

IT'15
ŽABLJAK

XX

međunarodni naučno - stručni skup

**INFORMACIONE
TEHNOLOGIJE**

SADAŠNJOST I BUDUĆNOST

Urednik
Božo Krstajić

IT'15

**INFORMACIONE
TEHNOLOGIJE**

- SADAŠNJOST I BUDUĆNOST -

Urednik
Božo Krstajić

*Zbornik radova sa XX međunarodnog naučno - stručnog skupa
INFORMACIONE TEHNOLOGIJE - sadašnjost i budućnost
održanog na Žabljaku od 23. do 28. februara 2015. godine*

Zbornik radova
INFORMACIONE TEHNOLOGIJE - sadašnjost i budućnost 2015

Glavni urednik
Prof.dr Božo Krstajić

Izdavač
Univerzitet Crne Gore
Elektrotehnički fakultet
Džordža Vašingtona bb., Podgorica
www.etf.ucg.ac.me

Tehnička obrada
Aleksandra Radulović
Centar Informatičnog Sistema
Univerziteta Crne Gore

Tiraž
150

Podgorica 2015.

Sva prava zadržava izdavač i autori

Organizator

Elektrotehnički fakultet, Univerzitet Crne Gore

Suorganizatori:

Elektrotehnički fakultet, Univerzitet u Beogradu

Elektrotehnički fakultet, Univerzitet u Banja Luci

Elektronski fakultet, Univerzitet u Nišu

Fakultet tehničkih nauka, Univerzitet u Novom Sadu

Skup su podržali:

Ministarstvo za informaciono društvo i telekomunikacije

Agencija za elektronske komunikacije i poštansku djelatnost

doMEn d.o.o.

Terna Crna Gora

Pošta Crne Gore

Programski odbor

Dr Novak Jauković, Elektrotehnički fakultet, Podgorica, MNE
Dr Ljubiša Stanković, Elektrotehnički fakultet, Podgorica, MNE
Dr Zdravko Uskoković, Elektrotehnički fakultet, Podgorica, MNE
Dr Vujica Lazović, Ekonomski fakultet, Podgorica, MNE
Dr Branko Kovačević, Elektrotehnički fakultet, Beograd, SRB
Dr Milorad Božić, Elektrotehnički fakultet, Banja Luka, BIH
Dr Miroslav Bojović, Elektrotehnički fakultet, Beograd, SRB
Dr Zoran Jovanović, Elektrotehnički fakultet, Beograd, SRB
Dr Milica Pejanović-Đurišić, Elektrotehnički fakultet, Podgorica, MNE
Dr Despina Anastasiadou, Research & Development Innovation Academy, Solun, GRC
Dr Dejan Popović, Elektrotehnički fakultet, Beograd, SRB
Dr Gabriel Neagu, National Institute for Research & Development in Informatics, Bucharest, ROU
Dr Božo Krstajić, Elektrotehnički fakultet, Podgorica, MNE
Dr Tomo Popović, Texas A&M Univerzitet, College Station, TX, USA
Dr Milovan Radulović, Elektrotehnički fakultet, Podgorica, MNE
Dr Le Xie, Texas A&M University, College Station, TX, USA
Dr Sašo Gelev, Elektrotehnički fakultet, Radoviš, MKD
Dr Budimir Lutovac, Elektrotehnički fakultet, Podgorica, MNE
Dr Igor Radusinović, Elektrotehnički fakultet, Podgorica, MNE
Dr Alex Sprintson, Texas A&M University, College Station, TX, USA
Dr Igor Đurović, Elektrotehnički fakultet, Podgorica, MNE
Dr Miloš Daković, Elektrotehnički fakultet, Podgorica, MNE
Dr Milutin Radonjić, Elektrotehnički fakultet, Podgorica, MNE
Dr Ana Jovanović, Elektrotehnički fakultet, Podgorica, MNE
Dr Vesna Rubežić, Elektrotehnički fakultet, Podgorica, MNE
Dr Ramo Šendelj, Fakultet za Informacione Tehnologije, Podgorica, MNE
Dr Stevan Šćepanović, Prirodno-matematički fakultet, Podgorica, MNE

Organizacioni odbor

Dr Novak Jauković, Elektrotehnički fakultet, Podgorica
Dr Božo Krstajić, Elektrotehnički fakultet, Podgorica / CIS UCG
Dr Milovan Radulović, Elektrotehnički fakultet, Podgorica
Dr Zoran Veljović, Elektrotehnički fakultet, Podgorica
Dr Ana Jovanović, Elektrotehnički fakultet, Podgorica
Dr Saša Mujović, Elektrotehnički fakultet, Podgorica
MSc Žarko Zečević, Elektrotehnički fakultet, Podgorica
Vladan Tabaš, dipl.ing., Čikom, Podgorica

Sekretarijat

Aleksandra Radulović, CIS Univerzitet Crne Gore

P R E D G O V O R

Poštovani učesnici i čitaoci,

Pred vama je jubilarni XX zbornik radova međunarodnog naučno-stručnog skupa “INFORMACIONE TEHNOLOGIJE – sadašnjost i budućnost” (IT’15) koji je uspješno održan od 23. do 28. februara 2015. godine na Žabljaku. Programski odbor je izvršio selekciju kvalitetnih radova koji su pred vama, a najbolji među njima će biti prošireni i objavljeni u časopisu Elektrotehničkog fakulteta Univerziteta Crne Gore u Podgorici ("ETF Journal of Electrical Engineering").

