ABSTRACT AND REFERENCES

INFORMATION AND CONTROLLING SYSTEM

MODELING OF SELECTIVE GALOIS COUNTER MODE WITH RAPID GENERATION OF GALOIS MESSAGE AUTHENTICATION CODE (p. 4-12)

Olexander Kuznetsov,
Ievgeniia Kolovanova, Dmytro Ivanenko, Olena Vynokurova

This article discusses the selective Galois counter mode with rapid generation of Galois message authentication code (Galois/Counter Mode and GMAC - GCM & GMAC). Specification of this coding mode is presented in NIST SP 800-38D. This coding mode is designed for realization of rapid cryptotransformation in providing information security services using different cryptographic primitives, such as polynomial hashing, counter and other. Using of proposed coding mode ensures the integrity and confidentiality of information. The article developed a reduced model of the mode. Reduced model preserves the algebraic structure of all main cryptotransformations by their scaling. Developed reduced model will use for experimental studies of collision properties of generated message authentication codes using the methods of statistical testing of hypotheses and mathematical statistics. This article discusses practical examples of cryptoprimitives and cryptotransformations.

Keywords: mini-model, message authentication code, hashing, coding, key, information security, message, block symmetric cipher.

References

1. GOST 28147-89. Information processing systems. Cryptographic protection. Cryptographic transformation algorithm. (1989). M., 28.
2. GOST R ISO/IEC 10116-93. Information technology. Modes of operation for an n-bit block cipher algorithm. (1994). M., 20.
3. ISO/IEC 10116. Information technology – Security techniques – Modes of operation for an n-bit block cipher. (2006). Available: http://www.iso.org
4. Dworkin, M. (2007). NIST Special Publication 800-38. Block Cipher Modes. Gaithersburg. Available at: http://csrc.nist.gov.
5. Information Technology. Cryptographic protection. Symmetric block algorithm transformation. (2014). Draft DSTU. Ed. 2. K., 238.
6. Gorbenko, I. D.; JSC «IIT». (2014). Development of a new symmetric block cipher: Report on the first phase of research «Algorithm» (intermediate), Tom 4, 304.
7. Kuznetsov, O. O., Ivanenko, D. V., Kolovanova, Ie. P. (2014). Analysis of collision properties of Galois Message Authentication Code with selective Counter. Bulletin of V. Karazin Kharkiv National University. Series «Mathematical Modelling. Information Technology. Automated Control Systems», № 1097, Issue 23, 55-71
8. National Institute of Standards and Technology. (2001). FIPS 197: Advanced Encryption Standard. Available: http://www.nist.gov/aes
9. Stinson, D. R. (1994, July). Universal hashing and authentication codes. Designs, Codes and Cryptography, Vol. 4, № 3, 369–380. doi:10.1007/bf01388651
10. Carter, J. L., Wegman, M. N.; International Business Machines Corporation, Armonk, N.Y. (1986). Polynomial hashing: 4,588,985 United States Patent: H 03 M 7/00, field of search 340/347 DD.
11. Phan, R. C.-W. (2002, October). Mini Advanced Encryption Standard (Mini-AES): A testbed for Cryptanalysis Students. Cryptologia, Vol. 26, № 4, 283–306. doi:10.1080/0161-110291890948
12. Bellare, M., Canetti, R., Krawczyk, H. (1996). Keying Hash Functions for Message Authentication. CRYPTO '96 Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology, Vol. 1109, 1–15. doi:10.1007/3-540-68697-5_1
13. Igoe, K., Solinas, J. (2009). AES Galois counter mode for the secure shell transport layer protocol. IETF Request for Comments 5647. Available: http://tools.ietf.org/html/rfc5647.
14. Law, L., Solinas, J. (2007). Suite B cryptographic suites for IPsec. IETF Request for Comments 4869. Available: http://tools.ietf.org/html/rfc6379
15. Salter, M., Rescorla, E., Housley, R. (2009). Suite B profile for transport layer security (TLS). IETF Request for Comments 5430. Available: http://tools.ietf.org/html/rfc5430
16. Lemsitzer, S., Wolkerstorfer, J., Felber, N., Braendli, M. (2007). Multi-gigabit GCM-AES Architecture Optimized for FPGAs. Cryptographic Hardware and Embedded Systems - CHES 2007, Vol. 4727, 227-238. doi:10.1007/978-3-540-74735-2_16.
17. McGrew, D. A., Viega, J. (2013). The Galois/Counter Mode of Operation (GCM), 41.
18. Käsper, E., Schwabe, P. (2009). Faster and Timing-Attack Resistant AES-GCM. Cryptographic Hardware and Embedded Systems CHES 2009, Lecture Notes in Computer Science, Vol. 5747, 1-17. doi:10.1007/978-3-642-04138-9_1.
19. Misdetection of MIPS endianness & How to get fast AES calls? (2010). Available at: http://groups.google.com/group/cryptopp-users/msg/a688203c2314ef08
20. Gueron, S. (2013, Jan. 9-11). AES-GCM for Efficient Authenticated Encryption – Ending the Reign of HMAC-SHA-1? Workshop on Real-World Cryptography. Stanford University, 32.
21. Gopal, V., Feghali, W., Guilford, J., Ozturk, E., Wolrich, G., Dixon, M., Locktyukhin, M., Perminov, M.; Intel Corp. (2010). Fast Cryptographic Computation on Intel Architecture Via Function Stitching. Available: http://download.intel.com/design/intarch/PAPERS/323686.pdf
22. Manley, R., Gregg, D. (2010). A Program Generator for Intel AES-NI Instructions. Progress in Cryptology INDOCRYPT 2010, Lecture Notes in Computer Science, Vol. 6498, 311-327. doi:10.1007/978-3-642-17401-8_22
23. McGrew, D. A., Viega, J. (2004). The Security and Performance of the Galois/Counter Mode (GCM) of Operation. Proceedings of INDOCRYPT 2004, Lecture Notes in Computer Science, Vol. 3348, 343-355. doi:10.1007/978-3-540-30556-9_27
24. Ferguson, N. (2005). Authentication Weaknesses in GCM. Microsoft Corp. Available at: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/CWC-GCM/Ferguson2.pdf
25. Saarinen, M.-J. O. (2012). Cycling Attacks on GCM, GHASH and Other Polynomial MACs and Hashes. Fast Software Encryption. Lecture Notes in Computer Science, Vol. 7549, 216-225. doi:10.1007/978-3-642-34047-5_13

