METADATA FOR ROOT CAUSE ANALYSIS

Alexander A. Grusho, Nick A. Grusho, Michael I. Zabezhailo,
Elena E. Timonina and Vladimir V. Senchilo
Federal Research Center "Computer Science and Control"
of the Russian Academy of Sciences
Vavilova 44-2, 119333, Moscow, Russia
Email: grusho@yandex.ru, info@itake.ru, zabezhailo@yandex.ru,
eltimon@yandex.ru, volodias@mail.ru

KEYWORDS

Anomalies in distributed information systems, Approximate method of searching for anomalies, Metadata.

ABSTRACT

The paper is devoted to the task of finding the root cause of anomaly in a distributed information and computing system. An approximate approach is considered to detect implicit anomalies with accuracy to the object (of a component of the technical device, a node of a network infrastructure, an application or of an information resource). The approximate solution is based on the use of integral parameters that allow you to identify an anomaly, but do not allow you to indicate its cause. To work with such methods for determining the root causes of anomalies, auxiliary data is required, which is called metadata in the work.

The work describes a metadata construction algorithm and shows ways of using metadata to build an object in which the root cause of the anomaly is located. An approximate solution to the problem of finding the root cause of an anomaly with a help of quickly computable values of integral parameters is necessary to reduce the time of interruption of work processes due to implicit anomalies. It is assumed that small subsystems and nodes are easier to replace than to delve into the study of the cause.

INTRODUCTION

The increase in the size of distributed information and computing systems (DICS) exacerbates the problem of timely detection of failures, errors and shutdowns due to conflicts with information security (IS) requirements (hereinafter, anomalies). Implicit anomalies do not demonstrate their damage immediately, and Root Cause Analysis (RCA) is required to analyze and restore them. The problem of a remote search of implicit anomalies root causes is often a complicating factor. Modern operating systems can collect a large amount of data for RCA. However, remote analysis requires to transfer this data to the system administrator or IS officer (Grusho et al., 2020a), but most of this data will not be in demand, and their transfer over communication channels is not cheap and is not always possible. Big data requires more computing resources. RCA acceleration is often achieved by successful localizing of an anomalous DICS subsystem, which allows you to replace this subsystem and reduce the time to restore workflows.

Such a search requires certain auxiliary data, the collection and the organization of which depends on the speed and the effectiveness of the finding of a minimum possible object containing the root cause of the anomaly sought.

In the paper these supporting data are called metadata (MD). This name was chosen due to the fact that this term has already been used to solve such problems (Grusho et al., 2020b). The basis of MD is formed by a special case of Knowledge Graphs in which the arc from the object O_1 going to the object O_2, means that the anomaly in O_1 can initiate anomaly in O_2.

Arbitrary technical devices, network infrastructure, software and information resources will be called elements of the DICS. Arbitrary sets of elements are called DICS objects. Anomalies can occur in case of errors in data and data transformations, in case of technical breakdowns, as well as in case of unacceptable interactions of DICS objects. Anomalies can manifest themselves in the improper development of computing processes, obtaining incorrect calculation results. The most obvious manifestation of the anomaly is the unexpected shutdown of the computing process, the failure of the technical devices of the DICS. However, in all cases, implicit anomalies are possible, the location of which and the causes of their occurrence require a deep analysis (Grusho et al., 2018).

The model of implicit anomalies and search of root causes using integral parameters (IP) is constructed in (Grusho et al., 2020c). Such parameters are determined on the basis of generating algorithms (GA) that create the values of these parameters, and effective algorithms that display the values of these parameters. The RCA procedure proposed in (Grusho et al., 2020c) creates a DICS object containing a damaged GA fragment, the IP of which showed the presence of an anomaly.

Close problems arise when finding vulnerabilities in software using intelligent fuzzing (Jurn et al., 2019). Fuzzing is a technique for generating input values suitable for generating an error through target software analysis (Bekrar et al., 2012). Smart fuzzing has the advantage of knowing where errors can occur through software analysis. The tester can create test cases for that branch to extend the coverage of the code and generate valid conflicts. However, analyzing the target soft-

Communications of the ECMS, Volume 35, Issue 1,
Proceedings, ©ECMS Khalid Al-Begain, Mauro Iacono,
Lelio Campanile, Andrzej Bargiela (Editors)
ISBN: 978-3-937436-72-2 / 78-3-937436-73-9(CD) ISSN 2522-2414

ware requires expert knowledge and takes a long time to generate a template suitable for software input.

Thus, it is recognized that the most difficult problems, equivalent to RCA, require a lot of human labor. In this paper the reduction of labor is achieved by using the anomaly's IP which is used in search for the root cause.

