MAIN TASKS AND ALGORITHMS OF WIRELESS NETWORK SECURITY SUPPORTING AUTOMATED SYSTEM

Didmanidze Ibraim,*[*] *Beridze Zebur

Batumi Shota Rustaveli State University, Batumi, Georgia

(Received September 14, 2018)

Safety and service quality in wireless networks has recently become an important subject of active research, which is caused by the growing demand for supporting data packages. Without adequate security, organizations avoid using wireless networks. Security issues are an important obstacle for wireless network adaptation. Consequently, security of wireless networks is an important area, which requires reaction, if such networks are widely used. It is necessary for the researchers of this field to identify open problems and to provide relevant solutions to them. Each of such attempts makes the wireless network a bit more secure. The present work aims at the development of a number of measures that would contribute to increasing the safety of wireless networks and through which it would be possible to manage remote workstations.

PACS: 519.713:631.411.6

1. INTRODUCTION

Development of the main objectives of automated system begins with analysis of manual data processing in order to study and generalize the difficulties that a user faces. Such a research is of a general nature and its aim is to identify the difficulties and not to determine their causes. Initially, there is a general examination of existing management procedures, and subsequently, the tasks of management, that are considered to be automated, are analyzed separately.

2. THE TASK

Based on the above objectives, the attention is paid to the following tasks:

- Analysis of different communication channels in wireless networks and development of new methods to enhance security;

- Administration and management of remote work places (local or regional offices) using wireless networks;

- Building and realization of automated system.

The structure of the main tasks of the security system is given in Fig.1.

On the basis of the main tasks of the automated security system, it is necessary to define and develop system algorithms, information security and dialog procedures and create an automated system software complex.

There should be determined the input and output data for each algorithm, created such databases that would help carry out the security processes provided by algorithms (Fig.2.).

The system requires the development of such dialogue procedures, which facilitate the organization of the relationship between a client and the system; it is selected in such a sequence, where such functions, as creating, updating, modifying, applying, reading, processing, exporting, etc. of data, are effectively implemented.

After conducting the above procedures, the automated system software complex and its structure are processed. Classes, constructors, procedures, functions and methods of software complex are created as well.

The efficiency of the solution of security supporting automated system depends on the system algorithmic support. For the optimal solution of this issue, a security task is allocated by separate algorithms for each method.

Each algorithmic block should be considered to perform some kind of automated security function. At the stage of system algorithmization it is necessary to analyze each algorithmic block to make the programming process easier.

The algorithmic blocks also include a set of such programs that run various parts of the computer and allow a user to solve the task in a desired way.

The algorithms are built for each method of security automated system and a separate algorithmic block is described by its functional purposes.

The encryption of the image (password or words consisting of symbols) created by a user, its decoding and the corresponding formation of the database occur according to the algorithm of the combined processing of symbol encryption.

[*] Corresponding author E-mail address: Ibaim.didmanidze@bsu.edu.ge

Let's consider the algorithm of symbol encryption combined method (Figs.3.1-3.6).

The initial stage of the algorithm's work is determined by the information, entered by a user. At the first stage a user's password is written in a special array, where the beginning and the end of a word are defined. Also, the word is separated into symbols and an individual symbol has its own index.

The system introduces additional variables in order to define the indexes of symbols and additional symbols by their quantity. After this, the symbols in a word are split, and the separated symbols obtain their indexes, what results in creating a word, consisting of the combination of symbols, in which the individual symbol is defined by its index.

Each symbol is viewed in ASCII (decimal) encoding and receives its own code. For this purpose we introduce an array, that defines the beginning and the end of symbol codes. Then, a code for the individual symbol is determined and recorded in the array of symbol codes. Eventually, we receive the numbers, consisting of the combination of symbol codes, where the individual symbol is defined by its index code.

