ABSTRACT AND REFERENCES

INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2017.96296

DEVELOPMENT OF A MATHEMATICAL MODEL OF INFORMATION SERIAL REDUNDANCY OF MANAGEMENT INFORMATION SYSTEMS OF THE AIRCRAFT FIRE ALARM (p. 4-10)

Al-Ammouri Ali
National Transport University, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-0375-6108

Petr Dyachenko
Cherkasy State Technological University, Cherkasy, Ukraine
ORCID: http://orcid.org/0000-0001-8475-5854

Anastasiia Degtiarova
National Transport University, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0001-5883-6060

The issues of improving the effectiveness of information systems by means of serial information redundancy due to an increase in the reliability of control of dangerous flight situations on board aircrafts are considered. The use of microprocessor equipment taking into account the physical principles of connection of sensors to determine dangerous situations on board aircrafts is proposed. The method for serial switching of detectors (with memory), considering a priori information according to the Bayes' method is proposed. The mathematical and graphical dependencies of the a priori probability of fire detection on the sensor quality with the given values of a posteriori probability and the number of repeated requests $\alpha=f(P_1, \gamma, k)$ are obtained.

It is found that, in order to implement serial information redundancy, the following requirements shall be taken into account: high technical reliability of a particular information source; relatively large permissible information aging time; short correlation time of random technical faults, transient failures, fluctuation noise, etc.

If the a priori probability α of a controlled phenomenon is low, the probabilities p_1 and p_2 change slowly with increasing k, and the probability p_3 (false alarm) can be quite high, in comparison with the probability of non-detection p_2.

If the probability α is sufficiently high, the probability p_1 effectively increases with increasing k, and the probability of non-detection p_2 will be greater than the probability of false alarm p_3.

Keywords: alarm system efficiency, information reliability, serial redundancy, information source, fire.

References

1. Al-Ammori, A., Haritonova, L. (2014). Issledovanie vozmozhnostey povyisheniya effektivnosti primeneniya mikrokontrollera v informatsionno-upravlyayuschih sistemah. Iskusstvennyiy intellect, 1, 90–94.
2. Al-Ammouri, A., Kasyanenko, A. O., Al-Ammouri, H., Degtiarova, A. O. (2016). Optimization structures of onboard aircraft navigation systems. 2016 4th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC). doi: 10.1109/msnmc.2016.7783163
3. Zaripova, G. (2013). Increase of information transfer authenticity for non-stationary processes on the basis of neurofuzzy data processing system. Applied Technologies and Innovations, 9 (1), 1–11. doi: 10.15208/ati.2013.1
4. Li, H., Zhao, Q., Yang, Z. (2008). Reliability Monitoring of Fault Tolerant Control Systems with Demonstration on an Aircraft Model. Journal of Control Science and Engineering, 2008, 1–10. doi: 10.1155/2008/265189
5. Gribov, V. M., Hryshchenko, Yu. V., Kozhokhina, O. V. (2015). To the question of dependability calculation failures based on the exponential model of distribution of failures. Electronics and control systems, 1, 59–66.
6. Zieja, M., Ważny, M. (2014). A Model for Service Life Control of Selected Device Systems. Polish Maritime Research, 21 (2). doi: 10.2478/pomr-2014-0018
7. Gokdere, G., Gurcan, M. (2015). Erlang Strength Model for Exponential Effects. Open Physics, 13 (1), 395–399. doi: 10.1515/phys-2015-0057
8. Qiang, L. (2011). Estimation of Fire Detection Time. Procedia Engineering, 11, 233–241. doi: 10.1016/j.proeng.2011.04.652
9. Izadi, I., Shah, S. L., Shook, D. S., Chen, T. (2009). An Introduction to Alarm Analysis and Design. IFAC Proceedings Volumes, 42 (8), 645–650. doi: 10.3182/20090630-4-es-2003.00107
10. Bonfe, M., Castaldi, P., Mimmo, N., Simani, S. (2011). Active fault tolerant control of nonlinear systems: The cart-pole example. International Journal of Applied Mathematics and Computer Science, 21 (3), 441–455. doi: 10.2478/v10006-011-0033-y
11. Al-Ammouri, A., Melnichenko, O., Mironova, V., Tscvetkov, V. (2014). Effectiveness of the Information Redundancy System under Real Technical Reliability. Procedings of the Section of Young Researchers and Scientists (SYRAS) on the 10th International Conference on Digital Technologies. Zilina, 1–4.
12. Gnedenko, B., Pavlov, I., Ushakov, I. (1999). Statistical Reliability Engineering. New York: John Wiley & Sons, 503. doi: 10.1002/9780470172407