Ovakav jubilej i jubilarni Zbornik je prilika da se osvrnemo i na misiju ove konferencije, na neke univerzalne vrijednosti koje smo zadržali, a i na inovacije koje smo uveli. U proteklih 20 godina IT je prepoznat kao relevantna, nekad nacionalni, sada međunarodni naučno stručni skup koji se trudio i trudi da omogući širokom spektru naučnika i stručnjaka prezentaciju, kako rezultate naučnih istraživanja i trendova, tako i uspješnih stručnih projekata i rješenja. Nijesmo se nikad ograničavali samo na ICT, već smo ostavljali prostor za sve oblasti nauke i djelatnosti u kojima se primjenjuje ICT, a teško je danas naći izuzetke. Trudili smo se da se na IT-u pojavljuju najeminentniji naučnici i stručnjaci, ali i mladi istraživači, inženjeri, a zadnje dvije godine i studenti. Uveli smo i neke nove prakse kao posledice primjene tehnologija koje promoviramo: elektronsku obradu korespondencije sa autorima, elektronski proces recenzije, objavljivanja radova na sajtu, katalogizaciju istih te online praćenje i prezentovanje radova. Proširili smo djelatnost konferencije sa učešćem kompanija i institucija sa uspješnim projektima, a posebno smo ponosni i na studentsko učešće. Ove godine smo posvetili čitav segment samo studentima i pripremili posebna predavanja i prezentacije za njih. Konačno i tradicionalno, vjerovatno jedan od značajnih argumenata za učešće na IT-u je neponovljiva priroda Durmitora, gostoprimstvo grada i poslovnično nezaboravna druženja učesnika.

Ovdje je svakako mjesto da se pomenu i rodonačelnici ovog skupa, koji su prije 20 godina započeli ovu konferenciju: prof. dr Novak Jauković, prof. dr Srbijanka Turajlić, prof. dr Dejan Popović i prof. dr Srđan Stanković, i čije je aktivno učešće u radu jubilarnog skupa potvrda da isti ima kontinuitet, kredibilitet i budućnost.

Sve detalje o ovom, prošlim i narednom skupu možete naći na web adresi konferencije www.it.ac.me.

Prof. dr Božo Krstajić

SADRŽAJ

Dejan Popović, Lana Popović Maneski (<i>Rad po pozivu</i>) ROBOTIKA U REHABILITACIJI: EGZOSKELETI I PROTEZE ZA GORNJE EKSTREMITETE ROBOTICS FOR REHABILITATION: EXOSKELETONS AND PROSTHESES FOR UPPER LIMBS... 1	
Tomo Popović NAPREDNE TEHNIKE U PYTHON-U: DEKORATORI ADVANCED PYTHON TECHNIQUES: DECORATORS	7
Žarko Zečević, Zdravko Uskoković, Božo Krstajić NOVI ALGORITAM ZA ESTIMACIJU FAZORA U ELEKTROENERGETSKIM SISTEMIMA A NEW ALGORITHM FOR PHASOR ESTIMATION OF POWER SYSTEMS.....	11
Vladana Mrdak, Božo Krstajić PRIMJER IMPLEMENTACIJE RJEŠENJA ZA BACKUP I RESTORE PODATAKA AN IMPLEMENTATION EXAMPLE OF BACKUP AND RESTORE SOLUTION	15
Marija Blagojević, Maja Božović, Zoran Jevremović, Miloš Papić ANALIZA OBRAZACA PONAŠANJA KORISNIKA RAZLIČITIH STILOVA UČENJA U OKVIRU KOLABORATIVNIH MODULA ANALYSIS OF USERS' BEHAVIOUR PATTERNS OF STUDENTS WITH DIFFERENT LEARNING STYLES WITHIN THE COLLABORATION MODULES	19
Bogdan Mirković PRIKAZIVANJE ONTOLOGIJA U MIKS-METODSKIM ISTRAŽIVANJIMA MEĐUORGANIZACIONIH INFORMACIONIH SISTEMA PRESENTING ONTOLOGY IN MIXED METHOD RESEARCH OF INTERORGANIZATIONAL INFORMATION SYSTEMS.....	23
Bogdan Mirković INTEGRACIJA METODOLOGIJA U RAZVOJU SOFTVERA ZA PODRŠKU INFORMACIONOM SISTEMU INTEGRATION OF METHODOLOGY IN SOFTWARE DEVELOPMENT FOR SUPPORTING INFORMATION SYSTEM.....	27
Jelena Šoškić, Budimir Lutovac IMPLEMENTACIJA PROGRAMSKOG PAKETA WIPL-D ZA PRORAČUN PRILAGOĐENJA SA JEDNIM REAKTIVNIM ELEMENTOM IMPLEMENTATION OF THE WIPL-D PROGRAM PACKAGE FOR SINGLE STUB MATCHING....	31
Luka Lazović, Ana Jovanović, Vesna Rubežić IMPLEMENTACIJA TEORIJE HAOSA U OPTIMIZACIJI LMS ALGORITMA PRIMJENJENOG NA LINEARNIM ANTENSKIM NIZOVIMA IMPLEMENTATION OF CHAOTIC BASED OPTIMIZATION OF LMS ALGORITHM APPLIED ON LINEAR ANTENNA ARRAYS.....	35
Sanja Bauk, Radoje Džankić O IZAZOVIMA PRIMJENE RFID TEHNOLOGIJE U LANCIMA SNABDIJEVANJA UPON CHALLENGES OF RFID TECHNOLOGY IMPLEMENTATION IN SUPPLY CHAINS	39