OPTIMIZATION OF ANTENNAS ELEVATION ANGLES FOR ATMOSPHERIC BOUNDARY LAYER ACOUSTIC SOUNDING SYSTEM (p. 13-19)

Yaroslav Sydorov, Gennadii Sidorov

Using acoustic locators is effective to solve the problems of studying wind conditions in the atmospheric boundary layer. These locators are based on the monostatic and bistatic principle. In the first case, the wind velocity vector is determined by the results of sounding in three directions, in the second – three-channel system with three different receiving antennas, radiation patterns of which intersect vertically-oriented radiation pattern of the transmitter antenna at a given point in space is used. In each direction of signal reception by the measured value of the Doppler frequency shift, the value of the wind velocity projection at the geometric axis of the receiving antenna is determined and then using the appropriate matrix transformations, wind velocity projections in the Cartesian coordinate system are calculated. The most important characteristic of any measurement system is the total standard measurement error, the value of which depends on the system configuration and total error components, defined by technical characteristics of the system. The analysis of the dependence of the measurement error of the most important for the practice horizontal component of the wind velocity depending on the antenna elevation angle was carried out, the nonlinear dependence of this quantity was shown. Its values are minimized in the certain range of angles that are optimal for the system construction.

Keywords: acoustic sounding, atmospheric boundary layer, antenna elevation angles, standard error.

References

1. Davey, R. F. (1978). A comparison of doppler sodar antenna configurations used for horizontal wind measurement. J. Acust. Soc. Am., 63 (5), 68–78. doi:10.1121/1.381887
2. Gryning, S. E., Batchvarova, E., Floors, R., Pena, A. (2012). Some challenges of wind modelling for modern wind turbines: the Weibull distribution. 16th Int. Symp. for the Advancement of Boundary-Layer Remote Sensing, 194–197.
3. Lothon, M., Lenschow, D. H., Angevine, W. et al. (28–30 June 2010). Studying the Boundary Layer Late Afternoon and Sunset Turbulence (BLLAST). 15th Int. Symp. for the Advancement of Boundary-Layer Remote Sensing. Paris, France.
4. Strehz, A., Bradley, S., Underwood, K. (2012). Field results from a new miniature bistatic sodar. 16th Int. Symp. for the Advancement of Boundary-Layer Remote Sensing, 120–123.
5. Al-Sakka, H., Weill, A., Legac, C., Chardenal, L. (28–30 June 2010). Analysis and studies of the Atmospheric Boundary Layer properties (wind and turbulence) with the CURIE radar. 15th Int. Symp. for the Advancement of Boundary-Layer Remote Sensing. Paris, France.
6. Krasnenko, N. P., Shamanaeva, L. G. (2012). Retrieval of the temperature and velocity structure parameters from sodar data with allowance for the excess turbulent attenuation. 16th Int. Symp. for the Advancement of Boundary-Layer Remote Sensing, 194–197.
7. Steeneveld, G. J., Tolk, L., Moene, A. F. et al. (28–30 June 2010). Daytime boundary-layer growth in models and observations: in search of missing energy. 15th Int. Symp. for the Advancement of Boundary-Layer Remote Sensing. Paris, France.
8. Corn, G., Corn, T. (1973). Handbook of Mathematics. Moskow, USSR: Science, 764.
9. Zejdel, A. N. (1974). Physical quantities measurement errors. Leningrad, USSR: Science, 108.
10. Astapenko, P. D., Baranov, A. M., Shvarev, I. M. (1979). Aerop nautical meteorology: Tutorial. Moscow, USSR: Transport, 263.
11. Tuzov, G. I. (1976). Information extracting and processing in the Doppler systems. Moskow, USSR: Soviet radio, 256.
12. Little, C. G. (1969). Acoustic methods for the remote probing of the lower atmosphere. Pros. IEEE, 57 (4), 571–578. doi:10.1109/proc.1969.7010
13. Kalistratova, M. A. (1962). Experimental studies of the sound waves scattering in the atmosphere. Trans. IFA USSR, №4, 203–256.
14. Smith, P. L. (1961). Remote measurement of wind velocity by the electromagnetic acoustic probe I: System analysis. Proc. Natnl. Conv. Mil. Electron 5th, 48–53.
15. Bronshtein, I. N., Semedajev K. A. (1956). Handbook of Mathematics. Moskow, USSR: SPITL, 608.

FORECASTING CHANGES OF FRAME ALIGNMENT LOSS PROBABILITY IN CONVERGENT NETWORKS (p. 19-24)

Yuriy Babich, Lesia Nikityuk

The paper provides a developed method that allows to predict a change in the frame alignment loss probability when using the unstructured circuit emulation services in mobile backhaul networks based on the bit-error monitoring. This method allows to determine the moments of exceeding the threshold value by frame alignment loss probability for any technically possible number of TDM cycles, encapsulated in an Ethernet frame.

The fragments of dependences of the frame alignment loss probability on the bit error value with different values of the number of TDM cycles, encapsulated in an Ethernet frame, produced using the developed model were shown. It was shown that large threshold values of frame alignment loss probability correspond to the large values of the number of TDM cycles, encapsulated in an Ethernet frame. With the increase in the number of TDM cycles, encapsulated in an Ethernet frame, the probability that frame alignment loss probability exceeds its threshold value grows, which is undesirable. The developed method allows to decide on the possibility to increase the communication channel utilization by increasing the number of TDM cycles, encapsulated in an Ethernet frame, based on data of forecasting changes in the frame alignment loss probability.