DOI: 10.15587/1729-4061.2017.95194

EXAMINATION AND IMPLEMENTATION OF THE FAST METHOD FOR COMPUTING THE ORDER OF ELLIPTIC CURVE (p. 11-21)

Ivan Gorbenko
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0003-4616-3449

Roman Hanzia
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0001-7945-3683

Present study provides detailed analysis of the theoretical and experimental complexity of methods for canonical lift of elliptic curves that are defined over the binary field. The SST, MSST and Harley methods were used in the research. Results of theoretical studies revealed that the fastest (by execution time) algorithm for computing the order of the curve is the Harley method. Present work gives the substantiation (approximately 10 seconds for 1024 bits) of this method and the possibility of its application for binary fields. By the data obtained, we constructed a program model of the examined methods for canonical lift of elliptic curves and computing the norm. The software model allowed us to conduct experimental analysis of the algorithms for canonical lift of elliptic curves. In present article we

experimentally confirmed a quasi quadratic dependence of the field size, over which curve is defined, and the time required for its canonical lift. Based on the results received, it is possible to argue that at present the fastest method for canonical lift is the Harley method. Our work demonstrated that the given method might be employed to modify the Ukrainian standard of electronic digital signature.

The relevance of research is related to the emergence of threats to the protection of information from the quantum cryptoanalysis for most modern asymmetric cryptosystems. However, modern cryptosystems should exist over the time that is necessary to find the candidates to replace them from the post-quantum cryptosystems. During such "transition period", classical cryptosystems should provide for the necessary level of stability, even under condition of constant extension of size in the system-wide parameters. The Ukrainian standard DSTU 4145–2002 has limitations on the size of system-wide parameters (up to 431 bits) and may not be able to account for a large reserve of stability. In addition, given the adoption of new standards for encryption and hash functions, in order to ensure the same level of security with the apparatus of elliptic curves, the latter must have parameters of size to 1024 bits.

Keywords: Satoh method, Harley method, order of elliptic curves, binary field, trace of Frobenius.

References

1. Horbenko, Yu. I., Hanzia, R. S. (2014). Analysis of the possibility of quantum computers and quantum computings for cryptanalysis of modern cryptosystems. Eastern-European Journal of Enterprise Technologies, 1 (9 (67)), 8–16. Available at: http://journals.uran.ua/eejet/article/view/19897/18759
2. Hanzia, R. S., Horbenko, Yu. I. (2014). Analiz shlyakhiv rozvytku kryptohrafiyi pislya poyavy kvantovykh kompyuteriv. Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika": Kompyuterni systemy ta merezhi, 806, 40–48.
3. Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 26 (5), 1484–1509. doi: 10.1137/s0097539795293172
4. Horbenko, I. D., Horbenko, Yu. I. (2012). Prykladna kryptolohiya. Kharkiv: Fort, 868.
5. Schoof, R. (1995). Counting points on an elliptic curve over finite fields. Proc. Journees Arithmetiques, 93, 219–252.
6. Skjernaa, B. (2003). Satoh's algorithm in characteristic 2. Mathematics of Computation, 72 (241), 477–488. doi: 10.1090/s0025-5718-02-01434-5
7. Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K., Vercauteren, F. (Eds.) (2005). Handbook of Elliptic and Hyperelliptic Curve Cryptography. NW.: Chapman & Hall/CRC, 807. doi: 10.1201/9781420034981
8. Vercauteren, F. (2003). Computing zeta functions of curves over finite fields. Katholieke Universiteit Leuven, 195.
9. Satoh, T. (2000). The Canonical Lift of an Ordinary Elliptic Curve over a Finite Field and its Point Counting. J. Ramanujan Math. Soc., 15 (4), 247–270.
10. Satoh, T., Skjernaa, B., Taguchi, Y. (2003). Fast computation of canonical lifts of elliptic curves and its application to point counting. Finite Fields and Their Applications, 9 (1), 89–101. doi: 10.1016/s1071-5797(02)00013-8
11. Harley, R. (2002). Asymptotically optimal p-adic point-counting. E-mail to NMBRTHRY list. Available at: https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0212&L=NMBRTHRY&F=&S=&P=7824
12. Gaudry, P. (2002). A Comparison and a Combination of SST and AGM Algorithms for Counting Points of Elliptic Curves in Characteristic 2. Lecture Notes in Computer Science, 311–327. doi: 10.1007/3-540-36178-2_20
13. Lercier, R., Lubicz, D. (2003). Counting Points on Elliptic Curves over Finite Fields of Small Characteristic in Quasi Quadratic Time. Lecture Notes In Computer Science, 360–373. doi: 10.1007/3-540-39200-9_22
14. Hanzia, R. S. (2016). Otsinka obchyslyuval'noyi skladnosti metodiv pidrakhunku kil'kosti tochok na eliptychniy kryviy. Systemy obrobky informatsiyi, 8, 92–99.
15. Satoh, T. (2001). Asymptotically fast algorithm for computing the Frobenius substitution and norms over unramied extension of p-adic number fields. Department of Mathematics, Faculty of Science, Saitame University, 1–21.