PROPERTIES OF GENERATING ALGORITHMS

Further there are often used two terms: an algorithm and a process. The complete definition of the term "an algorithm" can be found in (Uspensky and Semenov, 1987)[7], and process concepts in a computer system can be found in (Hoare, 1985)[8]. In this paper, the links of these concepts are used. The process implements some algorithm or fragment of the algorithm. The algorithm in the computer system is implemented using one or more processes.

It is said that the algorithm passes through the object O if processes as elements of O are involved in its implementation.

The generating algorithm (GA) of the parameter I is the algorithm for generating and calculating values of parameter I (Grusho et al., 2020c), further will be denoted through GA(I). If I is an integral parameter, the values of I can be calculated using an algorithm independent of GA, but giving the same value as GA. In the case of an anomaly, both algorithms show the anomaly. At the same time, only GA is involved in the formation of an anomaly that both algorithms are able to identify. In (Grusho et al., 2020c) it is shown that there can be several GA for the parameter I. In this case it is necessary to determine the influence of several GA on the values of the parameter I. However, in the assumption of the presence of an anomaly, we do not take into account the influence of several GA on reducing the capability of the detection of the anomaly, and in terms of increasing for the detection capability of the anomaly with the help of I, it is not necessary to take into account the influence of other GA. Therefore, instead of considering the effect on the value I of several algorithms, we can talk about GA that have failures of fragments of algorithms or do not have them. It has been proved (Grusho et al., 2020c) that the uniqueness of the root cause of the anomaly is a sufficient condition for the manifestation of the anomaly in the integral parameter I, when the anomaly is generated by the failed fragment of the GA(I).

Consider a few questions about the content of DICS facilities. Since it is not always possible to enumerate all DICS elements included in the object O, inductive definitions should be used. Let the objects $O_1, ..., O_k$ be defined. Then the theoretical-plural union O of objects $O_1, ..., O_k$ is also an object. At the same time, these objects as sets of elements may not intersect, but may interact.

We define the interaction of objects O_1 and O_2 as the presence of processes ξ_1 in the object O_1 and ξ_2 in the object O_2 such that ξ_1 can at a given time of its implementation transmit information about its state to the process ξ_2 over a certain channel. In this case, the process ξ_2 is able to receive this information and use it in its algorithm (Hoare, 1985).

However, the anomaly in GA(I) is not always the root cause of the anomaly. Acceptable localization of the anomaly with the help of integral parameters is possible when the source of the anomaly is some unobserved process mediated by interacting with GA(I), through which the anomaly is detected. It is said that in the ξ_1 process, the anomaly error is spread to GA(I) if there are a number of interactions ξ_1 with ξ_2,..., ξ_k with ξ_{k+1}, where the last process belongs to GA(I). Hence, an abnormal fragment GA(I)(t) of GA(I) arises, where t is the value in a certain enumeration of fragments of GA(I). If in the process of ξ_1 is the root cause of the anomaly and it is the only one in the computer system, then (Grusho et al., 2020c) it can be proved that the anomalous fragment of GA allows you to see the anomaly in I. The process of such an anomalous transmission can be represented in the form of the following graph, which we will call the attachment.

$$GA(I)(t-1) \to GA(I)(t) \to$$

$$\uparrow$$

$$\xi_k$$

If you allow an attachment operation, you must define a branch operation. GA(I)(t) having an anomaly, when interacting with some ξ process, may initiate an anomaly in ξ.

$$GA(I)(t-1) \to GA(I)(t) \to GA(I)(t+1)$$

$$\downarrow$$

$$\xi$$

In this case as ξ can be GA fragment of another integral parameter I^*, so GA(I^*) will show an anomaly (with the only root cause of the anomaly, this will happen necessarily).

Let $O_1 \to O_2$ be objects in which ξ_1 can transmit to ξ_2 anomaly. Let O_{11}, O_{12} be partition of the object O_1 into two nonintersect objects, and O_{21}, O_{22} be a partition of the object O_2 into two nonintersect objects. The condition $O_1 \to O_2$ means that there are at least a pair of objects from different partitions for which it is carried out, for example, $O_{12} \to O_{21}$. Indeed, the process is an indivisible entity. Then if ξ_1 is in O_{12} and ξ_2 is in O_{21} then $O_{12} \to O_{21}$. Back, if $O_{12} \to O_{21}$, then in the object of merge we get $O_1 \to O_2$. If objects O_1 and O_2 intersect and ξ_1 is the common process, then when dividing each of them into two objects, there is a pair where ξ_1 will be in, and for this pair it remains possible to transmit an anomaly. From here we get the following statement.