Keywords: circuit emulation service, forecasting frame alignment loss probability, mobile backhaul.

References

1. ITU-T Recommendation G.8001 Terms and definitions for Ethernet frames over Transport. (2008). Approved 2008-03-29. Geneva: ITU, 12.
2. ITU-T Recommendation G.706 Frame Alignment and Cyclic Redundancy Check (CRC) Procedures Relating to Basic Frame Structures Defined in Recommendation G.704. (1991). Approved 1991-04-05. Geneva: ITU, 18.
3. Biriukov, N., Triska, N. (21.09.2005). Seti sinhronizatsii: stsenarii vzaimodeystvia. Seti i telecomunicatsii. Available: http://www.seti.ua.com/?in=seti_show_article&seti_art_ID=148&_by_id=2&_CATEGORY=14/
4. Bregni, S. (2002). Synchronization of digital telecommunications networks. West Sussex: John Wiley & Sons, Ltd, 395. doi:10.1002/0470845880
5. MEF 3 Circuit Emulation Service Definitions, Framework and Requirements in Metro Ethernet Networks. (13.04.2004). The Metro Ethernet Forum. Available at: http://www.metroethernetforum.org/Assets/Technical_Specifications/PDF/MEF3.pdf
6. MEF 8 Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks. (October 2004). The Metro Ethernet Forum. Available at: http://www.metroethernetforum.org/Assets/Technical_Specifications/PDF/MEF8.pdf
7. Babich, Yu. O., Nikityuk, L. A. (2013). Analysis and optimiA zation of parameters of circuit emulation service in mobile networks. Eastern-European Journal Of Enterprise Technologies, 4(9(64)), 59-62. Available at: http://journals.uran.ua/eejet/article/view/16396
8. Babich, Y. O. (2012). Estimation of frame alignment forced losses in mobile backhaulnetwork under the circuit emulation conditions. Scientific works of ONAT n.a. Popov, №2, 117-119.
9. ITU-T Recommendation G.826 Error performance parameters and objectives for international, constant bit rate digital paths at or above the primary rate. (2002). Approved 2002-12-14. Geneva: ITU, 34.
10. Chetirkin, E. M. (1977). Statisticheskie metodi prognozirovania. M.: Statistika, 200.
11. Nikityuk, L. A., Babich, Y. O. (2014). Influence of Frame Aligner's Probabilistic and Time Characteristics on CESon ETH Channel Usage Efficiency. Proceedings of the Intere national Conference TCSET'2014 Dedicated to the 170th anniversary of Lviv Polytechnic National University (Lviv-Slavske, Ukraine). Lviv: Publishing House of Lviv Polytechnic, 465–466.
12. Sukachev, E. A. (2013). Sotovie seti radiosviazi s podvizhi nimy obektami: handbook. Odessa: ONAS n.a. A. S. Popov, 256.
13. Technical specifications Nokia FlexiHopper. (06.07.2014). TelecomConsulting. Available at: http:// http://telekom.org.ru/katalog-naimenovanii-res/nokia-flexihopper-7/

ANALYSIS OF MODELS AND OPTIMIZATION OF INFORMATION COLLECTION IN WIRELESS SENSOR NETWORKS (p. 24-30)

Pavel Galkin

The paper analyzes various models of information collection from currently existing wireless sensor networks.

The analysis has shown that depending on the collection model chosen, its application is limited. The model of data collection on schedule is optimal for tasks of permanent tracking of parameters of the investigated environment. Using the model of data collection on request allows partially obtain the benefits of the model of collection on schedule and arrange access to the nodes as to the database. The model of data collection on events is the most effective for monitoring the environment in terms of state changes and identifying significant events. Adaptive information collection models implement the idea of self-organizing wireless sensor networks.

At the same time, there is no collection model that can be used with some restrictions for various wireless sensor networks. The only model that partially satisfies this condition, in some approximation, is a hybrid model.

The hybrid information collection model allows to combine several models for solving specific operation problem of the wireless sensor network. The disadvantages of hybrid models are very complex network construction algorithms.

Different approaches, which allow to optimize such information collection are proposed. Positioning nodes and introducing network aggregators provides enhanced adequacy and objectivity of the data obtained at low energy costs.

The optimization problem of existing information flows in different information collection models in WSN remains relevant and practically significant.

Keywords: model of information collection, wireless sensor networks, routing, optimization, wave transmission.