DOI: 10.15587/1729-4061.2017.96321

EXAMINING A POSSIBILITY TO USE AND THE BENEFITS OF POST-QUANTUM ALGORITHMS DEPENDENT ON THE CONDITIONS OF THEIR APPLICATION (p. 21-32)

Ivan Gorbenko
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0003-4616-3449

Volodymyr Ponomar
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0001-5271-2251

We established the need for comparative analysis and evaluation of the possibility to use asymmetric post-quantum cryptographic mechanisms. In order to compare, a procedure for evaluation was selected based on integral assessments of unconditional and conditional criteria. An analysis was conducted among the algorithms that fulfilled general unconditional criteria. As conditional criteria, we chose numerical characteristics of algorithms. In addition, additional unconditional criteria were put forward that differed depending on the conditions of use. The relevance of present research is associated with the emergence of a quantum computer. Previous studies have already proved that the existing cryptographic algorithms are vulnerable to the methods of quantum cryptanalysis. That is why, at present, leading organizations in the standardization of crypto algorithms conduct research and comparisons for selecting the post-quantum standard of cryptography.

As a result of present research, we found a lack of a universal post-quantum cryptographic algorithm. In addition, not all algorithms can be employed under different conditions. It is proposed to separate three variants in the application of post-quantum algorithms: for lightweight cryptography, for the use by standard automated systems and use in a cloud-based environment. For all conditions of use, a separate evaluation of benefits in the cryptographic algorithms was carried out. We detected shortcomings in the leading candidate in that it may possible have a reduced resistance for the specialized quantum attack. That is why the recommendations were given to employ these algorithms as the basic ones in the transition period. And, if the suspicion is confirmed, then we proposed alternatives for each variant of application. Results of present research allow us to understand current state in the development of post-quantum crypto algorithms and to predict their possible further development.

This forecast is important in that the post-quantum cryptographic mechanisms represent a new stage in the development and use of cryptography. In addition, the practical value of the research consists in obtaining the evaluation for post-quantum algorithms, depending on the conditions of their application.

Keywords: post-quantum cryptographic algorithms, comparative assessment of crypto algorithms, comparison criteria of crypto algorithms.

Refernces

1. Koblitz, N., Menezes, A. J. (2016). A riddle wrapped in an enigma. ePrint Archive, 1–21. Available at: http://eprint.iacr.org/2015/1018.pdf
2. Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 26 (5), 1484–1509. doi: 10.1137/s0097539795293172
3. Grover, L. K. A fast quantum mechanics algorithm for database search. CERN Document Server. Available at: http://cds.cern.ch/record/304210/files/9605043.pdf
4. Moody, D. (2016). Post-Quntum Cryptography: NIST's Plan for the Future. The Seventh International Conference on Post-Quntum Cryptography. Available at: https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf
5. Mosca, M., Lenhart, G., Pecen, M. (Eds.) (2013). Setting the Scene for the ETSI Quantum-safe Cryptography Workshop. E-proceedings of "1st Quantum-Safe-Crypto Workshop". Sophia Antipolis, 289. Available at: https://docbox.etsi.org/Workshop/2013/201309_CRYPTO/e-proceedings_Crypto_2013.pdf
6. Jao, D., Soukharev, V. (2014). Isogeny-Based Quantum-Resistant Undeniable Signatures. Lecture Notes in Computer Science, 160–179. doi: 10.1007/978-3-319-11659-4_10
7. Gorbenko, I. D., Kuznetsov, O. O., Potii, O. V., Gorbenko, Yu. I., Ganzya, R. S., Ponomar, V. A. (2016). Post quantum cryptography and mechanisms for its implementations. Radiotekhnika, 186, 32–52.
8. Gorbenko, Yu. I. (2015). Methods of construction and analysis, standardization and application of cryptographic systems. Kharkiv: Fort, 959.
9. Lenstra, H. W., Tijdeman, Jr., Tijdeman, R. (Eds.) (1982). Analysis and comparison of some integer factoring algorithms, in Computational Methods in Number Theory. Math. Centre Tract, 89–141.
10. Gorbenko, Yu., Yesina, M. (2016). Methods of cryptographic primitives comparative analysis. Inzynier XXI wieku. Bielsko-Biala: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Bialej, 451–462.
11. Nogin, V. D. (2004). A simplified version of the analytic hierarchy method based on non-linear convolution of criteria. Zhurn. vychislit. matem. i matematich. fiz., 44 (7), 1259–1268. Available at: http://www.apmath.spbu.ru/ru/staff/nogin/nogin_p11.pdf
12. Expert assessments for solutions developing. Available at: http://books.ifmo.ru/file/pdf/817.pdf
13. Wang, H., Ma, Z., Ma, C. (2013). An efficient quantum meet-in-the-middle attack against NTRU-2005. Chinese Science Bulletin, 58 (28-29), 3514–3518. doi: 10.1007/s11434-013-6020-y
14. Xiong, Z., Wang, Y., Zhang, T., Chen, L. (2012). An Improved MITM Attack Against NTRU. International Journal of Security and Its Applications, 6 (2), 269–274.

