Models and classifications of secure resource management methods in distributed information communication networks

R R Turluyev¹, M Yu Ivanov² and G M Beregova³

¹ Chechen State University, 17a, Dudaev Boulevard, Grozny, 364015, Russia
² Bratsk State University, 40, Makarenko str., Bratsk, 665709, Russia
³ Irkutsk National Research Technical University, 83, Lermontova str., Irkutsk, 664074, Russia

E-mail: ibr024@mail.ru

Abstract. This paper analyzes the models and classification of secure resource management methods in distributed information communication networks in order to identify the most optimal model.

1. Introduction

Despite many problems that arise in organizing the interaction of objects in distributed information systems, the main one remains the task of protecting a share when organizing its division among many competing processes (resource management task) [9-11, 24-26]. This task is divided into two key subtasks.

The first subtask relates to a conflict that occurs when processes share a share. In this case, if the algorithm is chosen incorrectly, there is a threat of self-destruction of such a resource. For example, multiple accesses of a database may result in incorrect results, and in the worst case, complete database destruction. When accessing a common communication channel, a situation is possible when the LAN stops transmitting data, spending all the time to resolve the conflict [4].

Thus, the system can be destroyed without any malicious intent for natural reasons hidden in it itself. The second sub-task is related to malicious intent on the part of persons wishing to access information hidden from them, or wishing to destroy the information (telecommunication) system [12–14]. In this case, we have to talk about the attack, and, if it succeeds, about the intervention (forced introduction) of certain alien objects that disrupt the normal operation of the system.

When solving these problems, the choice of the control model is of fundamental importance, since many key parameters depend on it, primarily the safety and effectiveness of control algorithms [20]. Thus, the classification of control models according to certain characteristics is of great importance. For example, there is traditionally a classification of models on the principle of the presence or absence of a control center [8, 11, 21-23].

This classification is conceptual and can only help to develop the most general principles for the construction of the system. Therefore, it is interesting to find classifications and models that provide the most informed solutions when choosing a management method.
2. Analysis of models

ISO/OSI Model

The ISO/OSI model (seven-tier open systems architecture) is developed on the basis of the concept of interaction of user processes (application processes) through the transport network using the messaging method (Fig. 1) [15].

At the same time, the task of the transport network is to deliver messages from one point to another without any interpretation, as well as masking the message delivery mechanism (i.e., smoothing out various implementations of network segments, or ensuring transparency). Thus, according to the concept, the network appears to be homogeneous to user processes [1, 2].

The ISO/OSI model (Figure 2) is a detail of the concept considered. In addition to detail, the model arranges processes vertically (interface interactions) and horizontally (protocol interactions). Let us consider the main features of the ISO/OSI model (hereinafter simply models). As can be seen from the figure, at least two systems are required for its consideration. In the figure, these two systems are designated as System A and System B.

The lower four layers (transport-physical) according to the concept form a transport network transparent to high-level processes (application-session). Protocols for the transport network are currently standardized (for example, the IP or X.25 protocol family).
Figure 3. Mechanisms for interaction of protocol processes

The mechanisms of process interaction in accordance with these protocols are well described in the literature [2, 4, 5] and in the documentation on standards (RFC and CCTT), so we will not touch them. We note only that the transport layer protocol is called end-to-end. Processes of this level provide a network-wide interface (transport layer interface) within the systems.

Monitoring (throughout the session) of the correct use of resources includes (if necessary) maintaining the interaction statistics of the participating processes of the session.

The main difficulty in organizing a session is solving the problem of building a logical star of processes (Fig. 3), i.e. building an algorithm for mutual exclusion during multiple access (MD) of processes to a shared resource (server) in time sharing mode [3, 18, 19]. This task is difficult even for centrally managed, concentrated systems; in distributed systems, it is complicated by at least an order of magnitude. The goal of the task is to eliminate the conflict that arises during CBM, and, as a result, to ensure the safe management of common resources (CR).

Figure 4. Hoor's monitoring

Moreover, the work provides a method that allows you to organize the storage of history in the memory area of client processes. In this method, after executing each elementary command, it is proposed to send the client only the data (result), but also the current state of the server process (context). At the same time, the client sends the server not only a command with the necessary data, but also a saved context. Thus, the server resumes service from the point of execution of the last client command. The disadvantage of the method is the impossibility of using it in distributed telecommunications systems (PTCS) with a low data rate.
The following process interoperability is based on server parallelization (Figure 5). At the same time, a certain generating process is constantly present on the server machine. Each time a new client is connected, this process starts a copy of the server so that each client has its own query queue. Thus, the storage of the history and the preservation of the context is assigned to the operating system. The scheme is very popular due to the simplicity of its implementation, and is used in a wide class of client-server systems (for example, in the WWW - worldwide web). However, due to the absence of a common query queue in the schema, it becomes necessary to solve access to a share - for example, a database, and transaction synchronization problems come to the fore. A typical situation for such systems is a denial of service, when all the time is spent on resolving the conflict [4–6], or incorrect maintenance (selling two tickets for the same place is the Siren system).