References

1. Mobile Ad-hoc Networks (2014). Internet Engineering Task Force Available at: http://datatracker.ietf.org/wg/manet/charter
2. Center for Embedded Networked Sensing (2014) The University of California Available at: http://www.cens.ucla.edu/about
3. James, E. W. (2010) Large-Scale Multiple-Source Detection Using Wireless Sensor Networks. Dissertation, 168.
4. Kucheryaviy, A. E. (2013). Internet of Things. Electrosvyaz, 12, 21–24.
5. Kucheryaviy, A. E., Salim A. (2013) Selecting the cluster head node in a homogeneous wireless sensor network. Electrosvyaz, 8, 32–36.
6. Kucheryaviy, A. E., Ermoshkina, D. D. (2011) Classification of wireless sensor networks by type of load. Telecommunications and transport, 5 (7), 64–65
7. Andreyev, Y. V., Dmitriev, A. S., Efremova, E. V., Lazarev, V. A. (2014). Ultra Wideband Transceivers Based on Chaotic Pulses and their Application to Wireless Body Area Networks. IEICE Proceeding Series, 2, 221–224. doi:10.15248/proc.2.221
8. Wireless system for collecting information (2014). Inform-Chaos Lab. Available at: http://www.cplire.ru/win/informchaoslab/products/products.htm
9. Proceedings of the XIII Conference on Radiophysics 85th anniversary of MA Miller (2009). Nizhny Novgorod, 1–275.
10. Molchanov, D. A., Kucheryaviy, A. E. (2006). Application of wireless sensor networks. Electrosvyaz, 6, 20–23.
11. IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks –Specific Requirements – Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (2009). IEEE Std. 802.15.4-2009, 1–39 Available at: http://standards.ieee.org/getieee802/download/802.15.4d-2009.pdf
12. Terentev, M. N. (2010). The method of operation of systems for monitoring the parameters of objects with configurable based on discrete wireless sensor networks. Dissertation, 154.
13. Ivanova, I. A (2010). Defining the perimeter coverage of wireless sensor networks. Industrial process control, and controllers, 10, 25–30.
14. Measuring Power Consumption of CC2530 With Z-Stack (2012). Texas Instruments Application Ноте AN079, 1–18.
15. Second Generation System-on-Chip Solution for 2.4 GHz IEEE 802.15.4 / RF4CE / ZigBee (2014). Texas Instruments, 1–34 Available at: http://www.ti.com/lit/ds/symlink/cc2530.pdf
16. Vlasova, V. A., Zelenin, A. N. (2012). Analysis of the energy cycle nodes of wireless sensor networks. Eastern-European Journal of Enterprise Technologies, 3 (9), 13–17.
17. Arkov, V. Y., Friedland A. M., Zhevak A. V. (2007) Optimizing the data acquisition in wireless sensor networks using the neural network learning algorithm gradient. Neurocomputers – development, application, 10, 47–49.
18. Zhevak, A. V. (2008) Simulation and optimization of data collection in wireless sensor networks based on a fixed schedule. Dissertation, 111.
19. Timkov, A. V., Telyatnikov, A. O. (2010). Development of a simulation model of the wireless sensor network. Information control systems and computer monitoring, The materials of the first all-Ukrainian scientific-technical conference of students, postgraduates and young scientists DonNTU, Donetsk 117–121. Available at: http://ea.donntu.edu.ua/handle/123456789/12697
20. Voskov, L. S., Komarov, M. M. (2012). Method of energy balancing stationary wireless sensor networks with Autonomous power sources. Business Informatics, 1, 70–75
21. Voskov, L. S., Komarov, M. M. (2012). Positioning sensors wireless sensor networks as a way of saving power sources. Sensors and systems, 1, 34–38.
22. Chen, Y., Nasser, N. (2006). Energy-balancing multipath routing protocol for wireless sensor networks. Proceedings of the 3rd International Conference on Quality of Service in Heterogeneous Wired/wireless Networks - QShine '06. doi:10.1145/1185373.1185401
23. Soro, S., Heinzelman, W. B. (2005). Prolonging the lifetime of wireless sensor networks via unequal clustering. Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05), 236–243. doi: 10.1109/IPDPS.2005.365
24. Abolhasan, M., Wysocki, T., Lipman, J. (2005). Investigation on three-classes of MANET routing protocols. Asia-Pacific Conference on Communications, 774–778. doi: 10.1109/APCC.2005.1554167
25. Vahabi, M., Rasid, M. F. A., Abdullah, R. S. A. R., Ghazvini, M. H. F. (2008). Adaptive Data Collection Algorithm for Wireless Sensor Networks. International Journal of Computer Science and Network Security, 8 (6), 125–132.
26. Jayant Gupchup, Andreas Terzis, Randal C. Burns, Alexander S. Szalay (2009). Computing Research Repository, abs/0901.3., 1–6
27. Chao, W., Huadong, M., Yuan, H., Shuguang, X. (2010). International Conference on Parallel and Distributed Systems – ICPADS, 164–171. doi: 10.1109/ICPADS.2010.32
28. Feng, W., Jiangchuan, L. (2011). Networked Wireless Sensor Data Collection: Issues, Challenges, and Approaches. Communications Surveys & Tutorials, IEEE, 13 (4), 673–687. doi: 10.1109/SURV.2011.060710.00066
29. An, M. K., Cho, H. (2014). Data Aggregation with multiple sinks in Information-Centric Wireless Sensor Network. Computer, Information and Telecommunication Systems (CITS), 2014 International Conference, 1–5 doi: 10.1109/CITS.2014.6878957
30. Yonghui, S., Younghan, K. (2014). Data Aggregation with multiple sinks in Information-Centric Wireless Sensor Network. Information Networking (ICOIN), 2014 International Conference on, 13–17. doi: 10.1109/ICOIN.2014.6799475
31. Wei, W., Hock, B. L., Kian-Lee, T. (2010). Query-Driven Data Collection and Data Forwarding in Intermittently Connected Mobile Sensor Networks. VLDB 2010 – 36th International Conference on Very Large Data Bases.– Singapore, 13–17. Available at: http://www.vldb2010.org/proceedings/files/

vldb_2010_workshop/DMSN_2010/individual-files/05.wu-04.pdf doi: 10.1145/1858158.1858166

32. Galkin, P. V., Borisenko, A. S. (2013). Adequacy of model wireless sensor networks in imitation simulation tools. Eastern-European Journal of Enterprise Technologies, 4/9(64), 52–55.

COMPUTER SIMULATION OF POLYNOMIAL ALGORITHMS OF RADIO SIGNALS DISTINCTION AND ESTIMATING THEIR PARAMETERS (p. 31-39)

Volodymyr Palahin, Artem Honcharov, Volodymyr Umanets

The use of bifunctional rule of processing input sample values was proposed in the paper. The first function is a hypothesis distinction function, which is based on using polynomial decision rules (DR) of signals distinction, the optimal coefficients of which are in accordance with moment quality criterion of upper limits of error probabilities. The second is a signals parameters estimation function, which is based on methods of polynomial maximization and truncated stochastic polynomial maximization.

Using a generator of pseudorandom sequences, based on bigaussian model, computer simulation of common algorithms of signals distinction and evaluating their parameters was performed. Experimentally obtained computer simulation results in general correspond to theoretical.