Novica Daković, Milovan Radulović FLATNESS I LQR UPRAVLJANJE FURUTA KLATNOM FLATNESS AND LQR CONTROL OF FURUTA PENDULUM	43
Tomislav B. Šekara, Milovan Radulović NOVA METODA ZA OPTIMIZACIJU PID REGULATORA ZASNOVANA NA PRINCIPU NESIMETRIČNOG OPTIMUMA A NOVEL METHOD FOR OPTIMIZATION OF PID REGULATORS BASED NON-SYMMETRICAL OPTIMUM METHOD	47
Vasilija Šarac PRIMENA SIMULINKA U SIMULACIJI ELEKTRIČNIH MAŠINA APPLICATION OF SIMULINK IN SIMULATION OF ELECTRICAL MACHINES	52
Vasilija Šarac IMPLEMENTACIJA SCADA SISTEMA U HIDORELEKTRANI “KOZJAK” IMPLEMENTATION OF SCADA SYSTEM IN HPP “KOZJAK”	56
Aleksandar Ristić, Dalibor Damjanović KRITIČKA ANALIZA UPOTREBE MEDIJA U OBRAZOVANJU NA UNIVERZITETU OREGON SA OSVRTOM NA MOGUĆU PRIMJENU PRIMJERA DOBRE PRAKSE NA UNIVERZITETIMA U REPUBLICI SRPSKOJ CRITICAL ANALYSIS OF THE USE OF MEDIA IN EDUCATION AT THE UNIVERSITY OF OREGON, WITH A REVIEW OF POSSIBLE IMPLEMENTATION OF GOOD PRACTICE AT UNIVERSITIES IN REPUBLIC OF SRPSKA	60
Edin Salković DIGITALIZACIJA PEDOLOŠKIH PODATAKA CRNE GORE DIGITAZING THE PEDOLOGIC DATA OF MONTENEGRO	64
Aleksandar Dedić JEDAN METOD MJERENJA NAPONA I STRUJE BAZIRAN NA MIKROKONTROLERU A MICROCONTROLLER BASED VOLTAGE AND CURRENT MEASUREMENT METHOD	68
Duško Parezanović, Dragan Vidaković KAKO SE POTPISUJE PORUKA HOW TO SIGN THE MESSAGE	72
Radiša Stefanović, Aleksa Srdanov NESPECIFICIRANI USLOVI U IMPLEMENTACIJI ALGORITAMA PRI REŠAVANJU LOGIČKIH ZADATAKA UNSPECIFIED CONDITIONS IN THE IMPLEMENTATION OF ALGORITHMS IN SOLVING LOGICAL PROBLEMS	76
Matija Ratković, Slavica Tomović, Nikola Žarić, Milutin Radonjić, Igor Radusinović EMULACIJA SDN MREŽA SOFVERSКИM ALATOM MININET SDN NETWORK EMULATION WITH MININET SOFTWARE TOOL	80
Slavica Tomović, Milutin Radonjić, Milica Pejanović-Đurišić, Igor Radusinović SOFVERSКИ DEFINISANE BEŽIČNE SENZORSKE MREŽE SOFTWARE DEFINED WIRELESS SENSOR NETWORKS	84

Jelena Šuh, Branislav Sisojević INFORMACIONO-KOMUNIKACIONI ALATI ZA UPRAVLJANJE IP/MPLS MREŽOM INFORMATION-COMMUNICATION TOOLS FOR IP/MPLS NETWORK MANAGEMENT	88
Blažo Popović, Ranko Vojinović ANALIZA WIFI MREŽA U URBANOM DIJELU PRIJESTONICE ANALYSIS OF WIFI NETWORKS IN URBAN PART OF OLD ROYAL CAPITAL	92
Veselin N. Ivanović, Nevena Radović, Srdjan Jovanovski, Zdravko Uskoković UNAPRIJEDJENA PROCEDURA ZA ESTIMACIJU LOKALNE FREKVENCije VISOKO NESTACIONARNIH DVO-DIMENZIONALNIH FM SIGNALA AN IMPROVED PROCEDURE FOR THE LOCAL FREQUENCY ESTIMATION OF HIGHLY NONSTATIONARY TWO-DIMENSIONAL FM SIGNALS.....	96
Mirza Mulešković NIVO RAZVIJENOSTI IKT U CRNOJ GORI I E-SERVISA ZA PREDUZEĆA LEVEL OF DEVELOPMENT OF ICT IN MONTENEGRO AND E-SERVICES FOR COMPANIES ..	100
Milan Marić, Duško Pavićević, Maja Medenica ONLINE UPARIVANJE VISOKOG OBRAZOVANJA I TRŽIŠTA RADA U CRNOJ GORI ONLINE MATCHING HIGHER EDUCATION AND LABOUR MARKET IN MONTENEGRO.....	104
Aleksandar Milenković, Dragan Janković PRIMENA MEDICINSKIH INFORMACIONIH SISTEMA U REPUBLICI SRBIJI – TRENUTNO STANJE I MOGUĆA UNAPREĐENJA APPLICATION OF MEDICAL INFORMATION SYSTEMS IN THE REPUBLIC OF SERBIA – CURRENT STATUS AND POSSIBLE IMPROVEMENTS	108
Obradović Milovan PODRŠKA ICT PRAĆENJU I MERENJU ZADOVOLJSTVA KORISNIKA ZDRAVSTVENE ZAŠTITE ICT SUPPORT TO MONITORING AND HEALTHCARE USERS SATISFACTION MEASUREMENT	112
Jelena Končar, Sonja Leković PRIMENA B2C ELEKTRONSKOG PLAĆANJA U REPUBLICI SRBIJI IMPLEMENTATION OF B2C ELECTRONIC PAYMENT IN REPUBLIC OF SERBIA	116
Zoran Milivojević, Zoran Veličković, Bojan Princević INHARMONIČNOST KONTRA OKTAVE STEINWAY B KLAVIRA INHARMONICITY OF CONTRA OCTAVE OF THE PIANO STEINWAY B.....	120
Milesa Srećković, Magdalena Dragović, Aleksandar Čučaković, Biljana Đokić Milošević, Nada Ratković Kovačević DIZAJN, SIMULACIJA I MODELOVANJE U INŽENJERSTVU U OKVIRU IZABRANIH PROBLEMATIKA DESIGN, SIMULATION AND MODELING IN ENGINEERING WITHIN SELECTED PROBLEMS.....	124
Mirko Kosanović, Miloš Kosanović ENERGETSKI PROFIL POTROŠNJE ENERGIJE U SENZORSKOM ČVORU ENERGY PROFILE OF ENERGY CONSUMPTION IN SENSOR NODE	128