DOI: 10.15587/1729-4061.2017.96694

DEVELOPMENT OF A METHOD TO IMPROVE THE PERFORMANCE SPEED OF MAXIMAL FIRE DETECTORS (p. 32-37)

Vladimir Andronov
National University of Civil Protection of Ukraine, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0001-7486-482X

Boris Pospelov
National University of Civil Protection of Ukraine, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0002-0957-3839

Evgeniy Rybka
National University of Civil Protection of Ukraine, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0002-5396-5151

We conducted a theoretical analysis of the known method for improving performance speed of a maximal thermal fire detector under the action of temperature perturbation in the environment during fire in the interval of defining the temperature. It is demonstrated that the main shortcoming of this method is that the improvement in performance of a fire detector under complicated conditions is achieved by reducing the time constant of a detector. This leads to the growth in fluctuations of the output signal, reduces accuracy in determining the temperature and increases the number of false triggering in such detectors.

Theoretical substantiation of the proposed method to improve performance speed of MTFD is based on the dynamic correction of output signal from a thermal sensor in fire detector by the inertial-forced link with a transfer function whose inertial part's time constant is changed by time in the interval of temperature measurement. We proposed a rule for changing the time constant.

A comparative analysis of the known and the proposed methods revealed that the new method provides for an increase in performance speed of a fire detector without increasing the fluctuations in the output signal. Increasing the speed of action relative to the mathematical expectation and dispersion of fluctuations in the output signal is achieved at different moments of time, which are much less than the time of actuation of the maximal thermal detector – 20 s. The method proposed allows us to increase performance speed of a fire detector relative to the mathematical expectation of the output signal larger than by 5 times, and relative to the dispersion of fluctuations in the output signal – by 1.5 times.

The method we devised is recommended to improve the performance speed of maximal thermal fire detectors under complicated conditions for operation, specific to industrial enterprises of metallurgy and petrochemical sector, for the purpose of their efficient fire protection.

Keywords: maximal thermal fire detector, performance speed, environment, complicated temperature conditions.

References

1. Poulsen, A., Jomaas, G. (2011). Experimental Study on the Burning Behavior of Pool Fires in Rooms with Different Wall Linings. Fire Technology, 48 (2), 419–439. doi: 10.1007/s10694-011-0230-0
2. Oppelt, U. (2006). Improvement on fire detectors by using multiple sensors. Fire & Safety. Available at: http://www.securitysa.com/regular.aspx?pklregularid=2502

