broadcast nodes' public keys in the network (in DH and RSA) and to deliver session keys K to the particular destination (in RSA) we use Epidemic routing [13]. The algorithm is floodingbased in nature, as nodes continuously replicate and transmit messages to newly discovered contacts that do not already possess a copy of the message. Epidemic routing results in a high per message delivery probability and the lowest delay. Despite its benefits, this oblivious forwarding strategy consumes much the constraint resources of mobile nodes, such as storage and power.

4. Simulation Results

In this section, we present the simulation results that compare the key transfer delay and cost performance of DH with that of RSA in OMNs. In the first experiment, we consider a random node movement model in the simulation. In the second experiment, we use real human contact data traces as the simulation's node mobility scenario.

4.1. Random Node Movement Scenario

We now discuss the key transfer delay and cost performance comparison results between DH and RSA in a random node movement scenario. We used a synthetic random walk model available in the ONE simulator's library. In this setting, node contacts are spread evenly between the nodes over the network. From the simulation results, in figure 3 we depict the key transfer delay and cost performance comparison results of DH and RSA in the random node scenario. We defined a fixed simulation area at 2500m x 2500m but varied the number of nodes in the network from 50 up to 150 nodes. The length of the simulation time was 2500ks for both protocols.



Figure 3. Key transfer delay and cost performance comparison of DH and RSA in the random node mobility scenario

Figure 3 shows that DH outperforms RSA in terms of key transfer delay, measured by average key convergence time. This is because the key convergence time in DH relies merely on the speed of public keys spreading in the network. In RSA, on the other hand, the key convergence time depends not only on the broadcast rate of public keys to all the network nodes, but also on the delivery time of session keys to their destinations (unicast transmissions). Moreover, the increase of total nodes in the

2nd International Conference on Computing and Applied Informatics 2017IOP PublishingIOP Conf. Series: Journal of Physics: Conf. Series 978 (2018) 012016doi:10.1088/1742-6596/978/1/012016

network significantly reduces the key transfer delay in RSA, but it gives little impact in DH. In terms of key transfer cost performance, on the other hand, both protocols perform almost similarly. Indeed, DH slightly reduces the total key (copies) forwards of RSA. In RSA, the majority of key (copies) distributed in the network are nodes' public keys and the delivery of session keys consequently less contributes on the total key (copies) forwarded during the simulation time. In line with this, the absence of the unicast transmissions of session keys in DH slightly decreases the key transfer cost below that of RSA. Finally, the key transfer cost grows linearly with the increasing of total nodes in the network for both DH and RSA.

4.2. Real Human Mobility Scenario

In the second experiment, we consider a real human mobility scenario to evaluate the key transfer delay and cost performance of DH compared to that of RSA. We used Reality, Sassy and Infocomm as the simulation's node mobility scenario. We again used the simulation settings of the previous experiment, except for the number of nodes and the length of simulation time which vary depending on the datasets.

From the simulation results, in figure 4 we depict the key transfer delay performance comparison of DH and RSA, measured by avg. key convergence time, for all datasets. It is clear that DH outperforms RSA in this performance metric (i.e. a lower avg. key convergence time of DH compared to that of RSA) in all there datasets. Moreover, the key transfer delay performance's difference between DH and RSA is more obvious in Reality and Sassy. In these datasets, node contacts are sparser (than Infocomm's) and, as a result the delivery time of session keys to the destinations is larger, leading to the significant increase of the key transfer delay of RSA beyond that of DH in both Reality and Sassy.



Figure 4. Key transfer delay performance comparison of DH and RSA in the real human mobility scenario



Figure 5. Key transfer cost performance comparison of DH and RSA in the real human mobility scenario

Finally, in figure 5 we show the key transfer cost performance comparison results, measured by total key (copies) forwards, for DH and RSA in all the datasets. As in the random node mobility scenario, both protocols perform nearly equally in this evaluation metric and DH slightly reduces the total key (copies) forwards of RSA in all three datasets. The explanation of this is similar to that given in the key transfer cost performance evaluation in the previous scenario as follows: in RSA, the unicast transmissions of session keys give a little impact on the total key (copies) forwarded during the simulation time since the majority of the key (copies) distributed in the network are nodes' public

keys. According this, the absence of the unicast transmissions of session keys in DH results in a small decrease of the key transfer cost below that of RSA in all the datasets.

5. Conclusion

We have discussed the delay and cost performance evaluation of the DH key exchange protocol in OMNs. We have demonstrated that DH outperforms a typical key distribution scheme based on RSA in terms of key transfer delay, measured by average key convergence time, in both the random node mobility and real human mobility scenarios. However, in the key transfer cost performance DH performs as well as RSA in both scenarios. Indeed, DH slightly reduces the total key (copies) forwards below that of RSA.

References

- [1] Van der Lubbe J C A 1998 *Basic Methods of Cryptography* (London: Cambridge University Press) chapter 8 pp 194-199
- [2] Diffie W and Hellman M E 1976 New Directions in Cryptography *IEEE Trans. on Information Theory* **IT-22** (New Jersey: IEEE) pp 644-650
- [3] Fall K 2003 A Delay-Tolerant Network Architecture for Challenged Internets *Proc. ACM SIGCOMM* (Karlsruhe: ACM) pp 27-34
- [4] Clarke N L, Katos V, Menesidou S-A, Ghita B and Furnell S 2012 A Novel Security Architecture for a Space-Data DTN Proc. Int. Conf. on Wired/Wireless Internet Communications (Santorini: Springer) pp 342-349
- [5] Menesidou S A, Katos V and Kambourakis G 2017 Opportunistic Key Management in Delay-Tolerant Networks Int. J. Information and Computer Security 9 (Geneva:Inderscience) pp 212-228
- [6] Menesidou S A and Katos V 2012 Authenticated Key Exchange (AKE) in Delay-Tolerant Networks *Proc. Int. Conf. on Information Security* (Creta: Springer) pp 49-60
- [7] Andrade D and Albini L C P 2016 Fully Distributed Public Key Management through Digital Signature Chains for Delay and Disrupt Tolerant Networks Proc. Int. Conf. on Mobile Ad Hoc and Sensor Systems (Brasilia: IEEE) pp 316-324
- [8] Lv X, Mu Y and Li H 2014 Non-Interactive Key Establishment for Bundle Security Protocol of Space DTNs *IEEE Trans. on Information Forensics and Security* 9 (New Jersey: IEEE) pp 5-13
- [9] Keranen A, Ott J, and Karkkainen T 2009 The ONE Simulator for DTN Protocol Evaluation Proc. Int. Conf. on Simulation Tools and Techniques (Rome: IEEE) pp 1-10
- [10] Scott J, Gass R, Crowcroft J, Hui P, Diot C and Chaintreau A 2009 CRAWDAD Dataset Cambridge/Haggle/Infocom (online: http://crawdad.cs. dartmouth. edu/cambridge/haggle/ imote/infocom)
- [11] Eagle N and Pentland A 2006 Reality Mining: Sensing Complex Social Systems J. Personal and Ubiquitous Computing 10 (London: Springer-Verlag) pp 255-268
- [12] Bigwood G, Henderson T, Rehunathan D, Bateman M, and Bhatti S 2011 CRAWDAD Dataset st_andrew/sassy v. 2011-06-03 (online: http://crawdad.org/st_andrews/sassy/20110603/)
- [13] Vahdat A and Becker D 2000 Epidemic Routing for Patially Connected Ad Hoc Networks *Tech. Report CS-200006 Duke Univ.* (Durham: Duke University)