Nataša Savić, Zoran Milivojević, Vidoje Moračanin ANALIZA EFIKASNOSTI POLYA RACIONALNOG PARAMETARSKOG INTERPOLACIONOG JEZGARA KOD PROCENE FUNDAMENTALNE FREKVENCije ANALYSIS OF EFFICIENCY OF POLYA RATIONAL PARAMETRIC INTERPOLATION KERNEL IN THE ESTIMATION OF FUNDAMENTAL FREQUENCY	132
Zoran Veličković, Zoran Milivojević, Miloško Jevtović PRIMENA ITERATIVNOG ALGORITMA ZA POPRAVKU KVALITETA EKSTRAHOVANOG VODENOG ŽIGA IZ VIDEA STRIMOVANOG U BEŽIČNOM OKRUŽENJU APPLICATION OF ITERATIVE ALGORITHM FOR ENHANCEMENT OF EXTRACTED WATERMARK FROM THE VIDEO STREAMED IN A WIRELESS ENVIRONMENT	136
Martin Čalasan, Vladan Vujičić, Gojko Joksimović, Nikola Šoć, Chen Hao PREGLED MATEMATIČKIH MODELA MORSKIH STRUJA REVIEW OF MARINE CURRENT MATHEMATICAL MODELS	140
Risto Bojović, Ivana Milošević, Hristina Bojović ULOGA MODELA SPIRALNE DINAMIKE U RAZVOJU IT SISTEMA THE ROLE OF SPIRAL DYNAMICS MODEL IN IT SYSTEMS DEVELOPMENT	144
Maja Kukuševa Paneva, Biljana Čitkuševa Dimitrovska, Goce Stefanov PREGLED INTEGRISANE ŠEME PO ELIPTIČKOJ KIRIVULJI OVERVIEW OF ELLIPTIC CURVE INTEGRATED SCHEME.....	148
Ana Grbović, Bojan Đordan PCS7 VREMENSKA SINHRONIZACIJA U HE PERUĆICA PCS7 TIME SYNHRONIZATION IN HPP PERUĆICA	152
Tomče Velkov, Ace Panev, Roman Golubovski, Sašo Gelev, Vlatko Čingoski, Goce Stefanov, Maja Kukuseva Paneva SISTEM ZA KONTROLU AMBIJENTA U STAKLENIKU AMBIENT CONTROL SYSTEM IN GREENHOUSE.....	156
Slavica Kostadinova, Vlatko Čingoski, Roman Golubovski, Sašo Gelev POVEĆANJE ENERGETSKE EFIKASNOSTI VODOVODNIH SISTEMA POBOLJŠANJEM FAKTORA SNAGE PUMPNIH POSTROJENJA INCREASING ENERGY EFFICIENCY OF WATER SUPPLY SYSTEMS WITH PUMP SYSTEMS POWER FACTOR IMPROVEMENT.....	160
Goran Klepov, Vlatko Čingoski, Roman Golubovski, Sašo Gelev, Goce Stefanov NOVI METOD UPRAVLJANJA ASINHRONIH MOTORA SA INTERMITIRANIM REŽIMOM RADA U NAPAJANJU ARTISTIČKIH (MUZIČKIH) FONTANA A NEW CONTROL METHOD FOR INDUCTION MOTORS IN INTERMITTED WORKING REGIME FOR ARTISTIC (MUSIC-DRIVEN) FOUNTAINS	164
Goce Stefanov, Sašo Gelev, Vlatko Čingoski, Vasilija Šarac, Roman Golubovski ODREĐIVANJE IZLAZNIH KARAKTERISTIKA KVAZI-REZONANTNOG KONVERTORA POMOĆU KOMPJUTERSKIH SIMULACIJA DETERMINATION OF OUTPUT CHARACTERISTICS OF QUASI-RESONANT POWER CONVERTER WITH COMPUTER SIMULATION.....	168