It was found that the efficiency of polynomial distinction and evaluation algorithms increases with the stochastic polynomial degree and as the values of coefficients of asymmetry and kurtosis approach the tolerance range limit, i.e. the probability of type I and type II errors and dispersion of the obtained estimates decreases. The results can be used to reduce the error probability of radio signals distinction and improve the estimation accuracy of their parameters in radiolocation, radio navigation and other areas, where the accuracy of signal processing algorithms plays an important role.

Keywords: truncated stochastic polynomials, moment quality criterion, signals distinction, non-Gaussian noise.

References

1. Trifonov, A. P., Shinakov, Y .S. (1986). Joint discrimination of signals and estimation of their parameters at background noise, Moscow, USSR: Radio and Communications, 264.
2. Van Trees, H. L., Bell, K. L., Tiany, Z. (2013). Detection Estimation and Modulation Theory, John Wiley & Sons, 1176.
3. Litvin-Popovich, A. I. (2013). Signal Detection and measurement of parameters in tracking radio systems, Technology Audit and production reserves, 6/1(14), 30–34.
4. Sobolev, V. S. (2014). Maximum-likelihood estimates of the frequency of signals of laser Doppler anemometers, Journal of Communications Technology and Electronics, 59(4), 294–301. doi: 10.1134/S1064226914030103
5. Krupiński, R. (2013). Modified Moment Method Estimator for the Shape Parameter of Generalized Gaussian Distribution for a Small Sample Size, Computer Information Systems and Industrial Management, 8104, 420–429. doi: 10.1007/978-3-642-40925-7_39
6. Kunchenko, Yu. P. (2002). Polynomial Parameter Estimations of Close to Gaussian Random Variables, Aachen: Shaker Verlag, 396.
7. Malakhov, A. N. (1979). Cumulant analysis of non-Gaussian processes and their transformations, Moscow, USSR: Radio and Communications, 376.
8. Palahin, V. V. (2012). Nonlinear algorithms of radio signals detection at additive-multiplicative non-Gaussian interference, Eastern-European Journal of Enterprise Technologies, 6/11(60), .23–28.
9. Palahin, V. V., Zhila, O. M. (2009). Recognition of radio signals at asymmetric non-Gaussian interference by moment criterion quality, Electrical machinery and electrical equipment, (73), 125–130.
10. Honcharov, A. V., Umanets, V. M. (2013). Estimation of radio signal amplitude at additive skewness-kurtosis interference using kunchenko's truncated polynomials, Visnyk CHDTU, (2), 111–118.
11. Kunchenko, Yu.P., Zabolotniy, S. V., Gavrish, O. S., Ivanchenko, A. Y. (2002). Generation of pseudorandom sequences based on bigauss distribution, Computer technology of printing, 343–351.

12 Palahin, V. V., Honcharov, A. V., Umanets, V. M. (2013). Computer modeling of joint algorithms of distinction of radio signals and estimation of their parameters at non-gaussian interferences, PREDT-2013, 109–110.

DEVELOPMENT OF MATHEMATICAL AND SOFTWARE MODELS OF THE PERSPECTIVE ENCRYPTION ALGORITHM FOR IMPLEMENTATION VERIFICATION (p. 39-45)

Yuri Gorbenko, Ruslan Mordvinov, Olexander Kuznetsov

The structure, basic transformations and application modes of the perspective encryption algorithm of symmetric block transformation “Kalina” are considered. Mathematical and software models of the cryptographic algorithm for the implementation verification are examined. In particular, verification method of software implementation of BSC “Kalina” in the respective operating modes is justified, reference software implementation of the basic cipher transformations and test cases for the implementation verification are designed. To eliminate sources of common errors in various cipher components, multi-version development is used, the essence of which is to create two or more software components to implement the same function by the methods that eliminate errors in various cryptographic transformation elements. The results allow to perform verification of the software, software-hardware and hardware implementation of BSC “Kalina” and all relevant application modes, both at the design stage and in the case of a self-test while the system operation.

Keywords: symmetric block cipher, cryptographic transformation, software implementation correctness, test cases.

References

1. Decree of the President of Ukraine “On Regulations on cryptographic protection in Ukraine” from 22.05.98 № 505/98. L. D. Kuchma.
2. Decree of the President of Ukraine “On the Doctrine of Information Security of Ukraine” from 08.07.2009 № 514. V. A. Yushchenko.
3. Law of Ukraine “On National Security of Ukraine” from 19.06.2003 № 964-IV. Verkhovna Rada of Ukraine.
4. Law of Ukraine “On Information” from 02.10.1992 № 2657-XII. Verkhovna Rada of Ukraine.
5. Law of Ukraine “On protection of information in telecommunication systems” from 05.07.1994 № 80/94 VR. Verkhovna Rada of Ukraine.
6. The Law of Ukraine “On the National System confidential communication” from 10.01.2002 № 2919-III. Verkhovna Rada of Ukraine.
7. Regulations on the procedure for the development, manufacture and operation of cryptographic protection of information from 30.07.2007 p. № 862/14129. State Service for Special Communication and Information Protection of Ukraine.
8. Statement on the State examination in the field of cryptographic protection, approved by order of the State Service Administration 23.06.2008 № 100 registered with the Ministry of Justice of Ukraine July 16, 2008 under № 651/15342. State Service for Special Communication and information Protection of Ukraine.
9. ISO. Information Technology. Cryptographic protection. The algorithm is a symmetric block transformation (2014). Exposure draft second (final) version.
10. Development of a new symmetric block cipher: a report on the first phase of research “Algorithm” (2014). (intermediate) / JSC “IIT”; supervisor. ID Gorbenko.
11. Gorbenko, I., Gorbenko, Y. (2012). Applied Cryptology. Monograph. Kharkiv KNURE Fort, 868.

