Project № 1994P

Annual Technical Report

For the first year
(December 01, 2000 - November 30, 2001)

1. Title of project

Formal Methods for Information Protection Technology

2. Contracting Institute

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS)

3. Participating Institutes

None

4. Project Manager

Oleg V. Karsayev
(812)-323-3570,
(812)-328-0685,
ok@mail.iias.spb.su

5. Commencement Date, Duration

December 01, 2000
3 years

6. Partner

European Office of Aerospace Research and Development

SPIIRAS Director,

Prof. Rafael M.Yusupov

Project Manager

Dr. Oleg V. Karsayev

December 2001

Task # 2

MATHEMATICAL FOUNDATIONS, ARCHITECTURE AND PRINCIPLES OF IMPLEMENTATION OF MULTI-AGENT LEARNING COMPONENTS FOR ATTACK DETECTION IN COMPUTER NETWORKS

1. Task Principal Investigator, phone number, fax number, e-mail address

Prof. Vladimir I. Gorodetski, (812)-323-3570, (812)-328-0685, gor@mail.iias.spb.su

2. Brief description of the work plan: objective, expected results, technical approach

Brief description of the work plan

B-1. Development of the learning task ontology, allocation of learning tasks over generic learning agents	1-3 Quarters
Interim Report #1 summarizing the results of the task B-1	3 Quarter
B-2. Development of architecture of the Multi-agent Learning System and mathematical methods realizing learning functionalities of the generic agents.	4-6 Quarters
Submitting a paper to an International Journal	5 Quarter
Interim Report #2 summarizing the results of the task B-2.	6 Quarter
B-3. Development of the protocols of inter-level intelligent agent interaction (negotiation), generalization of the particular agent decisions according to the meta-classification approach and development of architecture of the Multi-agent Learning System as a whole.	7-8 Quarters
B-4. Development of object-oriented conceptual project of the Multi-agent Learning System	6-8 Quarters
B-5. Development of the software prototype of the Multi-agent Learning System implementing theoretical results of research and its evaluation.	9-11 Quarter
Interim Report #3 describing the results of the task B-4 and partially developed software prototype of the components of the Multi-agent Learning System.	10 Quarter
B-6. Evaluation of the properties, advantages and disadvantages of the developed architecture and mathematical methods implemented within the prototype of the intelligent Multi-agent Learning system	12 Quarter
Final report, summarizing the results of simulation of the developed Multi-agent Learning System aimed at attack detection, as well as final conclusion concerning the research results on the task 2 as a whole.	12 Quarter

Notice: The grey shaded rows correspond to the tasks to be solved during the first year research. The Task B-2 has to be solved only partially.

Objective

The objectives of the Task 2 of this project are mathematical foundation, agent-based architecture, and principles of implementation of the Intrusion Detection Learning Systems operating in a parallel with the Computer Network Assurance System.

Expected results

1. Learning task ontology,
2. Allocation of learning tasks over generic learning agents and development of the architecture of their interaction within Multi-agent Learning System;

3. Mathematical basis and algorithms realizing learning functionalities of the particular agents and software prototypes of the components of the Multi-agent Learning System based on theoretical results of the research;
4. Simulation-based evaluation of the properties, advantages and disadvantages of the developed multi-agent model and architecture of the Multi-agent Learning system aimed to support adaptability and learnability of the Network Security System.

Technical approach

A key issue of an intrusion detection learning task is a selection and development (if necessary) of accurate and efficient methods and algorithms specialized for the data structures specifying intrusions. This data specifying is represented mainly by timely ordered sequences of audit data of various length specified in terms of repeatable symbols. These symbols correspond to the preprocessed messages of the input traffic at a host port of the computer network. In case of the distributed attack as well as in case of the normal distributed users' activity, a set of such sequences specifies user's activity. Mining of such data is a challenge in knowledge discovery from databases.