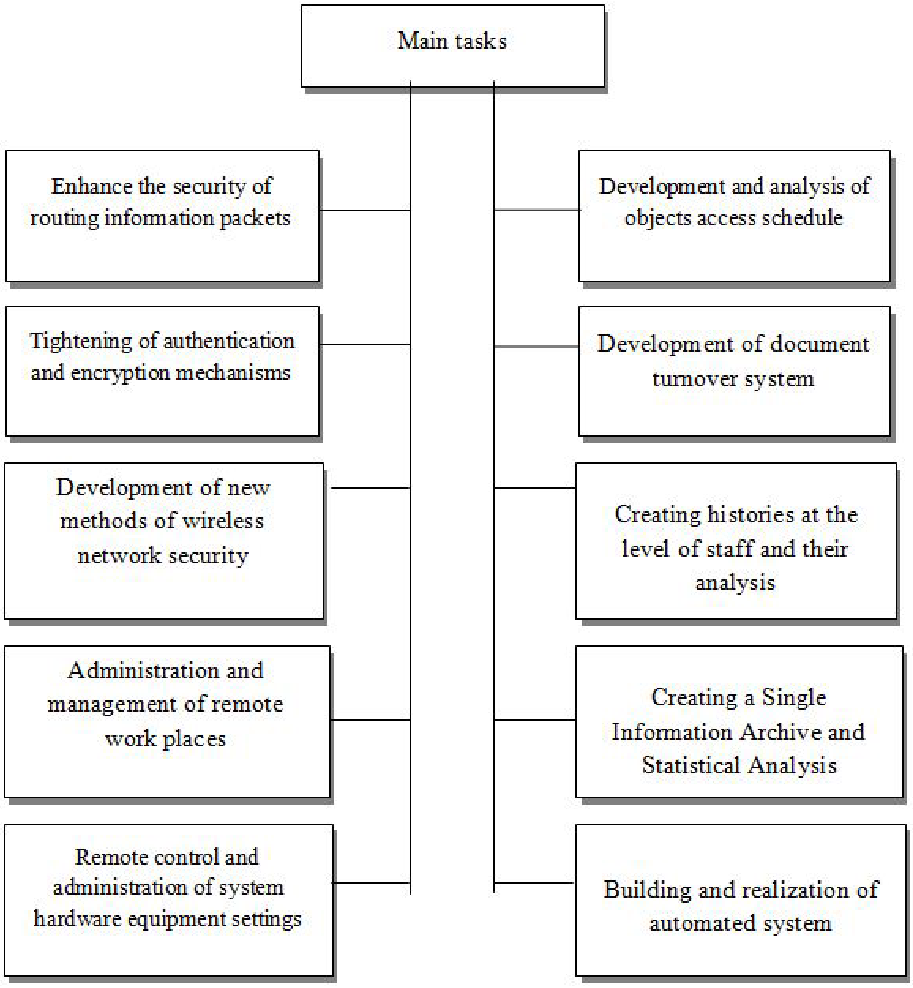
Main tasks
Enhance the security of routing information packets
Tightening of authentication and encryption mechanisms
Development of new methods of wireless network security
Administration and management of remote work places
Remote control and administration of system hardware equipment settings
Development and analysis of objects access schedule
Development of document turnover system
Creating histories at the level of staff and their analysis
Creating a Single Information Archive and Statistical Analysis
Building and realization of automated system

Fig.1. *Main tasks of security system*

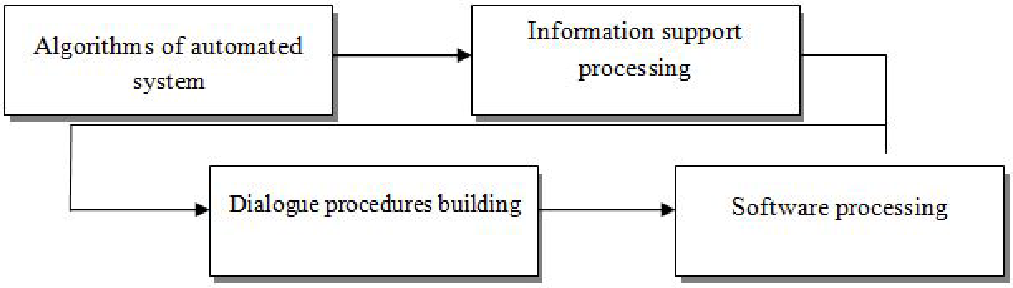
Algorithms of automated system
Information support processing
Dialogue procedures building
Software processing