The last, highest level of the ISO/OSI model - the application - allows us to solve any problems in case they cannot be solved using standard OS tools. For example, in UNIX and Microsoft Windows, the CBM problem is solved using the resource blocking flag, which actually leads us to random service algorithms with all the resulting negative consequences (congestion of systems, denial of service, and so on). Therefore, it is necessary to place the appropriate algorithms (operation with FIFO, HPF, RR queues and so on) at the application level in safe RIS and PTCS.

3. Analysis of classifications

Basic models. We consider the classification of systems based on the principle of interaction of command flows with data flows (Flynn classification [20]). This classification involves four models - SISD (Single Instructions, Single Data), SIMPLE (Single Instructions, Multiple Data), MISD (Multiple Instructions, Single Data) and MIMD (Multiple Instructions) Initially, models were developed to analyze the principles of instruction synchronization in multiprocessor systems, and they are currently used in this area.

Let us enter some definitions.
A flow (according to Flynn) will be called a process if it requires some (possibly remote) resource for its execution.

A resource means any object of the system (data, procedures, other processes), if it can be provided by the system at the disposal of one or more processes. Let us say that the task of managing a resource exists if there is competition between several processes for a certain resource. We consider the applicability of Flynn models within the definitions entered [7].

The SISD model (Figure 6) is conflict-free due to the presence of only one process (thread, processor) and cannot reflect the essence of the task of managing a resource due to the lack of competition in it. However, SISD can serve as an excellent model of the Hoora monitor - some privileged operating system (OS) process that is responsible for correctly separating the resource guarded by the monitor.

In fact, all the tasks that occur in the CBM are somehow reduced to ordering requests (i.e., placing parallel processes in some sequentially serviced queue) in order to facilitate process synchronization. Strictly speaking, the main task in solving the problem of mutual exclusion in a parallel environment is just to reduce all fairly complex interactions to the SISD model.

![Figure 6. SISD Model](image)

The SIMD model (Figure 6) assumes many processes running the same algorithm. Moreover, it is implicitly understood that at each point in time, all processes execute the same command, each with its own data stream. It will be appreciated that such scheme cannot be implemented on a single processor machine and requires a multiprocessor.

![Figure 7. SIMD Model](image)
Within such model (which is true for other classical multiprocessors in which each processor performs only one process), the terms "process" and "processor" are essentially identical. The model cannot be used to solve a resource management problem for two reasons. Firstly, unlike SISD, there is no share in it. Secondly, in RTCS, for topological reasons, it is impossible to synchronize the actions of several processes so that the commands in these processes are executed synchronously.

**Figure 8. MISD Model**

MISD model (Figure 8). Flynn defined this model as an "empty class" because at the time of classification creation there were no systems suitable for MISD. Currently, a system having explicit MISD features is known. This is a class of pipeline processors where many different processors perform operations on common data. In this case, the actions of the processors must be interconnected. Moving from pipeline processors to multiple processes in RTCS and from common data to a shared resource, we see that MISD is, in fact, ideal for solving our problem. In fact, MISD has both features that determine the task of managing a resource - the presence of many processes and their competition for a shared resource [16, 17].

4. Conclusion

Today's technologies provide a range of tools to control access to distributed resources. There are two groups of technologies used to provide security in distributed systems. The first group provides partial authentication, communication protection and independence of the access control mechanism from the applied communication technology. This group includes Kerberos, SESAME, and GAA API systems. This allows you to use any communication protocol, but application developers have to make significant efforts to integrate security technologies with the main communication mechanisms.

Here are the main results obtained during the work.

1. Models and classifications of distributed telecommunication systems construction were analyzed. Based on it, a resource monitoring classification (RMK) is proposed, which allows you to identify the main relationships between the processes and resources of the system at the early stages of design.

2. Analysis of distributed resource sharing algorithms in RTCS is performed. It has been found that the weak point of these algorithms is the procedure for delivering broadcast messages in a distributed environment.

3. Based on the studies conducted, the need was identified for the creation of reliable high-speed algorithms and software and hardware for managing the safe division of distributed resources.