Temelkovski Ordan, Sašo Gelev, Roman Golubovski, Vlatko Čingoski, Goce Stefanov PRIMENA FAZI LOGIKE U SISTEMU UPRAVLJANJA TOPLOTNIM PODSTANICAMA APPLICATION OF FUZZY LOGIC IN CONTROL SYSTEMS ARE HEAT SUBSTATIONS	172
Blažo Popović, Srđan Jovanovski PREGLED 6LOWPAN STANDARDA ZA POVEZIVANJE IOT OVERVIEW OF 6LOWPAN STANDARD FOR CONNECTING IOT	176
Mirko Jovović, Budimir Bukilić MOBILNI OPERATIVNI SISTEMI I BEZBJEDNOST. KAKO SE ZAŠTITITI? MOBILE OPERATING SYSTEMS AND SECURITY. HOW TO PROTECT YOURSELF?	180
Bogdan Krivokapić, Uglješa Urošević, Zoran Veljović, Milica Pejanović-Đurišić OPORTUNISTIČKI PRISTUP SPEKTRU U KOGNITIVNIM RADIO MREŽAMA OPPORTUNISTIC SPECTRUM ACCESS IN COGNITIVE RADIO NETWORKS	184
Branko Džakula DINAMIČKO TESTIRANJE I ANALIZA KLIJET-SERVER KOMUNIKACIJE U ANDROID APLIKACIJAMA DYNAMIC SECURITY TESTING AND ANALYSIS OF CLIENT-SERVER COMMUNICATION IN ANDROID APPLICATIONS	188
Stefan Vujović, Miloš Brajović, Slobodan Đukanović UPOTREBA WEB I MOBILNIH APLIKACIJA U AGRİKULTURI WEB AND MOBILE APPLICATIONS IN AGRICULTURE	192
Branko Džakula, Slobodan Đukanović REVERZNI INŽENJERING I METODE ZAŠTITE ANDROID APLIKACIJA REVERSE ENGINEERING AND ANDROID APPLICATION SECURITY	196
Bojan Domazetović, Enis Kočan POBOLJŠANJE ENERGETSKE EFIKASNOSTI BEŽIČNIH SENZORSKIH MREŽA KROZ KOOPERATIVNO PROSLJEĐIVANJE ENERGY EFFICIENCY IMPROVEMENT OF WIRELESS SENSOR NETWORKS THROUGH COOPERATIVE RELAYING	200
Stevan Šandi, Tomo Popović, Božo Krstajić IMPLEMENTACIJA IEEE C37.118 KOMUNIKACIONOG PROTOKOLA U PYTHON-U PYTHON IMPLEMENTATION OF IEEE C37.118 COMMUNICATION PROTOCOL	204
Miloš Brajović, Ljubiša Stanković, Miloš Daković REKONSTRUKCIJA NESTACIONARNIH SIGNALA SA NEDOSTAJUĆIM ODBIRCIMA PRIMJENOM S-METODA I GRADIJENTNOG ALGORITMA ZA REKONSTRUKCIJU RECONSTRUCTION OF NON-STATIONARY SIGNALS WITH MISSING SAMPLES USING S-METHOD AND A GRADIENT BASED RECONSTRUCTION ALGORITHM	208
Igor Ognjanović, Ramo Šendelj, Ivana Ognjanović PISMENOST U OBLASTI SAJBER BEZBJEDNOSTI U CRNOJ GORI CYBER SECURITY AWARENESS IN MONTENEGRO	212

Jelena Ljucović, Ivana Ognjanović, Ramo Šendelj ANALIZA OBRAZOVNOG SISTEMA U OBLASTI SAJBER BEZBJEDNOSTI U CRNOJ GORI ANALYSES OF CYBER SECURITY EDUCATIONAL SYSTEM IN MONTENEGRO	216
Tripo Matijević, Snežana Šćepanović, Marija Radojičić, Ivan Obradović, Saša Tatar RAZVOJ OKRUŽENJA ZA SPAJANJE AKADEMSKOG I PREDUZETNIČKOG ZNANJA PRIMJENOM OTVORENIH OBRAZOVNIH RESURSA CREATING ENVIROMENT FOR BLENDING ACADEMIC AND ENTREPRENEURIAL KNOWLEDGE USING OPEN EDUCATIONAL RESOURCES.....	220
Dejan Tomović, Ramo Šendelj, Ivana Ognjanović DOS I DDOS NAPADI I NJIHOVE KONTRAMJERE DOS AND DDOS ATTACKS AND THEIR COUNTERMEASURES	224
Aleksandar Rašović KORPORATIVNO UPRAVLJANJE INFORMATIKOM ICT GOVERNANCE.....	228
Biljana Stamatović, Armin Alibašić IZBOR I PRIKAZIVANJE PODATAKA IZ XML BAZA PODATAKA SELECTING AND REPORTING DATA FROM XML DATABASE	232

PREGLED INTEGRISANE ŠEME PO ELIPTIČKOJ KIRIVULJI OVERVIEW OF ELLIPTIC CURVE INTEGRATED SCHEME

Maja Kukuševa Paneva, Biljana Čitkuševa Dimitrovska, Goce Stefanov, Faculty of Electrical Engineering, UGD - Štip, R.Macedonia

Sadržaj: U ovom radu je data integrirana šema za enkripciju po eliptičkoj krivi (ECIES). ECIES je hibridna šema bazirana na eliptičkim krivama koja uključuju u sebe kriptiranje i dekriptiranje, izračunavanje haš funkcije i autentifikaciju. U ovom radu će biti prikazana analiza potrošene energije i upotrebljene RAM i ROM memorije.

Abstract: This paper gives overview of integrated encryption scheme over elliptic curve (ECIES). ECIES is hybrid scheme based on elliptic curve that includes encryption and decryption algorithm, hash computation and authentication. Analysis of simulation scenarios about energy and RAM and ROM memory consumption will be represented in this paper.

1. INTRODUCTION

Elliptic Curve Cryptography is public key cryptography proposed independently by N. Koblitz and V. Miller in 1985. Implementation of ECC include elliptic curve digital signature algorithm, Integrated Scheme and Diffie- Hellman. Elliptic Curve Integrated Scheme (ECIES) is hybrid scheme that uses public key system to transport the session key for usage in symmetric chipper. Also, ECIES provides semantic security against chosen plaintext and chosen chiphertext attacks.