Fig.2. *Main stages of designing an automated system*

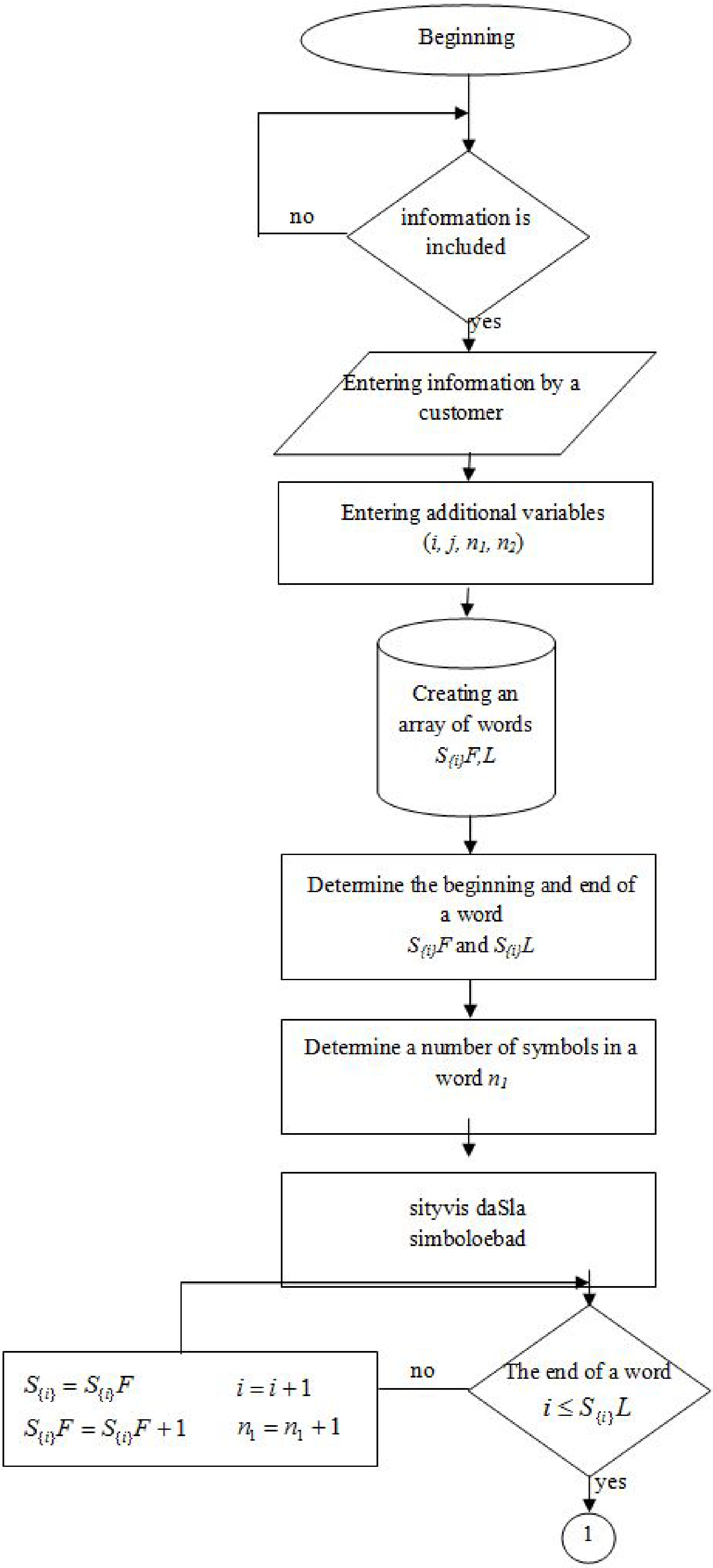
Beginning
no
information is included
yes
Entering information by a customer
Entering additional variables (i, j, n_1, n_2)
Creating an array of words $S_{\{i\}}F,L$
Determine the beginning and end of a word $S_{\{i\}}F$ and $S_{\{i\}}L$
Determine a number of symbols in a word n_1
sityvis daSla simboloebad
$S_{\{i\}} = S_{\{i\}}F$
$i = i + 1$
$S_{\{i\}}F = S_{\{i\}}F + 1$
$n_1 = n_1 + 1$
no
The end of a word $i \le S_{\{i\}}L$
yes
1