3. Pospelov, B. B., Chumachenko, S. N., Uriadnikova, I. V. (2015). Uchet priemlemogo riska pri obosnovanii trebovanij k sistemam kontrolja sostojanija opasnyh ob'ektov. Aktual'ni problemy modeljuvannja ryzykiv i zagroz vynyknennja nadzvychajnyh sytuacij na ob'jektah krytychnoi' infrastruktury. Kyiv: TOV «Instytut matematychnogo modeljuvannja «Fraksim», 139–145.
4. Ding, Q., Peng, Z., Liu, T., Tong, Q. (2014). Multi-Sensor Building Fire Alarm System with Information Fusion Technology Based on D-S Evidence Theory. Algorithms, 7 (4), 523–537. doi: 10.3390/a7040523
5. Cheng, C., Sun, F., Zhou, X. (2011). One fire detection method using neural networks. Tsinghua Science and Technology, 16 (1), 31–35. doi: 10.1016/s1007-0214(11)70005-0
6. Pospelov, B. B., Andronov, V. A. (2015). Improving Efficiency Monitoring Systems for Potentially Dangerous Objects Based on Optimization of Group Detection Sensors. Civil Engineering and Architecture, 3 (4), 69–72. doi: 10.13189/cea.2015.030401
7. Pospelov, B. B., Shevchenko, R. I., Kolenov, A. N. (2014). Sintez optimal'nogo izmeritelja opasnyh faktorov pozhara s proizvol'noj dinamikoj dlja pozharnyh izveshhatelej. Problemy pozharnoj bezopasnosti, 35, 172–178.
8. Siebel, R. (2006). Test of fire detection algorithms using artificially generated events. Fire Safety Journal, 41 (4), 258–265. doi: 10.1016/j.firesaf.2006.01.004
9. Gurevich, V. (2008). Microprocessor protection devices: The present and the future. Serbian Journal of Electrical Engineering, 5 (2), 325–339. doi: 10.2298/sjee0802325g
10. Radonja, P., Stankovic, S. (2009). Generalized Profile Function Model Based on Neural Networks. Serbian Journal of Electrical Engineering, 6 (2), 285–298. doi: 10.2298/sjee0902285r
11. Tsai, Y. C. (2007). The Design and Implementation of Early Fire Detection and Hierarchical Evacuation Alarm System, Master Thesis. Graduate Institute of Networking and Communication Engineering. Taiwan.
12. Ristic, J., Radosavljevic, D. (2011). Decision algorithms in fire detection systems. Serbian Journal of Electrical Engineering, 8 (2), 155–161. doi: 10.2298/sjee1102155r
13. Willstrand, O., Brandt, J., Svensson, R. (2016). Detection of fires in the toilet compartment and driver sleeping compartment of buses and coaches – Installation considerations based on full scale tests. Case Studies in Fire Safety, 5, 1–10. doi: 10.1016/j.csfs.2015.11.002
14. Zheng, W., Zhang, X., Wang, Z. (2016). Experiment Study of Performances of Fire Detection and Fire Extinguishing Systems in a Subway Train. Procedia Engineering, 135, 393–402. doi: 10.1016/j.proeng.2016.01.147
15. Abramov, Iu. A., Sadkovyi, V. P. (2006). Pat. No. 81975 UA. Maksymalno-dyferentsiinyi teplovyi pozhezhnyi spovishchuvach. MPK G08B17/06. No. 200603837; declareted: 7.04.2006; published: 17.07.2006, Bul. No. 4.

DOI: 10.15587/1729-4061.2017.96040

DEVELOPMENT OF THE MODEL FOR A BACKHAUL NETWORK BASED ON THE LONG TERM EVOLUTION TECHNOLOGY (p. 38-44)

Liubov Tokar
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0002-7780-1928

Ekaterina Belousova
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0003-1550-5100

Alexey Kolyadenko
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0001-6374-1664

Ivan Lukinov
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0001-5346-2143

The infrastructure of packet transfer offers great possibilities for organizing the universal transport networks using the LTE technology, which is linked to a wide variety of standards with many applications, as well as applying different protocols of interaction, management and service by contemporary networks.

In order to organize a broadband access, it is proposed to employ the rational approach to the mobile transport infrastructure, which is based on the model of network in line with the Unified MPLS Mobile Transport concept, at all levels of which a protocol is configured of multi-protocol commutation by the markers for a simultaneous support of several generations of mobile communication in the unified network flat-oriented architecture.

We analyzed the throughput and reliability of a backhaul network. The topology is selected for the optimal construction of a backhaul network using a star-shaped configuration, which will make it possible to create a dynamic fully connected network based on IP.

The throughput and transport efficiency of network are determined. It is established that the channel band, the modulation method and the type of morphology exert essential effect on obtaining the best results with a guarantee of data packet transfer without loss of frames. The indicators obtained contribute to an increase in the network capacity and throughput with higher speeds and less delays in the packet transfer.

Keywords: backhaul network, wireless technology, controller, topology, packet architecture, throughput.

References

1. Ksenzenko, P. Ya., Himich, P. V. (2012). Razvitie setey Backhaul. Telekom, 11, 28–38.
2. Dzhineven, Sh. (2007). «Mnogolikie» fiksirovannyie besprovodnyie sistemyi. Seti i sistemyi svyazi, 14, 58–63.
3. Kogan, S. S. (2008). Paketnyie opticheskie transportnyie seti: innovatsionnyie resheniya kompanii Alcatel – Lucent. Elektrosvyaz, 12, 70–74.
4. Ksenzenko, P. Ya., Naryitnik, T. N., Himich, P. V. (2014). Backhaul dlya geterogennyih setey. Telekom, 1-2, 10–21.
5. Katlerov, P. N. (2007). Ethernet over PDH: migratsiya k paketnoy transportnoy infrastrukture besprovodnyih setey. Komponentyi i tehnologii, 10, 116–120.
6. Christophe, D. (2011). Backhaul Transformation. RadioResourse international, 25 (2), 36–41.
7. Kaduskar, R. G., Kavishwar, A. D. (2011). Mobile Backhaul Network. International Conference on Information and Network Technology (IPCSIT), 4, 211–216.
8. Saranya, B., Muruganandham, S. (2015). Mobile Backhaul Network in wireless Sensor. International Journal of Engineering Research and General Science, 3 (1), 394–397.
9. Masud, M. M. (2015). Survey of security features in LTE Handover Technology. Scientific Research Journal (SCIRJ), 3 (8), 27–31.
10. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update. Available at: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