The approaches to be used within the last task are threefold. The first class of them is based on the specification of each input sequence (example) corresponding to a class of attacks or normal activity as a word of an unknown formal Context Free language. In this case the learning task may be reduced to a task of the inductive formal grammar recovery. The second class of approaches to be used is based on statistical properties of the examples specifying normal and abnormal activity of the user(s) accessing the network resources. The third class of methods intends to solve the task of the rule extraction from the training data sample, and its result is specified in terms of predicates given over higher level concepts like patterns.

An important issue is a decomposition of the whole intrusion detection learning task into multitude of sub-tasks in accordance with the ontology of attacks, and their allocation to specialized learning software agents. Intrusion detection learning system will be implemented on the basis of multi-agent architecture. Within it, each specialized learning agent is considered as the generic one capable to extract patterns of a particular class (association rules, frequent patterns, production rules given over patterns, etc.), and it should be capable to extract knowledge from data of the fixed formats (event sequences, sets of patterns, subset of rules, etc.).

For the purpose of the formal specification of learning agent interactions, as needed in learning detection of distributed attacks, the idea of meta-classification will be used. This idea entails the necessity of distributed learning which corresponds to the multi-level learning aiming at fusion of knowledge resulted from local learning procedures realized by particular learning agents.

3. Technical progress during the year of reference

Technical progress during the year of reference is fully compliant regarding both tasks predefined by the Work plan, and the schedule of their completion.

Achievements of the past year

The basic achievements of the past year correspond to the tasks scheduled. These tasks and respective results are described below.

Within the task B-1 "Development of the learning task ontology, allocation of learning tasks over generic learning agents" the following subtasks should be solved:

1. Analysis of the structure of the training data.
2. Development of the multi-level ontology of the learning tasks.
3. Development of conceptual model of the generic agents of the multi-agent learning system.

Also the part of the task B-2 "Development of architecture of the Multi-agent Learning System and mathematical methods realizing learning functionalities of the generic agents" scheduled for 4–6 Quarters should be solved partially. Since the related results are only at a preliminary stage, they are not summarized below.

Thus, in more detail, the main results obtained during the first year research are as follows.

1. Analysis of the structure and other peculiarities of the training data.

Conceptual analysis of any learning problem includes, first of all, analysis of the sources of the knowledge. Within the task in question the main sources of knowledge are historical interpreted audit data containing sequences of user' activities ("examples") that can correspond to "*normal*", "*abnormal*" or "*interpreted abnormal*" data. (In the latter case it is supposed that the class of attack is definitely determined). In the Project, intrusion detection system is considered as a multi-sensor knowledge-based data fusion system. As a rule, information from a single source does not contain much evidence that allows the timely and efficient detection of attacks and security policies violations. In order to construct an efficient intrusion detection system and a learning system, it is necessary to utilize an interconnected complex of audit data received from multiple sources and representing data on different levels of generalization (on the network level, OS level, application level, and additional sources level). Addressing multiple information sources may significantly increase the validity of decisions related to attack detection and network security. The respective learning task is considered as a distributed multi-level data mining and knowledge discovery problem to be implemented on the basis of multi-agent architecture.

The known attack detection learning mechanisms are computationally complex. The complexity can be significantly reduced due to the preliminary analysis and identification of the most representative and informative attributes of the subjects' (including malefactors') activities (both internal and external to the system under protection) registered in the audit data. Such attributes include repeated instances and combinations (patterns) of events; mistyped commands; indications of exploitation of the known vulnerabilities, illegal parameters, irregularities in the network traffic parameters and contents; substantial discrepancies in the values of attributes that characterize the system subjects' operations profile (e.g., time and date of activity, subject's address, services used by subjects, system resources characteristics including CPU usage data, RAM/HDD/files/ports access data, etc.), and unexplained problems (e.g., router failure, server overload, failure to launch a system service, etc.). Involvement of experts at this stage of learning could substantially cut down the pattern search and dimensions of data needed for learning.