Fig.3.1. *Combined method algorithm of symbols encryption*

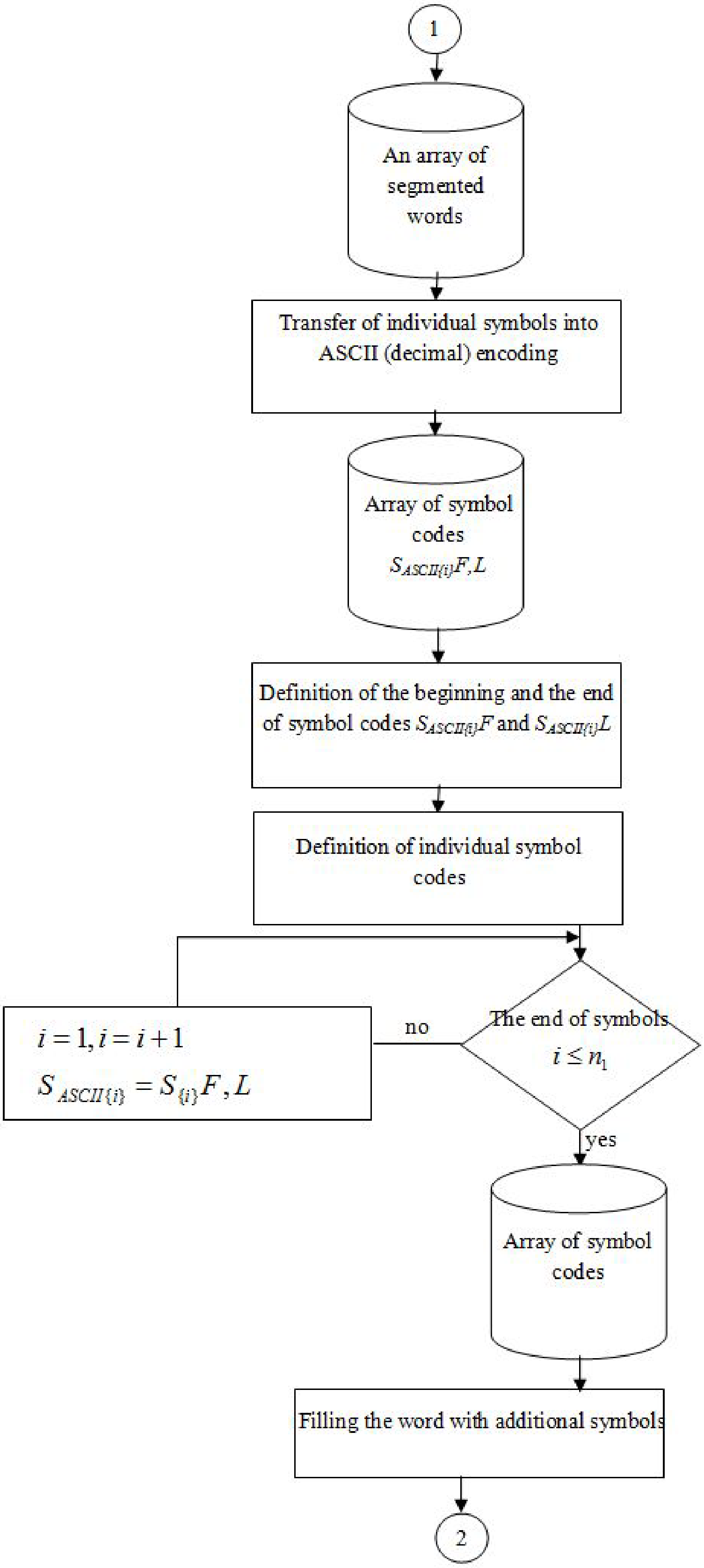
1
An array of segmented words
Transfer of individual symbols into ASCII (decimal) encoding
Array of symbol codes $S_{ASCII\{i\}}F,L$
Definition of the beginning and the end of symbol codes $S_{ASCII\{i\}}F$ and $S_{ASCII\{i\}}L$
Definition of individual symbol codes
$i=1, i=i+1$
$S_{ASCII\{i\}} = S_{\{i\}}F, L$
no
The end of symbols $i \le n_1$
yes
Array of symbol codes
Filling the word with additional symbols
2