11. Howard, M. (2013). Using Carrier Ethernet to Backhaul LTE. Infonetics Research, 18.
12. 3GPP TS 45.005 V8.8.0 (2010-03). 3rd Generation Partnership Project; Technical Specification Group GSM/EDGE Radio Access Network; Radio transmission and reception (Release 8). Available at: http://www.qtc.jp/3GPP/Specs/GSM_GERAN/45005-880.pdf
13. Kodentsev, D. (2016). Razvitie platform Cisco dlya MPLS dostupa i preagregatsii. Cisco.
14. UMMT 3.0 Design Guide Technical Paper (2012). Americas Headquarters Cisco Systems, Inc., 104. Available at: https://communities.cisco.com/docs/DOC-30621
15. Litovka, V. (2012). What is Carrier class. Business Development Manager, 4, 43–55.
16. Rosen, E., Rekhter, Y. (1999). RFC 2547. BGP/MPLS VPNs. RFC Editor, 25. doi: 10.17487/rfc2547
17. Muthukrishnan, K., Malis, A. (2000). RFC 2917. A Core MPLS IP VPN Architecture. RFC Editor, 16. doi: 10.17487/rfc2917
18. Chen, C. C. The Notion of overbooking and Its Application to IP/MPLS Traffic Engineering. Internet Traffic Engineering Working Group. Available at: http://www.ietf.org/proceedings/52/I-D/draft-cchen-te-overbooking-01.txt
19. Gasymov, I. (2012). Arhitektura Cisco Unified MPLS: Vnedrenie MPLS na vsekh urovnyah seti. Cisco.

DOI: 10.15587/1729-4061.2017.96653

ANALYSIS OF INTERFERENCE IMMUNITY OF THE SEARCHLESS METHOD OF CORRELATION-INTERFEROMETRIC DIRECTION FINDING WITH RECOSTRUCTION OF THE SPATIAL ANALYTICAL SIGNAL (p. 45-52)

Vitaliy Tsyporenko
Zhytomyr State Technological University, Zhytomyt, Ukraine
ORCID: http://orcid.org/0000-0001-8559-006X

An analysis of noise immunity of the searchless digital method of correlation-interferometric direction finding with reconstruction of the spatial analytical signal has been carried out. An analytical estimate of the direction finding error variance consisting of the noise and interference components was obtained. It was shown that the main controllable factors affecting the noise component of the direction finding error variance are as follows: the number of direction-finding channels, the amount of separation between the selected elements of the antenna array, the type of the weight function in spatial spectral analysis and the time of emission analysis. The interference component of the direction finding error variance, unlike the noise component, does not depend on the analysis time but is determined, first of all, by the quality of frequency-spatial selection.

In simulation, a family of dependencies of the root mean square deviation of the bearing estimate on the signal-to-noise ratio and the type of the weight function of the spectral analysis window was obtained. Possibility of direction finding with a value of the root mean square deviation of the bearing estimate of 0.03 degrees at an input signal-to-noise ratio of 0 dB has been shown. The estimates of the direction finding error variance obtained analytically and by software simulation practically coincided which confirms the analysis correctness. As a result of simulation, a family of dependences of root-mean square deviation of the bearing estimation on the separation of direction to the signal and interference sources at different signal frequencies was also obtained.

It was determined that when the 64-element linear array is used, the resolution of the direction finder depends on the signal frequency. It varies between 6–15 degrees in the range of the direction finder operating frequencies at a signal/interference ratio of 0 dB. The resolution of the direction finder which was found to be high compared to the annular antenna array is an important advantage in conditions of a complex electromagnetic situation.

Keywords: analysis of noise immunity, searchless digital method, correlation-interferometric direction finding, spatial analytical signal.