The main peculiarities of the problem in question are caused by the temporal and distributed nature of the processes to be learned and data reflecting these processes. In the Project this nature of the training and testing data is specified in terms of unified model of temporal sequences of events and patterns to be mined from the audit data.

2. Development of the multi-level ontology of the learning tasks

Consistent operation of a large scale distributed system, which makes decisions in a knowledge-based fashion, can be only provided in case if distributed entities are capable to "understand" each other. The efficient way to achieve mutual understanding between distributed entities (in our case–agents) is to use *ontology-based approach* representing the shared knowledge of distributed entities. The ontology forms the necessary basis for local knowledge bases consistency, distributed knowledge base integrity and correct interpretation of the messages, entities exchange with.

The multi-level ontology of the intrusion detection learning problem unites a structured multitude of basic notions. This ontology encompasses the notions from several domain ontologies, i.e. from the "Data fusion" & "Data fusion learning" problem domain ontology, from the "Intrusion detection" and "Intrusion Detection Learning" subject domain ontologies. The ontology developed serves as the basis for design and implementation of the upper-level representation of distributed knowledge base. This level of knowledge provides, on the one hand, for the integrity of the distributed knowledge base, and on the other hand, for the "mutual understanding" of the agents interacting via message exchange.

3. Development of conceptual model of the generic agents of the multi-agent learning system

The learned intrusion detection system is viewed as a multi-sensor multi-level data fusion system. This system makes decisions on the basis of a multi-level model of input data (network input traffic and/or audit data) processing. Based on this view, the conceptual model of the multi-agent learning system has been developed.

On the basis of analysis of the learning data structure a number of adequate learning methods (algorithms) that according to the authors' opinion should be efficient in solving the learning tasks are selected. The chosen multitude of methods includes both some of the widely known methods (e.g., from the multitude of them including *ID3*, *C4.5*, *AQ*, *CN2*, boosting, and the meta-

classification methodology) and also methods that have been or are being developed by the authors (e.g., *Visual Analytical Method –VAM*, *GK2* algorithm, *Algebraic Bayes Networks*).

The above mathematical fundamentals made it possible to develop a conceptual model of the intrusion detection learning system. In the research a multi-agent architecture of intrusion detection learning system is decided. Generic agent classes of the multi-agent intrusion detection learning system under development have been determined, as well as their functions and roles in the learning system. The set of agent classes includes

- Class of learning data management agents;
- Class of classifier testing agents;
- Class of meta-data forming agents; and
- Class of learning agents, namely, (a) class of *agents* designed for the learning attacks classifiers, whose input data are represented as sequences of events that are temporally ordered, and (b) class of *agents* designed for the learning of classifiers that extract knowledge from learning data represented in the form of attribute vector.

4. Current technical status

The progress in research fully matches the Work program and does not need in a refinement.

5. Cooperation with foreign partners

According to the Work plan, two Interim Reports were submitted to the Partner (to June 1, 2001 and to December 1, 2001). They contain the results of all predefined research.

The Project executors together with the Partner representative participated in the European Summer School on Multi-agent-systems. In March 2001 the project leader attended the Partner institution in the USA in order to discuss the forthcoming research. Partner's representative attended the St. Petersburg Institute for Informatics and Automation in May 2001. In February 2002 the Partner is going to organize a workshop to be held in the USA that aims at discussion of the interim results and further research on the Project

6. Problems encountered and suggestions to remedy

None

7. Perspectives of future developments of the research/technology developed

These perspectives will be discussed in the February meeting in the USA.

Attachment 1: Illustrations attached to the main text

None

Attachment 2: Other Information, supplements to the main text

Brief content of the Interim reports submitted to the Partner

Interim Report #1

Attachment 3: Abstracts of papers and reports published during the year of reference

1. V.Gorodetski, O.Karsaev, A.Khabalov, I.Kotenko, L.Popyack, V.Skormin. Agent-based model of Computer Network Security System: A Case Study. *Proceedings of the International Workshop "Mathematical Methods, Models and Architectures for Computer Network Security. Lecture Notes in Computer Science*, vol. 2052, Springer Verlag, 2001, pp.39-50.