ECIES [1, 2] is based on elliptic curve discrete logarithm problem [3]. The difficulty of ECDLP is based on finding integer $l \in [0, n-1]$ such that for given elliptic curve E , $P \in E(K)$ and $Q \in \langle P \rangle$ defined over finite fields F_p , $Q = lP$. The integer l must be large prime in order to avoid Pohling- Hellman [4] and Pollard's rho attacks [5, 6]. The method for solving ECDLP is fully exponential which results in decreasing key size needed to achieve same level of security when using conventional public key schemes. Comparing to 1034-bit RSA the same level of security is achieved using 160 bit key [7].

In this paper analysis about memory and energy consumption of ECIES will be represented. The analysis is done using software package TinyECC in TinyOS. In sector 2 the background of ECIES is represented. In sector 3 is given description of simulation scenario (grid and random topology), measured parameters (CPU Total, Radio Total and Total Energy), obtained results and their analysis. Sector 4 concludes this paper.

2. BACKGROUND

ECIES is standard encryption algorithm a variant of ElGamal encryption scheme proposed by Rogaway and Bellare [8]. This scheme is standardized in ANSI X9.63, ISO/IEC 15946-3 and IEEE P1363a. Based on shared secret obtained by Diffie- Hellman, ECIES derives two symmetrical keys. The first is used for encryption of the plaintext while

the second is used for authentication of the received encrypted message. The functional diagram of ECIES is represented in Figure 1 and includes key derivation function (KDF), encryption and decryption and message authentication. Key derivation function KDF is constructed from hash function H . For l - bits key KDF(S) is defined as concatenation of the hash values $H(S, i)$, where i is counter incremented for each hash function until l bits of hash values have been generated. ENC is symmetric key encryption scheme while DES is decryption function. MAC is message authentication code algorithm.

First step in using ECIES is selection of elliptic curve and domain parameters agreement between nodes Alice and Bob. Alice and Bob secretly choose random integer primes k_{rA} and k_{rB} so that $0 < k_{rA}$ and $k_{rB} < n$ (private keys). At the beginning Alice generates key pair which is consist of public key (point from the elliptic curve) obtained as multiplication of Alice's private key and the base point G . After that Alice uses key agreement function in order to obtain the shared secret. This is performed by multiplication of Alice's private key and Bob's public key:

$$Q_{uA} = k_{rA}G \quad (1)$$

Then the value obtained from Equation 1 is used as an input in key derivation function. The output of KDF is concatenation of symmetric encryption key k_{ENC} and MAC key k_{MAC} . Alice uses the encryption key k_{ENC} to encrypt the plaintext m and thus to obtain the encrypted message c . The value tag is generated from the encrypted message c and k_{MAC} . At the end Alice sends the values of Q_{uA} , tag and c to Bob. On the other side, Bob in order to decrypts the received message multiplies its private key k_{rB} with Alice's public key and obtains the shared secret. From the shared secret Bob derives the same k_{ENC} and k_{MAC} as Alice. Using the MAC key k_{MAC} and encrypted message Bob generates tag^*

value. If the values of tag and tag^* are not the same, Bob rejects the received message due to invalid verification.

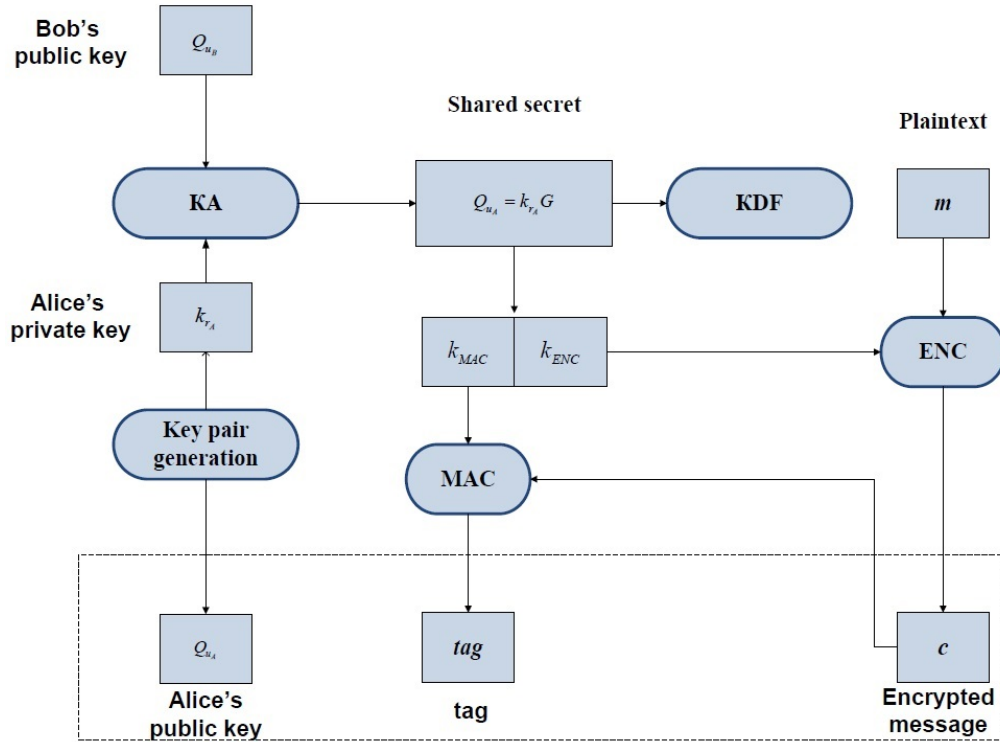


Figure 1. ECIES functional diagram

If the tag values are same, Bob decrypts the message using k_{ENC} and obtains the plaintext.