Fig.3.2. *Combined method algorithm of symbols encryption*

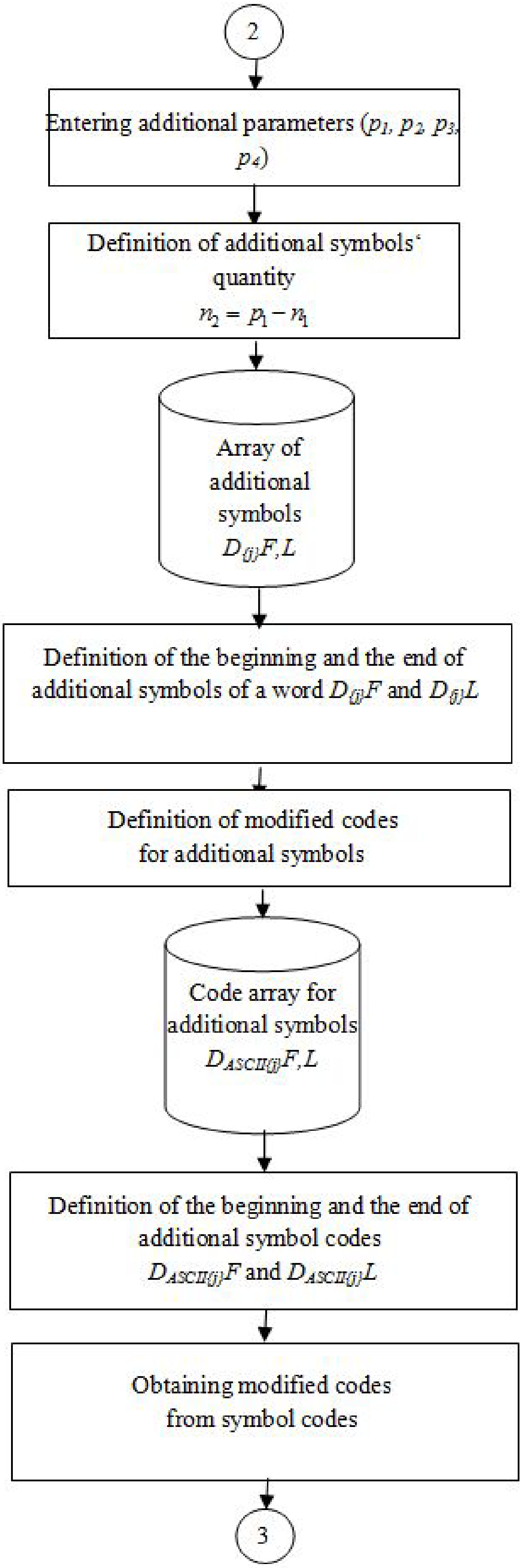
2
Entering additional parameters (p_1, p_2, p_3, p_4)
Definition of additional symbols' quantity
$n_2 = p_1 - n_1$
Array of additional symbols
$D_{(j)}F, L$
Definition of the beginning and the end of additional symbols of a word $D_{(j)}F$ and $D_{(j)}L$
Definition of modified codes for additional symbols
Code array for additional symbols
$D_{ASCII(j)}F, L$
Definition of the beginning and the end of additional symbol codes
$D_{ASCII(j)}F$ and $D_{ASCII(j)}L$
Obtaining modified codes from symbol codes
3