Abstract. The paper considers a multi-agent model of a computer networks security system, which is composed of particular autonomous knowledge-based agents, distributed over the hosts of the computer network to be protected and cooperating to make integrated consistent decisions. The paper is focused on an architecture, implementation and simulation of a case study aiming at exploration distinctions and potential advantages of using such an architecture for the computer network protection. The paper describes the conceptual model and architecture of the particular specialized agents and the system on the whole as well as implementation technology. Simulation scenario, input traffic model and peculiarities of the distributed security system operation are described. The major attention is paid to the intrusion detection task and agents interactions during detection of an attack against the computer network. The advantages of the proposed model of a computer networks security system are discussed.

2. V.Gorodetski, O.Karsaev, I.Kotenko, A.Khabalov. MAS DK: Software Tool for Multi-agent Systems Design and Examples of Applications. *Proceedings of the International Congress "Artificial Intelligence in XX1 Century"* (*ICAI 2001*), Russia, September 3–8, 2001, Physmatgis Publishers, Moscow, Russia, pp. 249-262, 2001 (in Russian).

Abstract. In the paper, the developed technology and respective software tool aiming at design and implementation of multi-agent system are described. This software tool comprises a multitude of reusable components assembled together within a so-called "Generic Agent". The design and implementation of an applied multi-agent system is realized as the process of specialization of the Generic agent classes and data structures according to the project of the system under development. This process is supported by a so-called "Multi-agent System Development Kit". The resulting specification of the system in question is presented in the "System Kernel", which is a specialized collection of databases, reusable classes and specialized library. Also the paper describes three multi-agent applications that have already been or are being currently developed. They are (1) MAS for operation planning; (2) MAS for data mining and knowledge discovery.

3. V.Gorodetski, O.Karsaev, I.Kotenko, A.Khabalov. Software Development Kit for Multi-agent Systems Design and Implementation. International Workshop of Central and Eastern Europe on Multi-agent Systems *(CEEMAS-2001),* Krakow, Poland, September 2001 (The paper will also be published in "*Lecture Notes in Artificial Intelligence*" Springer Verlag series in 2002).

Abstract. The paper presents the developed technology and software tool for design and implementation of knowledge-based multi-agent systems. The software tool comprises two

components that are “*Generic Agent*” and "*Multi-agent System Development Kit*" (MAS DK). The former comprises reusable Visual C++ and Java classes and generic data and knowledge base structures, whereas the latter comprises several developer-friendly editors aimed at formal specification of the applied multi-agent system (MAS) under development and installation of the resulting application in particular computer network environment. The developed technology and MAS DK were used in the design and implementation of the MAS prototype for computer network assurance and intrusion detection and distributed attacks simulator. Several other applications are currently under development.

4. V.Gorodetski, V.Samoilov. Visual synthesis of classification predicates and their use in meta-classification. Transactions of TRTU, #45, 2001, pp. 5-15 (in Russian).

Abstract. The task of mining knowledge from distributed databases is considered. Peculiarity of the task of interest is that it is supposed that data are measured in real-valued scale and data are of high size and dimension. The two procedures as follows are the key components of the proposed approach: (1) Visual mining of separation boundaries which subsequently are automatically represented in analytical terms as rules with premises specified as formulae of the first order logic with linear arithmetic terms. This procedure allows to visually design separation boundaries of wide classes including non-convex and those forming disconnected regions of the data cluster localization; (2) Meta-classification procedure allowing to fuse decisions of classifiers of the lower level is designed with the former procedure. Meta-classification approach is capable to design accurate and computationally efficient classifiers that can be extendible, adaptable and scalable.

Attachment 4: Information on patents and property rights.

Task manager
Ph.D. Prof. V.Gorodetski