3. SIMULATION AND RESULTS

TinyOS [9] is an open source operating system for low power and limited resource applications that utilize wireless sensor networks. TinyOS has specially designed simulator TOSSIM [10] that allows debugging, testing and analyze of code written in nesC. TOSSIM has extension that provides per node estimation of power consumption and power management. The power analyze is done using the software package TinyECC1.0. TinyECC1.0 includes three elliptic curve cryptography schemes Elliptic Curve Integrated Scheme, Elliptic Curve Diffie- Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) which are not scope of this paper. The simulations are performed according NIST recommendation [11] for domain parameters $T = (p, a, b, G, n, h)$. Two curves have been analyzed secp128r1 and secp192k1 with affine coordinates. According to NIST recommendation the key size for the curve secp128r1 is 128-bits from which 64- bits are for security, while the key size for secp192k1 is 192-bits from which 96-bits are for security. Number of nodes are integer from square root from 4 up to 100 nodes. Two types of topology were deployed, random and grid as shown on Figure 2. In random topology nodes are randomly placed in working environment, unlike grid topology were nodes are placed in regular square were the distance between neighbor nodes is same. The duration of every simulation is 20 seconds.

The consumption of RAM and ROM memory after compiling IEC algorithm for both curves are represented in Table 1.

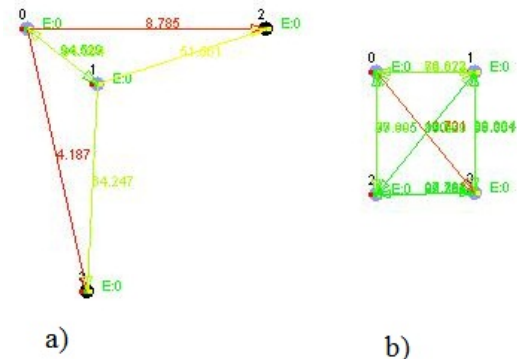


Figure 2. Simulation topology a) random b) grid

Table 1. ROM and RAM consumption

ECIES 128-bit key		ECIES 192-bits key	
1051	Bytes in ROM	1763	Bytes in ROM
28138	Bytes in RAM	28850	Bytes in RAM

The key parameters that were analyzed in term of energy consumptions are CPU Total, Radio Total and Total Energy. The parameter CPU total gives the mean energy (mJ) used for key pair derivation and generation and processing of messages. The parameter Radio Total gives the mean energy (mJ) used for transmission of the public key and communication with the other nodes in the network.