Fig.3.3. *Combined method algorithm of symbols encryption*

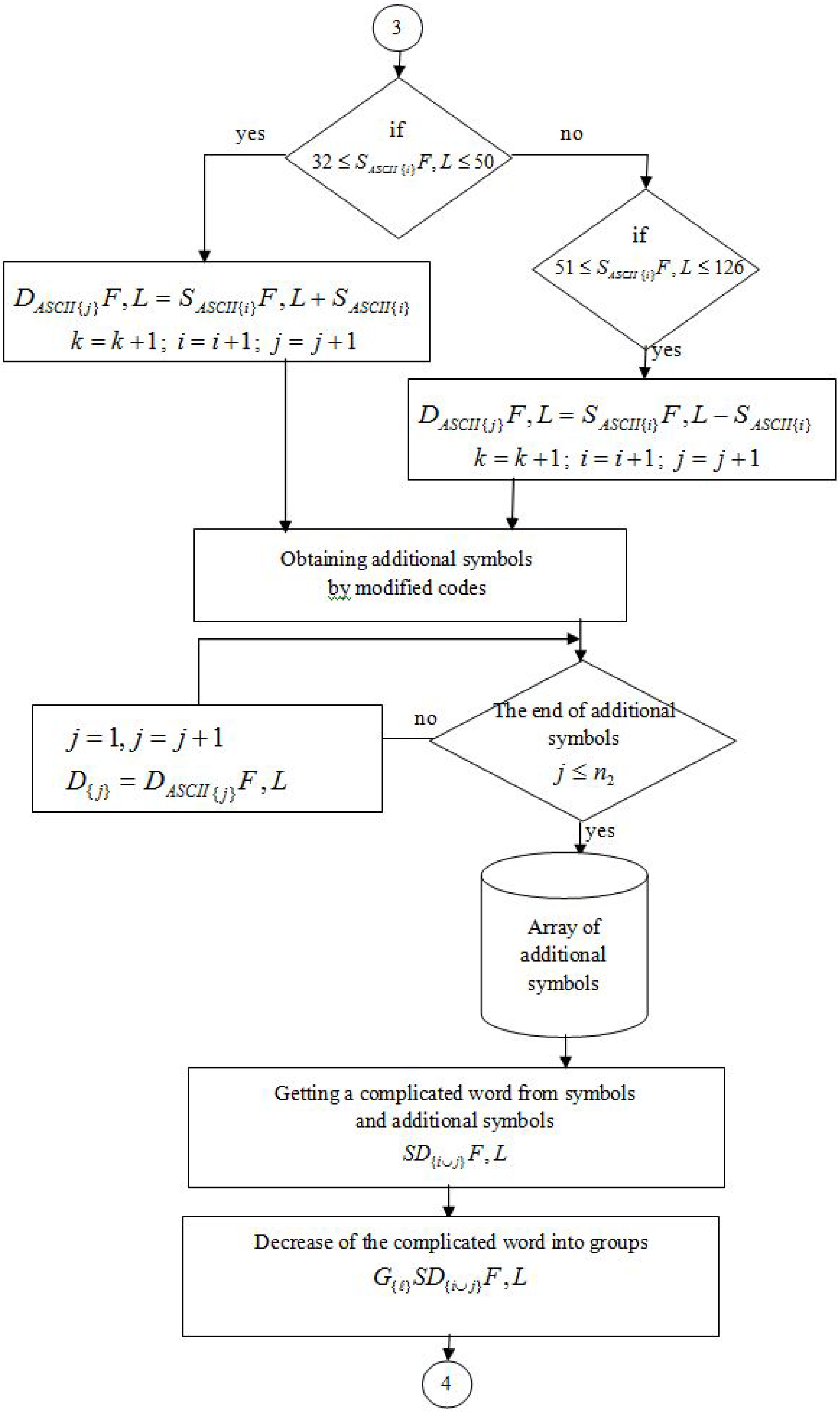
3
if
$32 \le S_{ASCII\{i\}} F, L \le 50$
yes
no
if
$51 \le S_{ASCII\{i\}} F, L \le 126$
$D_{ASCII\{j\}} F, L = S_{ASCII\{i\}} F, L + S_{ASCII\{i\}}$
$k = k+1;\ i = i+1;\ j = j+1$
yes
$D_{ASCII\{j\}} F, L = S_{ASCII\{i\}} F, L - S_{ASCII\{i\}}$
$k = k+1;\ i = i+1;\ j = j+1$
Obtaining additional symbols
by modified codes
$j = 1, j = j+1$
$D_{\{j\}} = D_{ASCII\{j\}} F, L$
no
The end of additional symbols
$j \le n_2$
yes
Array of additional symbols
Getting a complicated word from symbols and additional symbols
$SD_{\{i \cup j\}} F, L$
Decrease of the complicated word into groups
$G_{\{\ell\}} SD_{\{i \cup j\}} F, L$
4