References

1. Kratschmer, G. (2011). Introduction into Theory of Direction Finding. Radiomonitoring and Radiolocation 2010/2011. Rohde & Schwarz GmbH & Co., 49.
2. Rembovskiy, A. M., Ashyhmin, A. V., Kuzmin, V. A.; Rembovskiy, A. M. (Ed.) (2010). Radiomonitiring – tasks, methods, devices. Moscow: Hotline – Telecom, 624.
3. Rangarao, K. V., Venkatanarasimhan, S. (2013). Gold-MUSIC: A Variation on MUSIC to Accurately Determine Peaks of the Spectrum. IEEE Transactions on Antennas and Propagation, 61 (4), 2263–2268. doi: 10.1109/tap.2012.2232893
4. Fu, X., Sidiropoulos, N. D., Ma, W.-K., Tranter, J. (2014). Blind spectra separation and direction finding for cognitive radio using temporal correlation-domain ESPRIT. 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). doi: 10.1109/icassp.2014.6855108
5. Sorochan, A. G. (2013). Correlation direction finder with two OMNI-directional antennas. Microwave and Telecommunication Technology (CriMiCo), 2013: 23rd International Crimean Conference, 298–299.
6. Tsyporenko, V. V., Tsyporenko, V. G. (2016). Research of Direct Digital Correlative-Interferometric Radio Direction Finder with Double Correlation-convolutional Processing. Visn. NTUU KPI. Ser. Radioteh. radioaparatobuduv, 65, 51–61.
7. Lee, J.-H., Woo, J.-M. (2015). Interferometer direction-finding system with improved DF accuracy using two different array configurations. IEEE Antennas and Wireless Propagation Letters, 14, 719–722. doi: 10.1109/lawp.2014.2377291
8. Yang, J., Chen, W., Li, L., Ni, X. (2014). Long baseline direction finding and localization algorithms for noise radiation source. 2014 12th International Conference on Signal Processing (ICSP). doi: 10.1109/icosp.2014.7014968
9. Voskresenskiy, D. I., Ovchinnikova, E. V., Kondratieva, S. G., Shmachilin, P. A. (2012). Digital beam forming by means of matrix Fourier transform method. Proceedings of the 22nd International Crimean Conference on Microwave and Telecommunication Technology (CriMiCo), 455–456.
10. Tsyporenko, V. V. (2012). Direct Digital Method of the Correlation-interferometric Radio Direction-finding with Reconstructing of Spatial Analytical Signal. Visnyk of NTUU „KPI". Ser. Radioengeneering. Radiodevices construction, 48, 75–84.
11. Karavaev, V. V., Sazonov, V. V. (1987). Statistical theory of passive location. Moscow: Radio and Communications, 240.
12. Lawrence, M. J. (1987). Digital Spectral Analysis: With Applications. New Jersey: Prentice-Hall, Inc. Upper Saddle River, 492.
13. Proakis, J. G., Manolakis, D. G. (2006). Digital Signal Processing. New Jersey: Prentice-Hall, Inc. Upper Saddle River, 1004.

DOI: 10.15587/1729-4061.2017.96662

DEVELOPMENT OF THE INTELLIGENT DECISION-MAKING SUPPORT SYSTEM TO MANAGE CYBER PROTECTION AT THE OBJECT OF INFORMATIZATION (p. 53-61)

Valeriy Lakhno
European University, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0001-9695-4543

Yuliia Boiko
National Aviation University, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0003-2344-3632

Andrii Mishchenko
National Aviation University, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-7514-6245

Valeriy Kozlovskii
National Aviation University, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-8301-5501

Oleksandr Pupchenko
European University, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-0899-8843

We proposed an architecture for a protection control system of the object of informatization (OBI) with the subsystem of intelligent support for making decisions on the operational management of cyberprotection. The proposed architecture, in particular, can be used under conditions of the incompleteness of knowledge about the state of OBI protection. We developed a model for the operational management of cyberprotection at OBI and formed a rational complex of protection means. The model is based on the morphological approach. The model allows, taking into account morphological matrices for each of the five proposed perimeters prepared by the intelligent decision-making support system (IDMSS), generation of variants of sets that consider the compatibility of software and hardware tools of information protection. It is proposed to make the choice on the optimal variant of a set for the perimeter using an objective function that maximizes the ratio of the summary indicator "protection of information" to the summary indicator "expenditures". The software is realized and tested under real conditions of IDMSS in the contours for the organizational-technical and operational management of the OBI protection. An improved architecture of IPCS is different from the existing solutions in the possibility of simultaneous optimization of sets of software and hardware tools for the examined perimeters of OBI, for both centralized and decentralized variants for processing the information. In this case, an analysis of the level of protection of OBI is performed in real time. It is proven that the use of the developed IDMSS makes it posible to significantly reduce the planned spending on an information protection system, as well as reduce the time it takes to inform decision-makers about information security incidents.

Keywords: information security, management of information protection, morphological approach, decision support system.