4. For cluster RTCS with DNU and VOC, control algorithms are proposed using the communication channel not only as a means of transmitting information, but also as a common resource necessary for synchronizing distributed processes. This approach allows you to reduce overhead on management, making them independent of the number of subscribers of the distributed system.
5. An extended Shannon model is proposed, taking into account the specifics of data transfer and processing in RITCS.

References
[1] Butrimenko A V 1981 Development and operation of computer networks (Moscow: Finance and Statistics) 256 p
[2] Vine Yu and Paluoya R 2013 Specialized local data network of a distributed control system. In book: Local computer networks (Theses of reports of the All-Union Conference) (Riga: IEVT) pp 274-278
[3] Dedkov A F and Schers A L 1984 Language tools for organizing distributed processes in local networks. In book: Local computer networks (Theses of reports of the All-Union Conference) (Riga, EEVT) pp 146-148
[4] Prangishvili I V, Podlazov B C and Stetsyura G G 2012 Local microprocessor computing networks (Moscow: Science)
[5] Prangishvili I V and Stetsyura G G 1980 Microprocessor systems (Moscow: Science) 236 p
[6] Zimmermann H 1980 OSI Reference Model - the ISO Model of Architecture for Open Systems Interconnection IEEE Trans. Commun. 28(4) 425-432
[7] Illarionov Yu A and Monakhov M Yu 2004 Safe management of resources in distributed information and telecommunication systems, Monograph (Vladimir: VISU) 212 p
[8] Illarionov Yu A 2015 Introduction to the theory of information security. Comprehensive protection of informatization facilities. Book 8. Tutorial (Vladimir: VISU) 88 p
[9] William A 2011 System programming in Windows 2000 (St. Petersburg: Peter) 624 p
[10] Dijkstra E 1972 Interaction of sequential processes. In the book: Programming languages (Moscow: World) pp 9-86
[11] Cyclitzis D and Bernstein F 1977 Operating systems (Moscow: World) 336 p
[12] Levin M 2001 Methods of hacker attacks (Moscow: Educational book plus) 222 p
[13] Lukatsky A 2001 Detection of attacks (St. Petersburg: BHV-Petersburg) 624 p
[14] Lukatsky A V 2000 Year 1999: a look at the information security market (BYTE, JVb6-7)
[15] Material from the National Library named after N. E. Bauman Network model OSI 2015
[16] Zimmermann H 2013 OSI Reference Model - the ISO Model of Architecture for Open Systems Interconnection IEEE Trans. Commun. 28(4) 425-432
[17] Davis D et al 1984 Computing networks and network protocols (Moscow: World) 536 p
[18] Erkhov E 1998 Scenarios of attacks on banking systems in the Internet Analytical Banking J. 7
[19] Hoor K 2013 Record processing. In book: Programming languages (Moscow: World) pp 278-342
[20] Karpikov A V, Aliev R I and Babyr N V 2020 An analysis of the effectiveness of hydraulic fracturing at YS1 of the Northern field IOP Conf. Ser.: Mater. Sci. Eng. 952 012036
[21] Klyuev R, Bosikov I, Gavrina O, Madaeva M and Sokolov A 2021 Improving the energy efficiency of technological equipment at mining enterprises Advances in Intelligent Systems and Computing 1258 262-271. DOI: 10.1007/978-3-030-57450-5_24
[22] Klyuev R, Fomenko O, Gavrina O, Turluev R and Marzoev S 2021 Energy indicators of drilling machines and excavators in mountain territories Advances in Intelligent Systems and Computing 1258 272-281. DOI: 10.1007/978-3-030-57450-5_25
[23] Sidorenko A A, Dmitriyev P N and Ivanov V V 2020 A study of gas drainage methods efficiency in Kotinskaya mine in Russia ARPN J. of Engineering and Applied Sciences 15(4) 530-535
[24] Mazakov E B, Matrokhina K V and Trofimets V Y 2021 Traffic management at the enterprises of the mineral industry. Advances in raw material industries for sustainable development goals (London: CRC Press) pp 528
[25] Kortiev L I, Klyuev R V, Totchiev F G, Vaneev S D and Babunska N I 2020 Temporary and operational transport roads in construction of transfer linear structures and their scientific and
technical support *IOP Conf. Ser.: Mater. Sci. Eng.* 952 012023. DOI: 10.1088/1757-899X/952/1/012023

[26] Makhovikov A and Kryltskov S 2016 Development of secure and reliable communications system for corporate sector over mobile telecom networks *Asian J. of Information Technology* 15(24) 5120-5125