Fig.3.4. *Combined method algorithm of symbols encryption*

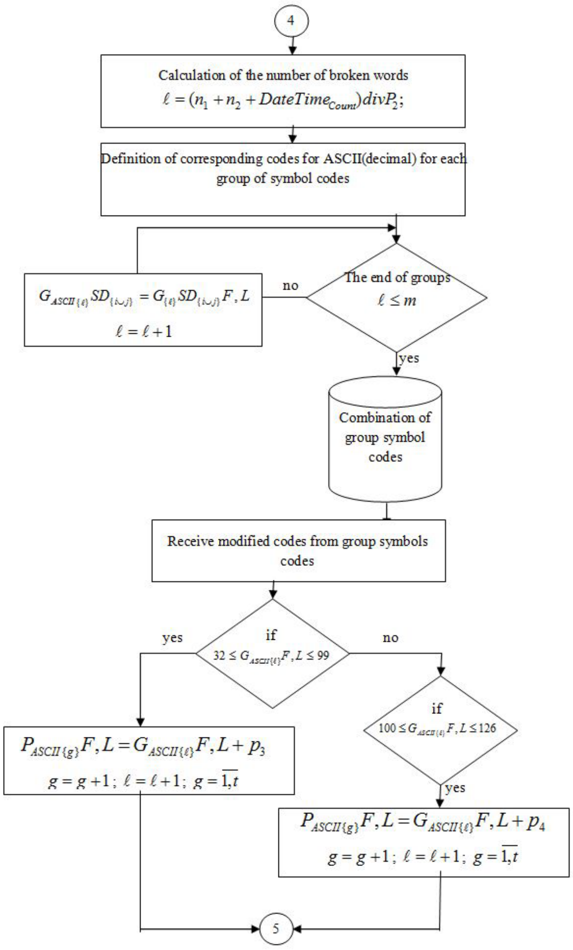
4
Calculation of the number of broken words
$\ell = (n_1 + n_2 + DateTime_{Count}) div P_2$;
Definition of corresponding codes for ASCII(decimal) for each group of symbol codes
The end of groups
$\ell \le m$
no
$G_{ASCII\{\ell\}} SD_{\{i \cup j\}} = G_{\{\ell\}} SD_{\{i \cup j\}} F, L$
$\ell = \ell + 1$
yes
Combination of group symbol codes
Receive modified codes from group symbols codes
if
$32 \le G_{ASCII\{\ell\}} F, L \le 99$
yes
no
$P_{ASCII\{g\}} F, L = G_{ASCII\{\ell\}} F, L + p_3$
$g = g + 1$; $\ell = \ell + 1$; $g = \overline{1,t}$
if
$100 \le G_{ASCII\{\ell\}} F, L \le 126$
yes
$P_{ASCII\{g\}} F, L = G_{ASCII\{\ell\}} F, L + p_4$
$g = g + 1$; $\ell = \ell + 1$; $g = \overline{1,t}$
5

Fig.3.5. *Combined method algorithm of symbols encryption*

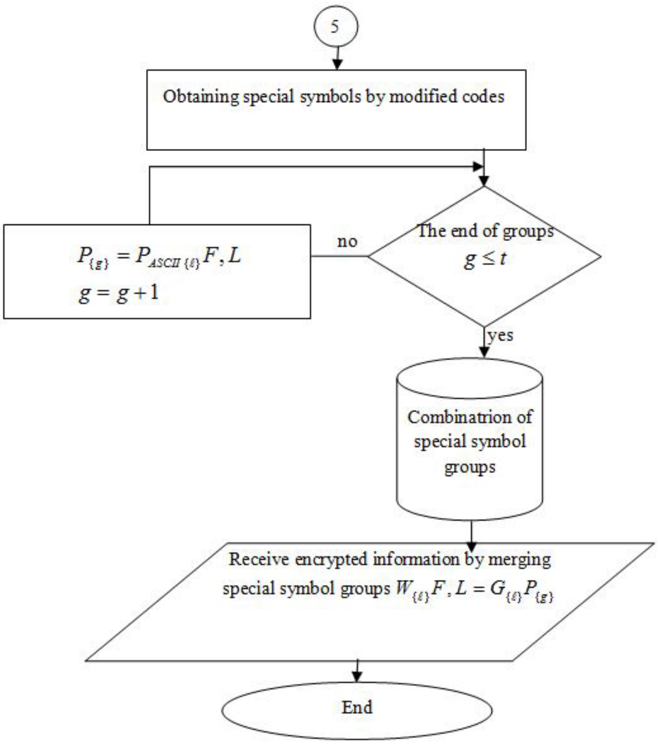
5
Obtaining special symbols by modified codes
The end of groups
$g \le t$
no
$P_{\{g\}} = P_{ASCII\{\ell\}} F, L$
$g = g + 1$
yes
Combinatrion of special symbol groups
Receive encrypted information by merging special symbol groups $W_{\{\ell\}} F, L = G_{\{\ell\}} P_{\{g\}}$
End