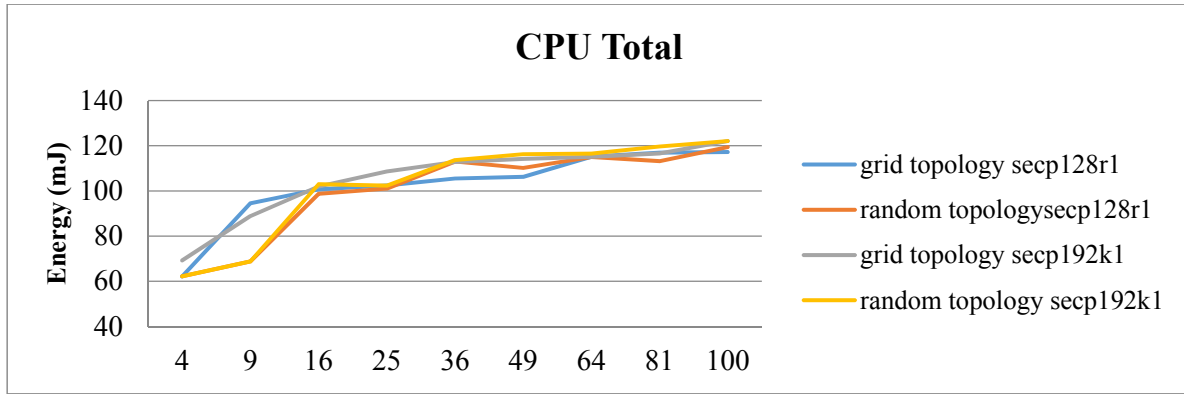


Figure 3. Parameter CPU Total

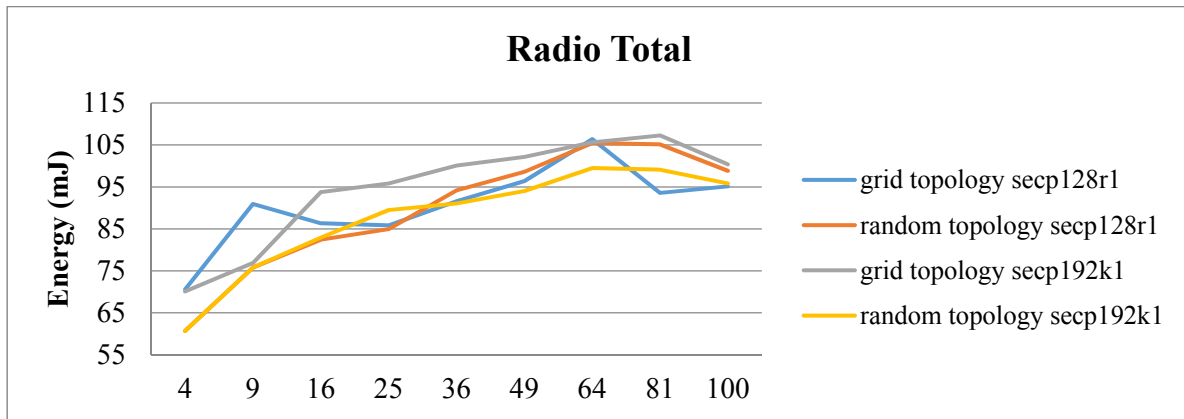


Figure 4. Parameter Radio total

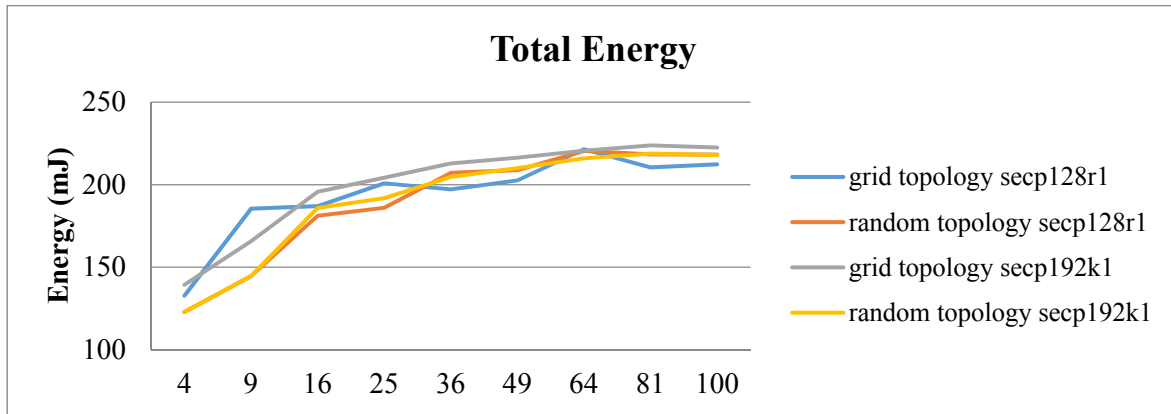


Figure 5. Parameter Total Energy

The parameter Total Energy gives the total mean energy (mJ) used and is sum of parameter CPU Total and Radio Total. The results from measurement of these parameters are shown in Figure 3, 4 and 5, appropriately.

4. CONCLUSION

ECIES is public key encryption scheme that includes public key derivation, encryption, decryption and authentication. In this paper was represented memory consumption and energy analysis in term of energy used for derivation of public key, communication with other nodes in the network,

message processing and encryption and decryption process. From the obtained results can be concluded that the RAM and ROM memory consumptions depends on the key size. For longer key size the consumption of RAM and ROM memory increases. Also by increasing the number of nodes the energy consumption increases due to more mathematical operation that have to be performed for every node. But, the energy consumption does not depend on used curve or network topology.

Future work will involve optimization of energy consumption by introduction of projective coordinates and optimization algorithms about mathematical operation (multiplication, reduction, inversion etc.).

REFERENCES

- [1] M. Abdalla, M. Bellare, P. Rogway, DHIES: An Encryption Scheme Based on the Diffie- Hellman Problem, *Contribution on IEEE P1363a*, 1998.
- [2] M. Abdalla, M. Bellare, P. Rogway, DHIES: An Encryption Scheme Based on the Diffie- Hellman Problem, *Contribution on IEEE P1363a*, 1998.
- [3] M. Abdalla, M. Bellare, P. Rogway, The oracle Diffie-Hellman assumptions and an analysis of DHIES, *Lecture Notes in Computer Science* 2020, 201 pp. 143-158.
- [4] C. Diem, On the discrete logarithm problem in elliptic curves II, *Algebra & Number Theory* 7, pp. 1281-1323, 2013.
- [5] S. Pohing, M. Hellman, An improved algorithm for computing logarithm over $GF(p)$ and its cryptographic significance", *IEEE Transactions on Information Theory*, pp.106-110, 1978.
- [6] P. van Oorshot, M. Wiener, Parallel collision search with cryptanalytic applications, *Journal of Cryptology*, 1-28, 1999.
- [7] J. Pollard, Monte Carlo methods for index computation mod p , *Mathematics of Computation*, pp. 918-924, 1978.
- [8] N. Gura, A. Patel, A. Wander, Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs, *In Proceedings of the 2004 Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004)*, pp 119-132, August 2004.
- [9] Bellare, Rogaway, Minimizing the use of random oracles in authenticated encryption schemes, *Information and Communication Security '97 (INCS 1334)*, 1-16, 1997.
- [10] Philip Levis, Sam Madden, Joseph Polastre, Robert Szewczyk, Kamin Whitehouse, Alec Woo, David Gay, Jason Hill, Matt Welsh, Eric Brewer, David Culler, TinyOS: An Operating System for Sensor Networks, *In Ambient Intelligence*, Springer- Verlag 2004.
- [11] Philip Levis, Nelson Lee, Matt Welsh, David Culler, TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Application, *Proceedings of SenSys' 03 First ACM Conference on Embedded Networked Sensor Systems*, 2003.
- [12] National Institute of Standards. Recommended Elliptic Curves for Federal Government Use, July 1999.

CIP - Каталогизација у публикацији
Национална библиотека Црне Горе, Цетиње

ISBN 978-86-85775-16-1
COBISS.CG-ID 27237136

ISBN 978-86-85775-16-1



9 788685 775161 >