Statement 1. Objects O_1 and O_2 satisfy the condition $O_1 \to O_2$ if and only if there are subsets of O_1^* in O_1 and O_2^* in O_2 such that $O_1^* \to O_2^*$.

The relation $\to$ is reflexive, transitive and antisymmetric, that is, it is a partial order.

For RCA using the integral parameter I for GA(I), the following important property is required. Let the objects $O_1, ..., O_k$ in MD can transfer anomaly to the object O. Then $O_1, ..., O_k$ satisfy the requirement of completeness for O if for parameter I provided that GA(I) passes through O, there is m, $m = 1, ... k$, such that GA(I) passes through O_m.

Requirements of completeness for O and $O_1, ..., O_k$ are difficult to verify. The following statement simplifies the situation somewhat.

Statement 2. The objects $O_1, ..., O_k$ satisfy the condition of completeness with respect to the object O for GA(I) if and only if the union $O_1, ..., O_k$ is the complete object with respect to the object O for GA(I).

Proof. The necessity follows from the following simple reasoning. If GA(I) passes through O_m, then it passes through the union $O_1, ..., O_k$.

Sufficiency. If GA(I) passes through the union $O_1, ..., O_k$, then there exists a fragment of this algorithm passing through this union. Each fragment of GA(I) is implemented by one or more processes $\xi_1, ..., \xi_l$, which are indivisible. The totality of these processes interacts in this order with the union $O_1, ..., O_k$. If there is an anomaly in fragment GA(I), then it must be at least in some ξ_n. If the indivisible process ξ_n passes through the union $O_1, ..., O_k$, then as an algorithm it passes through some set of this union. So the fragment GA(I) of ξ_n passes through at least one of the objects $O_1, ..., O_k$. The statement is proved.

Consequence. This statement is true for any parameter I and its GA(I).

Considering large disjoint components of the DICS, for which completeness is easy to check, we will transfer completeness to their partitions, which will automatically follow from Statement 2. Further, it will be assumed that for the considered sets of MD the completeness conditions are met.

If GA(I) passes through an object O in which interaction with an anomalous process ξ occurs, then it is easy to propose a simple probabilistic model for the propagation of the anomaly. Let p be the probability that GA(I) will receive an anomaly from ξ. If there are n independent interactions of GA(I) with abnormal processes in O, then the probability of an anomaly in GA(I) is $1-(1-p)^n$. It is interesting to look at this formula in various extreme cases of the values of these parameters.

If $p = 1$, then the propagation of the anomaly in interactions towards O occurs with probability 1. If error propagation occurs with probability 1, then the widespread propagation of the anomaly poses the greatest difficulties for RCA. An example of such an error is given in (Grusho et al., 2018, 2017).

If p is close to or equal to 0, then the probability of propagation of the anomaly is small, but it is easier to localize the cause of the anomaly (if such an anomaly can be seen). An example of such an anomaly is the prefailed state of the hard drive when it is still working, but an anomaly in its device will inevitably cause it to fail. It is possible to see such an anomaly by indirect signs, in particular, by a significant increase in the time of access to the disk (Grusho et al., 2020c).

Further, it is believed that the DICS propagates errors with $p = 1$. In order to effectively use the MD to search for root causes, it is necessary to construct a hierarchical decomposition of the MD and use it to accelerate algorithms for searching for objects containing an anomaly.

CONSTRUCTION AND USAGE OF MD

In the introduction, it was noted that MD are auxiliary information for a system administrator or an IS officer, which is built on the basis of knowledge graphs (Brandón et al., 2020; Nickel et al., 2016) of the form $X \to^c Y$, where X and Y are objects of the DICS, c is the action that is transmitted from X to Y. In our case, the hierarchy of the MD is built sequently. Let the object X may pass an anomaly to the object Y. This binary relationship was entered earlier and is denoted by $X \to Y$. As shown above, this relationship generates a partial order on a subset of objects. The largest element of this order is the DICS. Assuming the completeness of the partitions of objects and the finiteness of the tree representing the sequences of such partitions, we will build the MD of three parts.

1. The set of objects with the help of successive partitions into meaningful nodes and technologies and their hierarchy are formed from structural model of DICS (Denisov and Kolesnikov, 1982). They are used to search for objects that cover the anomaly using IP and object relationships derived from the structural model.

2. The set of integral parameters IP is defined in the constructed set of objects (where this can be done).

3. From IP, the completeness properties of object partitions and their relationships $O \to O"$, we build the MD as trees whose roots coincide with objects containing IP, and the arrows are directed to the roots.