12. Esin, V., Kuznetsov, A., Soroka, L. (2013). Security of information systems and technologies. H .: KNU. VN Karazina, 632.
13. Schneier, B. (2002). Applied kryptohrafyya. Protokolы, algorithms, yshodnыe tekstы language to SI. Moscow: "Triumf", 797.
14. Menezes, A. J., van Oorschot, P. C., A. V. Scott (1997). Handbook of Applied Cryptography - CRC Press, 794. . doi: http://dx.doi.org/10.5860/choice.34-4512
15. Daemen, J., Rijmen, V. (2003). Annex to AES Proposal Rijndael. Available at: http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf
16. Biham, E., Shamir, A. (1993). Differential Cryptanalysis of the Data Encryption Standard. SpringeriVerlag, New York, 77. doi: http://dx.doi.org/10.1007/978-1-4613-9314-6_4
17. Matsui, M. (1993). Linear Cryptanalysis Method for DES Cipher, EUROCRYPT'93, 112–123. doi: http://dx.doi.org/10.1007/3-540-48285-7_33
18. Knudsen, L. R. (2001). Integral Cryptanalysis, NESSIE internal report. Available at: https://www.cosic.esat.kuleuven.be/nessie/reports/phase2/uibwp5-015-1.pdf.
19. NESSIE security report (2003). Available at: https://www.cosic.esat.kuleuven.be/nessie/deliverables/D20-v2.pdf
20. AES discussion forum. Available at: http: // aes. nist. gov
21. Dolgov, V., Lisitskaya, I. (2013). Symmetric block ciphers. Methodology for assessing resistance to differential attacks and lineynogokriptoanaliza. Monograph. Kharkov, KNURE, Fort, 455.
22. Gorbenko, I., Dolgov, V., Olejnikov, R., Ruzhentsev, V., Mikhaylenko, M., Gorbenko, Y. (2007). Development of requirements and design principle perspective symmetrical block encryption algorithm. News SFU. Engineering science, 1 (76), 238–241.
23. Gorbenko, I., Dolgov, V., Olejnikov, R., Ruzhentsev, V., Mikhaylenko, M., Gorbenko, Y., Neyvanov, A. (2007). Principles of construction and properties of block symmetric cipher "Kalina". Applied electronics, 2.
24. Gorbenko, I., Dolgov, V., Olejnikov, R., Ruzhentsev, V., Mikhaylenko, M., Gorbenko, Y., Chichmar, S. (2007). Cryptographic cipher "Kalina". Applied electronics, 2.
25. Dolgov, V., Kuznetsov, A., Isaev, S. (2011). Differential properties of block symmetric ciphers submitted to the Ukrainian competition. Electronic simulation, 33 (6), 81–99.
26. Kuznetsov, A., Lisitskaja, I., Isaev, S. (2011). Linear properties of block symmetric ciphers submitted to the Ukrainian competition. Applied electronics, 10 (2), 135–140.
27. Lisitskaja, I., Nastenko, A. (2011). Large ciphers are random substitutions. Interdepartmental Scientific. technical collection ″Radiotehnika″, 166, 50–55.

USE OF NON-LINEAR DINAMICS METHODS FOR RESEARCHING NETWORK TRAFFIC BEHAVIOUR OF HIGH-SPEED NETWORKS (p. 46-50)

Aleksandr Karpukhin, Dmytro Gritsiv, Aleksander Tkachenko

An approach that allows to assess the behavior of network traffic of high-speed communication networks, which has self-similarity properties using the nonlinear dynamics methods is proposed in the paper. The number of Internet users is growing every year, which leads to an increase in the load on the communication channels. The works of many researchers have shown that network traffic possesses self-similarity property, caused by the TCP protocol behavior. With the advent of high-speed data transmission technology, this property of the network traffic has become particularly evident. Communication networks of information systems with TCP protocol are considered in the paper as nonlinear systems that exhibit chaotic properties under certain computer network parameters. Studies have shown that in the model network there are unwanted chaotic phenomena, which negatively affect its performance.

The results can be used to modify existing networks and design new ones. The proposed technique allows to predict the network traffic behavior under certain values of the computer network parameters at longer time axis intervals through its analysis at relatively small segments.

Keywords: self-similarity, network traffic, chaotic phenomena, dynamic system, TCP protocol.