Fig.3.6. *Combined method algorithm of symbols encryption*

Next, the word is filled with the additional symbols by setting certain parameters. Then, the number of additional symbols is re-determined and an array is created. It includes additional symbols, which determine the beginning and the end of additional symbols. At the next stage, the modified codes are defined for a specific code of an individual symbol. These codes are written in a special array and determine the beginning and the end of additional symbols.

The purpose of this method is to convert encrypted symbols into special ones by modified codes. The transformation of the symbol codes occurs in the following way:

Initially, the location of the first symbol code is checked. If the code is located from 32 to 50, then the following action is performed: the symbol code is added to its sequence, i.e. an index; then the second symbol code is added to the second index, etc., until the end of the word. If the code is located from 51 to 126, then it is deducted. The newly obtained codes create a group of additional symbols. This process is going on until the value of a certain parameter is satisfied. As a result, we get a word consisting of a combination of additional symbols, in which an individual symbol is defined by its index.

The "complicated" word (password) is created by the combination of obtained symbols and additional ones, that are added by numerical values of a date and a time.

Next, the obtained word gets split (the groups are created) according to the parameters set in the system. Then the encoding of each group symbol ASCII (decimal) results in the determining of their relevant codes. After this we receive numbers consisting of combination of group symbol codes, in which an individual symbol is defined by its index code.

The encrypted information is provided to the central server in the form of groups. If the identification of the first group is successfully completed, the server notifies and issues an order for the release of the second group, etc. until the end of the group. If a group does not match, the server immediately blocks the user. The central server decrypts the encrypted information, using the same parameters as the reverse algorithm of the above mentioned method.

3. SUMMARY

Every network device has its own unique MAC address and, by checking its and IP addresses, a biometutical authentication should be done to determine the identity of the devices before the information is transmitted.

The system algorithms and the informational support have been developed and determined on the basis of main tasks of the security supporting automated system. The input and output data has been set for each algorithm.

ОСНОВНЫЕ ЗАДАЧИ И АЛГОРИТМЫ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ БЕСПРОВОДНОЙ СЕТИ

Дидманидзе Ибраим, Беридзе Зебур

Безопасность и качество обслуживания в беспроводных сетях в последнее время стали важным предметом активных исследований, что вызвано растущим спросом на поддержку пакетов данных. Без адекватной системы безопасности организации избегают использования беспроводных сетей. Проблемы безопасности являются важным препятствием для адаптации беспроводной сети. Следовательно, безопасность беспроводных сетей является важной областью, которая требует реакции, если такие сети широко используются. Исследователям в этой области необходимо выявить открытые проблемы и предложить соответствующие решения для них. Каждая из таких попыток делает беспроводную сеть немного более безопасной. Настоящая работа направлена на разработку ряда мер, которые будут способствовать повышению безопасности беспроводных сетей и с помощью которых можно будет управлять удаленными рабочими станциями.

ОСНОВНІ ЗАВДАННЯ ТА АЛГОРИТМИ АВТОМАТИЗОВАНОЇ СИСТЕМИ БЕЗПЕКИ БЕЗДРОТОВОЇ МЕРЕЖІ

Дідманідзе Ібраїм, Берідзе Зебур

Безпека і якість обслуговування в бездротових мережах останнім часом стали важливим предметом активних досліджень, що викликано зростаючим попитом на підтримку пакетів даних. Без адекватної системи безпеки організації уникають використання бездротових мереж. Проблеми безпеки є важливою перешкодою для адаптації бездротової мережі. Отже, безпека бездротових мереж є важливою областю, яка вимагає реакції, якщо такі мережі широко використовуються. Дослідникам у цій області необхідно виявити відкриті проблеми та запропонувати відповідні рішення для них. Кожна з таких спроб робить бездротову мережу трохи більш безпечною. Ця робота спрямована на розробку ряду заходів, які сприятимуть підвищенню безпеки бездротових мереж і за допомогою яких можна буде управляти віддаленими робочими станціями.