Consider the issue of constructing integral parameters that lie in the objects constructed in item 1. Let O be an object (node, device, data conversion information technology, information resource, communication fragment, program, etc.) – this is a set of elements of the DICS. Each DICS element is described by a plurality of characteristics (Ashby, 1956). Each characteristic is described by one or more parameters and areas of their normal values (Ashby, 1962). That is, any system can be described by a plurality of its parameters (Ashby, 1962; Grusho et al., 2016). An anomaly in a parameter value is the appearance of a value that goes beyond normal values. Since the function of belonging to a set of normal values of a parameter can be calculated without knowledge of the GA of this parameter, then formally any parameter can be integral. However, in practice, not all system parameters can be seen and learned their values in the real system, then only a few set of integral parameters should be found that cover the most important subsystems of the DICS if possible. At the same time, the importance lies not only in the allocation of

risk objects, but also in the set of interactions of the selected integral parameters based on observations of the system. Therefore, it is necessary to build IP with an orientation on the following principles.

If IP could not be allocated in the desired object, then it is necessary to divide this object into subobjects before IP appears in each branch.

If it is not possible to achieve completeness in the selection of subobjects, then you need to supplement more subobjects before splitting.

If two or more IP are selected in the object, the object must be divided into subobjects so that horizontal links are converted to vertical or simply one of IP remains in each subobject.

From the set of IP, from objects which contain these IP, and from their relations $O_1 \rightarrow O_2$, we build influence trees. If IP is contained in the object O, then the influence tree has the root O, and the arcs of all objects are oriented to O. If an arc emerges from the object of the tree to a lower object of the tree, then this object can affect objects that are located deeper in this tree, then this object can be met again in the tree.

Consider the usage of MD for RCA.

1. IP allows you to identify an anomaly in objects of the constructed object hierarchy.

2. The search of the following object with the root cause is based on the search of the IP with an anomaly value on the branch of the corresponding MD tree.

3. If IP is detected on a branch of the tree, the tree generated by the object with this IP is considered and iteration is repeated. The lowest (from the root of the tree) object with an anomaly determines the coverage of the anomaly in the created diagram of GA. The anomaly may not be covered only when the root cause is in an object through which GA of the last identified IP with the anomaly value does not pass. Therefore, the last object with the anomaly must be extended to merge all the objects from which the arrows enter the object with the anomaly (including closure).

The effectiveness of RCA by the considered method is evaluated further.

1. When the condition of completeness is fulfilled, all potential carriers of the anomaly are covered by the last built object with the anomaly.

2. The coverage of the anomaly is determined by the object with the last detected IP with the abnormal value, provided that the root cause is unique.

3. The usage of last identified IP after objects located in the tree that do not have IP is based on the transitivity of the $\rightarrow$ relations.

CONCLUSION

The use of integral parameters in RCA allowed to get a new look at the problem of causality analysis. The idea of RCA based on IP is presented for the first time in the work (Grusho et al., 2020c). In this work, the regions covering the anomaly are more clearly defined and the organization of the creation and use of MD by the system administrator and the IS officer has been developed. Note that in remote cause analysis, search by IP with an abnormal values reduces the amount of information transmitted.

In addition, the interactions between IP and objects of DICS were investigated, which in fact can give an answer to the question about the coverage of the anomaly. A hierarchical organization of MD has been determined, which allows formalizing the algorithm for finding anomaly coverage using IP. It is shown under what conditions a good coverage of the anomaly is achieved using objects containing IP and when additional information needs to be collected and used to reduce the region of coverage of the anomaly.

Unfortunately, all experiments on the practical application of the proposed approach were carried out manually by organizing the actions of the system administrator according to the constructed algorithm. This does not mean that it is impossible to automate the collection, storage and application of the IP method in RCA. However, the authors are confident that the automated system should be built on the basis of algorithms that maximize usage of the experience of system administrators and IS officers. It should be noted that during the research, the initial vision of the problem has changed significantly.

Further research will be related to the construction of algorithms for big data in real large DICS.

Acknowledgements

This work was partially supported by the Russian Foundation for Basic Research (grant No. 18-29-03081).

REFERENCES

Grusho, N. A., A. A. Grusho, M. I. Zabezhailo, and E. E. Timonina. 2020. "Methods of finding the causes of information technology failures by means of metadata". *Informatics and applications* 14, No. 2, 33–39.

Grusho, N. A., A. A. Grusho, and E. E. Timonina. 2020. "Localizing failures with metadata". *Automatic Control and Computer Sciences* 54, No. 8, 988–992.