References

1. Panaousis, E., Fielder, A., Malacaria, P., Hankin, C., Smeraldi, F. (2014). Cybersecurity Games and Investments: A Decision Support Approach. Decision and Game Theory for Security, 266–286. doi: 10.1007/978-3-319-12601-2_15
2. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F. (2016). Decision support approaches for cyber security investment. Decision Support Systems, 86, 13–23. doi: 10.1016/j.dss.2016.02.012
3. Chang, L.-Y., Lee, Z.-J. (2013). Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system. 2013 International Conference on Fuzzy Theory and Its Applications (iFUZZY). doi: 10.1109/ifuzzy.2013.6825462
4. Atymtayeva, L., Kozhakhmet, K., Bortsova, G. (2014). Building a Knowledge Base for Expert System in Information Security. Advances in Intelligent Systems and Computing, 57–76. doi: 10.1007/978-3-319-05515-2_7
5. Grossklags, J., Christin, N., Chuang, J. (2008). Secure or insure? Proceeding of the 17th International Conference on World Wide Web – WWW '08. doi: 10.1145/1367497.1367526
6. Kanatov, M., Atymtayeva, L., Yagaliyeva, B. (2014). Expert systems for information security management and audit. Implementation phase issues. 2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS). doi: 10.1109/scis-isis.2014.7044702
7. Korzhyk, D., Yin, Z., Kiekintveld, C., Conitzer, V., Tamb, M. (2011). Stackelberg vs. Nash in Security Games: An Extended Investigation of Interchangeability, Equivalence, and Uniqueness. Journal of Artificial Intelligence Research, 41, 297–327.
8. Rees, L. P., Deane, J. K., Rakes, T. R., Baker, W. H. (2011). Decision support for Cybersecurity risk planning. Decision Support Systems, 51 (3), 493–505. doi: 10.1016/j.dss.2011.02.013
9. Akhmetov, B., Lakhno, V., Boiko, Y., Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity. Eastern-European Journal of Enterprise Technologies, 1 (2 (85)), 4–15. doi: 10.15587/1729-4061.2017.90506
10. Goztepe, K. (2012). Designing Fuzzy Rule Based Expert System for Cyber Security. International Journal of Information Security Science, 1 (1), 13–19.
11. Oglaza, A., Laborde, R., Zarate, P. (2013). Authorization Policies: Using Decision Support System for Context-Aware Protection of User's Private Data. 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. doi: 10.1109/trustcom.2013.202
12. Lakhno, V., Kazmirchuk, S., Kovalenko, Y., Myrutenko, L., Zhmurko, T. (2016). Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features. Eastern-European Journal of Enterprise Technologies, 3 (9 (81)), 30–38. doi: 10.15587/1729-4061.2016.71769
13. Gamal, M. M., Hasan, B., Hegazy, A. F. (2011). A Security Analysis Framework Powered by an Expert System. International Journal of Computer Science and Security (IJCSS), 4 (6), 505–527.
14. Ben-Asher, N., Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behavior, 48, 51–61. doi: 10.1016/j.chb.2015.01.039
15. Ou Yang, Y.-P., Shieh, H.-M., Tzeng, G.-H. (2013). A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. Information Sciences, 232, 482–500. doi: 10.1016/j.ins.2011.09.012
16. Linda, O., Manic, M., Vollmer, T., Wright, J. (2011). Fuzzy logic based anomaly detection for embedded network security cyber sensor. 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS). doi: 10.1109/cicybs.2011.5949392
17. Mashkina, I. V., Guzairov, M. B., Vasilyev, V. I., Tuliganova, L. R., Konovalov, A. S. (2016). Issues of information security control in virtualization segment of company information system. 2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM). doi: 10.1109/scm.2016.7519715

18. Gutzwiller, R. S., Hunt, S. M., Lange, D. S. (2016). A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts. 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA). doi: 10.1109/cogsima.2016.7497780
19. Lakhno, V. (2016). Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering. Eastern-European Journal of Enterprise Technologies, 2 (9 (80)), 18–25. doi: 10.15587/1729-4061.2016.66015
20. Burger, E. W., Goodman, M. D., Kampanakis, P., Zhu, K. A. (2014). Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies. Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security – WISCS '14. doi: 10.1145/2663876.2663883
21. Al-Jarrah, O., Arafat, A. (2014). Network Intrusion Detection System using attack behavior classification. 2014 5th International Conference on Information and Communication Systems (ICICS). doi: 10.1109/iacs.2014.6841978
22. Lahno, V. (2014). Protection of information in critical application data processing systems. MEST Journal, 2 (2), 102–112. doi: 10.12709/mest.02.02.02.11
23. Shin, J., Son, H., Khalil ur, R., Heo, G. (2015). Development of a cyber security risk model using Bayesian networks. Reliability Engineering & System Safety, 134, 208–217. doi: 10.1016/j.ress.2014.10.006
24. Tosh, D., Sengupta, S., Kamhoua, C., Kwiat, K., Martin, A. (2015). An evolutionary game-theoretic framework for cyber-threat information sharing. 2015 IEEE International Conference on Communications (ICC). doi: 10.1109/icc.2015.7249499
25. Hwang, J., Syamsuddin, I. (2009). Information Security Policy Decision Making: An Analytic Hierarchy Process Approach. 2009 Third Asia International Conference on Modelling & Simulation. doi: 10.1109/ams.2009.49