References

1. Sheluchin, O. I., Smolskiy, S. M., Osin, A. V. (2007). Self-Similar Processes in Telecommunications. New York: John Wiley & Sons, 320.
2. Willinger, W. Taqqu, M. S., Sherman, R., Wilson, D. V. (2007). Self-similarity through high-variability: Statistical analysis of Ethernet LAN traffic at the source level. IEEE/ACM Trans. Netw., 5 (1), 71–86. doi: 10.1109/90.554723
3. Leland, W. E., Taqqu, M. S., Willinger, W., Wilson, D. V. (1994). On the self-similar nature of ethernet traffic. IEEE/ACM Transactions of Networking, 2 (1), 1–15. doi: 10.1145/166237.166255
4. Park, K., Willinger, W. (2000). Self-similar network traffic: An overview. In: Self-similar network traffic and performance evaluation. Eds. New York: Wiley, 1, 19. doi: 10.1002/047120644x.ch1
5. Guillemin, F., Boyer, J., Dupuis, A. (1992). Burstiness in broadband integrated networks, 15 (3), 163–176. doi: 10.1016/0166-5316(92)90032-C
6. Hanaya, Y. S., Dwaraki, A., Huc, K., Wolf, T. (2013). High-performance implementation of in-network traffic pacing for small-buffer networks. Computer Communications, 36 (13), 1450–1459. doi: 10.1016/j.comcom.2013.07.002
7. Larsson, C. (2014). Chapter 8 – Flow-Controlled Packet Networks. Design of Modern Communication Networks. Methods and Applications, 237–271. doi: 10.1016/B978-0-12-407238-1.00008-7
8. Karpukhin, A. V. (2009). Osobennosti realizicaii protokola TCP v sovremennih komputernih setyah. Sistemi obrabotki informacii-KH.:KHUPS, 6 (80), 49–53.
9. Feng, W., Tinnakornsrisuphap, P. (2000). The failure of TCP in High-Performance Computational Grids. In Proceedings of International Conference on Parallel Processing (ICPP'00), 37.
10. Feng, W., Tinnakornsrisuphap, P. (2000). The Adverse Impact of the TCP Congestion-Control Mechanism in Distributed Systems. In Proceedings ICPP'00 of International Conference on Parallel Processing, 299–306. doi: 10.1109/icpp.2000.876145
11. Wireshark application and concomitant documentation. Available at: https://www.wireshark.org
12. Petrov, V. V. (2003). Statesticheskiy analiz setevofo trafika. MEI, IRE, 47.
13. Kantelhardt, J. W., Zschiegner, S. A., Bunde, A., Havlin, S., Koscielny-Bunde, E., Stanley, H. E. (2002). Multifractal detrended fluctuation analysis of non-stationary time series. Physica A, 316, 87–114. doi: 10.1016/S0378-4371(02)01383-3
14. Kirichenko, L. O. (2011). Issledovanie viborochnix harakteristik, poluchennix metodom multifraktalnogo fluktuacionnogo analiza. Vestnik NTUU «KPI». Informatika, upravlenie i vichislitelnaya tehnika, 54, 101–110.
15. The package of TISEAN programs and concomitant documentation. Available at: http://www.mpipks-dresden.mpg.de/~tisean
16. Kantz, H., Schreiber, T. (2003). Nonlinear Time Series Ana(lysis, 2nd edition. Cambridge University Press, Cambridge, 388.
17. Packard, N. H., Crutchfield, J. P., Farmer, J. D., Shaw, R. S. (1980). Geometry from a Time Series. Physical Review Letters, 45 (9), 712–716. doi: 10.1103/PhysRevLett.45.712

INCREASING DATA TRANSMISSION QUALITY INDICATORS UNDER THE INFLUENCE OF THE "INFORMATION AGING" (p. 51-55)

Mikola Zaharchenko, Matin Magsud-ogli Gadzhyiev, Volodymyr Korchinsky, Oleksandr Rabuha

The influence of information "aging" on selecting information transmission methods with a given reception quality is considered. The main disadvantages of data transmission systems with information "aging", using bit-digital encoding, which are caused by a necessary code combination length limitation with a given (desired) communication quality are analyzed.

It is shown that similar contradictions in terms of the Shannon's fundamental coding theorem are also typical for data transmission systems with feedback (FB).

New, more effective transmission methods, ensuring both required transmission quality and transmission of large amounts of information in a given time interval are proposed. Using timer encoding in transmission systems reduces information delivery time by two times compared with BDC.

It is theoretically proved that using the timer signal designs (TSD) when selecting the coding method and signal type allows to increase the capacity of many allowed signal designs and the number of code combination realizations in the interval of elements by hundreds of times. This in turn allows to change information transmission probability for rate, i.e. transmit more data (code words) in less time.

Keywords: information aging, timer signal designs, bit-numeric codes, transmission system, decision feedback.

References

1. Rid, R. (2005). Osnovy teorii peredachi informacii. Moscow: «Vil'jams», 320.
2. Gusev, O. Ju., Konahovich, G. F., Puzirenko, O. Ju. (2010). Teorija elektrichnogo zv'jazku. Lviv: «Magnolija 2006», 364.
3. Akulinichev, Ju. P. (2010). Teorija jelektricheskoj svjazi: Uchebnoe posobie. SPb.: Izdatel'stvo «Lan'», 240.
4. Rihter, S. G. (2010). Kodirovanie i peredacha rechi v cifrovyh sistemah podvizhnoj svjazi. Moscow: «Gorjachaja linija–Telekom», 304.
5. Prokis, Dzh. (2000). Cifrovaja svjaz'. Moscow: Radio i svjaz', 800.
6. Vasil'ev, K. K., Glushkov, V. A., Dormidontov, A. V., Nesterenko, A. G. (2008). Teorija jelektricheskoj svjazi: uchebnoe posobie. Ul'janovsk: UlGTU, 452.
7. Zaharchenko, V. N. (1999). Sintez mnogopozicionnyh vremennyh kodov. Kiev.: Tehnika, 281.
8. Zaharchenko, N. V., Gadzhiev, M. M., Radzimovskij, B. K. (2014). Comparison of syndromic methods for correcting block positional and timing codes. Eastern-European Journal of Enterprise Technologies, 2/9(68), 4–9. Available at: http://journals.uran.ua/eejet/article/view/23091/21144
9. Korchins'kij, V. V., Kil'dishev, V. J., Homich, S. V., Belova Ju. V. (2012). Efektivnist' j-kratnogo povtorennja nadlishkovih tajmernih signal'nih konstrukcij. Vestnik NTU «KhPI», 26, 36–38.
10. Kil'dishev, V. J., Miroshnichenko, A. Ju., Nikolaev, N. O. Tanzhi, Ljuaj (2005). Vlijanie sosredotochennyh vo vremeni pomeh na iskazhenii tajmernyh signalov. Telekomunikacijni sistemi ta merezhi na zaliznichnomu transporti: Zb. nauk. pr., 71, 52–58.

DEVELOPMENT OF A STRUCTURAL GRAPH OBJECT APPARATUS AS A MEANS OF DEVELOPING MODELS FOR STUDYING COMPUTER NETWORK SURVIVABILITY (p. 56-59)

Victor Bondarenko

The paper introduces a new concept of structural graph object. The structural graph object is a generalization of the well-known concept of graph. The generalization is made in such a way that the connection may be not only between the graph nodes, but also between nodes and branches, as well as between subgraphs of the graph. The generalization makes it possible to form a computer network model that includes all possible threats (attack, failure or emergency) in the network operation, both natural and human-related factors. In contrast to the existing models, this model allows making a comprehensive analysis of the computer network survivability, taking into account hardware, software, informational and organizational aspects of survivability. These directions make the contribution to the concept of computer network survivability and should be considered together. This will make the operation of computer networks more reliable and stable.