Grusho, A. A., M. I. Zabezhailo, A. A. Zatsarinny, A. V. Nikolaev, V. O. Piskovski, V. V. Senchilo, I. V. Sudarikov, and E. E. Timonina. 2018. "About the Analysis of Erratic Statuses in the Distributed Computing Systems". *Systems and Means of Informatics* 28, No. 1, 99–109.

Grusho, A.A., M.I. Zabezhailo, A.A. Zatsarinny, A.V. Nikolaev, V.O. Piskovski, V.V. Senchilo, and E.E. Timonina. 2017. "Erroneous states classifications in dictributed computing systems and sources of their occurences". *Systems and Means of Informatics* 27, No 2, 29–40.

Grusho, A. A., N. A. Grusho, M. I. Zabezhailo, and E. E. Timonina. 2020. "Root Cause Anomaly Localization". *Information Security Problems. Computer Systems* 4 (in press).

Jurn, J., T. Kim, and H. Kim. 2019. "A Survey of Automated Root Cause Analysis of Software Vulnerability". In: *Innovative Mobile and Internet Services in Ubiquitous Computing*, L. Barolli, F. Xhafa, N. Javaid, and T. Enokido (Eds), Advances in Intelligent Systems and Computing 773. Springer, Cham, 756–761.

Bekrar, S., C. Bekrar, R. Groz, and L. Mounier. 2012. "A taint based approach for smart fuzzing". In: *2012 IEEE Fifth International Conference on Software Testing, Verification and Validation*, Montreal, QC, 818–825.

Uspensky, V.A., and A.L. Semenov. 1987. *Theory of algorithms: the main discoveries and applications*, Moscow: Science, 288 p. (in Russian).

Hoare, C. A. R. 1985. *Comucating Sequential Processes*, Englewood Cliffs (N.J.): Prentice-Hall, 256 p.

Brandón, Álvaro, Marc Solé, Alberto Huélamo, David Solans, María S. Pérez, Victor Muntés-Mulero. 2020. "Graph-based root cause analysis for service-oriented and microservice architectures". *Journal of Systems and Software* 159, 1–17.

Nickel, M., K. Murphy, V. Tresp and E. Gabrilovich. 2016. "A Review of Relational Machine Learning for Knowledge Graphs". *Proceedings of the IEEE* 104, No. 1, 11–33.

Denisov, A.A., and D.N. Kolesnikov. 1982. *Theory of large control systems: Textbook for universities*, Leningrad: Energoizdat, 288 p. (in Russian).

Ashby, W. Ross. 1956. *An Introduction to Cybernetics*, London: Chapman and Hall, 295 p.

Ashby, W. Ross. 1962. *Design for a Brain. The Origin of Adaptive Behavior*, 2nd Ed. Revised.Moscow: Foreign literature, (Russian translation).

Grusho, A., N. Grusho, and E. Timonina. 2016. "Detection of anomalies in non-numerical data". In: *2016 8th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops* (ICUMT), Lisbon, 273–276.

AUTHOR BIOGRAPHIES

ALEXANDER A. GRUSHO,Professor (1993), Doctor of Science in physics and mathematics (1990). He is principal scientist at Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences and Professor of Moscow State University.

Research interests: probability theory and mathematical statistics, information security, discrete mathematics, computer sciences.

His email is `grusho@yandex.ru`.

NICK A. GRUSHO has graduated from the Moscow Technical University. He is Candidate of Science (PhD) in physics and mathematics. At present he works as senior scientist at Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences (FRC CSC RAS).

Research interests: probability theory and mathematical statistics, information security, simulation theory and practice, computer sciences.

His email is `info@itake.ru`.

MICHAEL I. ZABEZHAILO has graduated from the Institute of Physics and Technology and gained the Candidate degree (PhD) in theoretical computer science (1983). He is Doctor of Science in physics and mathematics (2016). Now he works as Head of laboratory in Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences.

Research interests: mathematical foundations of artificial intelligence, reasoning modeling, information security, theoretical computer sciences.

His email is: `zabezhailo@yandex.ru`.

VLADIMIR V. SENCHILO has graduated from the Moscow Institute of Physics and Technology. He is scientist at Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences.

Research interests: computer sciences, machine learning, optimization theory, data mining, financial risk.

His e-mail address is: `volodias@mail.ru`.

ELENA E. TIMONINA has graduated from the Moscow Institute of Electronics and Mathematics and obtained the Candidate degree (PhD) in physics and mathematics (1974). She is Doctor in Technical Science (2005), Professor (2007). Now she works as leading scientist in Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences (FRC CSC RAS).

Research interests: probability theory and mathematical statistics, information security, cryptography, computer sciences.

Her email is `eltimon@yandex.ru`.