Keywords: telecommunication systems, computer networks, survivability, structural graph objects, threats, destructive effect.

References

1. Dodonov, A. G., Lande, D. V. (2011). Zhivuchest informatsionnyih sistem. K.: Nauk. dumka, 256.
2. Gromov, Yu. Yu., Drachev, V. O., Nabatov, K. A., Ivanova O. G. (2007). Sintez i analiz zhivuchesti setevyih sistem. M.: Mashinostroenie-1, 152.
3. Stekolnikov, Yu. I. (2002). Zhivuchest sistem. SPb: Politehnika, 155.
4. Barabash, O.V. (2004). Postroenie funktsionalno ustoychivyih raspredelennyih informatsionnyih sistem. Kiev: Nats. Akadkmiya oboronyi Ukrainyi, 226.
5. Heegaard, P. E., Trivedi, K. S. (2009). Network survivability modeling. Computer Networks., 53 (8), 1215–1234. doi: 10.1016/j.comnet.2009.02.014
6. Sterbenz, J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., Smith P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks., 54 (8), 1245–1265. doi: 10.1016/j.comnet.2010.03.005
7. Huang, S., Xu, Y., Zhang, L. (2008). Study of network survivability based on multi-path routing mechanism. Science in China Series F: Information Sciences. 51 (11), 1898–1907. doi: 10.1007/s11432-008-0155-5
8. Wang, C., Ming, L., Zhao, J., Wang, D. (2011). A General Framework for Network Survivability Testing and Evaluation. Journal of Networks, 6 (6), 831–841.doi: 10.4304/jnw.6.6.831-841
9. Lin, F. Y.-S., Wang, Y.-S., Chung , H.-Y., Pan J.-L. (2012). Maximization of Network Survivability under Malicious and Epidemic Attacks. Presented at 26th International Conference on Advanced Information Networking and Applications Workshops. Japan. doi: 10.1109/WAINA.2012.10
10. Zaychenko, O. Yu. (2001). AnalIz pokaznikIv zhivuchostI merezh z tehnologIeyu ATM. NaukovI vIstI NTUU «KPI», 3, 14–21.

RESEARCH OF STABILITY AND SENSIBILITY OF THE METHOD OF PRIORITISATION OF KEY PERFORMANCE INDICATORS OF INFORMATION SYSTEM (p. 60-65)

Yaroslav Toroshanko, Volodymyr Shmatko, Maxim Vysochinenko, Anna Bulakovs'ka

The applied multi-criteria optimization problem - selecting the optimal structure of key performance indicators in the information system with heterogeneous data was considered. Preference relations are based on measurement results, probability estimates and subjective judgments. A modified analytic hierarchy process with exact calculations of the priority matrix eigenvalues was applied. Assessments of accuracy, stability and asymptotic sensitivity of the solving algorithms were given.

A mathematical model to assess the distribution of extreme eigenvalues of the pairwise comparison matrix, analyzed in the presence of errors and perturbations of the matrix elements using the analytic hierarchy process for decision-making within the multicriteria problem was developed. It was shown that the benefit from applying the new proposed methodology for accurate calculation of eigenvalues lies in ensuring the solution stability to perturbations of the values of the matrix elements and errors of intermediate calculations.

The obtained results can be used to improve the efficiency of information systems in two ways. Firstly, evaluation accuracy and detail of priorities of selected key indicators according to their relative importance are improved. Secondly, sustainability of information systems at selected and priority-arranged KPIs are critically evaluated.

Keywords: key performance indicators, stability, sensitivity, information system, priority level, analytic hierarchy process.

References

1. Floudas C. A., Pardalos, P. M. (2009). Encyclopedia of Optimization: Second Edition. Springer Science+Buisiness Media, LLC, 4645.
2. Saaty T. L. (1980). The Analytic Hierarchy Process.McGraw-Hill. New York, 278
3. Vinogradov, N., Drovovozov, V., Savchenko, A., Kudzinovskaya, I. (2011). An analysis of singularity of the matrices of priorities and sensibility of decisions as key performance indicators of the analytic hierarchies process. Journal of Qafqaz University (Mathematics and Computer Sciences), 32, 40–48.
4. Masood, S. A., Jahanzaib, M., Akhtar, K. (2013). Key Performance Indicators Prioritization in Whole Business Process: A Case of Manufacturing Industry. Life Science Journal, 10 (4s), 195–201.
5. Shahin, A., Mahbod, M. A. (2010). Prioritization of key performance indicators: An integration of analytical hierarchy process and goal setting. International Journal of Productivity and Performance Management, 56 (3), 226–240. doi: 10.1108/17410400710731437
6. Gantmakher, F. R. (1966). Matrix Theory. Moscow: Nauka, 576.
7. Faddeev, D. K., Faddeeva, V. N. (1963). Computational Methods of Linear Algebra, second ed. Moscow: Nauka, 656.
8. Tomovich, R., Vukobratovich, M. (1972). Total Theory of Sensibility. Moscow: Sovetskoe Radio, 240.
9. Ouyang, Ye., Hosein Fallah, M. (2010). A Performance Analysis for UMTS Packet Switched Network Based on Multivariate KPIs. International Journal of Next-Generation Networks (IJNGN), 2 (1), 80–94. doi: 10.1109/wts.2010.5479629
10. Nogin, V. D. (2004). The Borders of Appliance of Popular Methods of Scalarisation with Decision of the problems of Multi-criteria Choice. Methods of Disturbance in Homological Algebra and Systems Dynamics: Inter-university Proceedings. Saransk: Mordovia Univ., 59–68.
11. Abbasov, M. E., Barinov, N. P. Once more about the Borders of Appliance Еще раз of Linear Convolution in Analytic Hierarchy Process. Available at: http://www.labrate.ru/discus/messages/23/