International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

Construction of Schemes, Models and Algorithm for Detection Network Attacks in Computer Networks

GulomovSherzod, AbdullaevDilmurod,MalikovaNodira,AkhmedovaHusniya

Abstract*: This article is devoted to develop network attack detection schemes to search for vulnerable servers and the likelihood of determining the type of attacks by the contents of network packets, a network attack recognition scheme that allows to filter external network traffic by processing incoming requests is proposedas well a network detection model attacks as signs of detecting the position of a security policy is offered. Based on the analysis of time series, a network attack detection model that allows identifying network attacks by a threshold value is developed and a mathematical model for real-time recognition of network attacks is proposed.Model of the behavior of the information flows are shown that the linear model does not provide an adequate assessment of the current process to the critical states. Within the framework of developing models for detecting network attacks, an algorithm for detecting and identifying network attacks is proposed, which allows one to perform not only an exhaustive search for the classification features of network attacks, but to limit itself to a shortened search.The behavior of the queue of half-open compounds are described with an absorbing state, and a system of differential equations for state probabilities are obtained. Also new requests to belong to a particular cluster are analyzed.

Index Terms: traffic amplification, vulnerable, traffic filtering, filtering rules, security policy, fuzzy rules, dynamic systems, SYN packet, SYN cookies, Erlang formula.

I. INTRODUCTION

In the world, special attention is paid to the development and improvement of information protection systems on information and communication systems. At the current level of development of information and communication systems, issues of information protection in computer networks, which is one of the most important mechanisms for ensuring effective information security, are becoming especially relevant.

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author
GulomovSherzod*, Providing Information Security Department, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan
AbdullaevDilmurod, Providing Information Security Department, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan
MalikovaNodira, Information Technology Department, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan
AkhmedovaKhusniyaHardware and Software of Control Systems in Telecommunication Department, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

Of particular importance in the world is the improvement of effective methods and means of information protection, the organization of controlled information applications and the development of models and algorithms for detecting and recognizing network attacks in computer networks.

In this regard, in research works, special attention is paid to the following aspects: development of a mathematical model for recognizing network attacks in real time; improving the methodology and algorithm for detecting network attacks based on the inductive state prediction method; development of software packets for detecting network attacks in computer networks.

II. CONSTRUCTION OF DETECTION AND RECOGNITION SCHEMES OF NETWORK ATTACKS BY EXTERNAL UNAUTHORIZED TRAFFIC

Attack detection and recognition schemes are a set of measures taken to neutralize them and protect the availability of information. Currently, network attack detection and recognition schemes are divided into three main categories: proxy, docking, and software.

1. Proxy attack filtering systems. This solution is implemented at the expense of separate physical servers working as a proxy. The scheme of proxy attack filtering is shown in Figure 1.

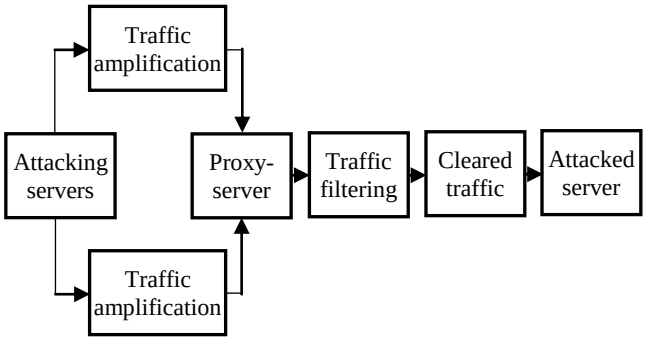

Figure 1-The scheme of proxy attack filtering

2. Docking systems for detecting attacks. This solution is an implementation of a physical network interface:

optical fibers are stretched from the client's servers to the company's data center, which provides protection against network attacks. The scheme of detection of attacks with a physical interface is shown in Figure 2.

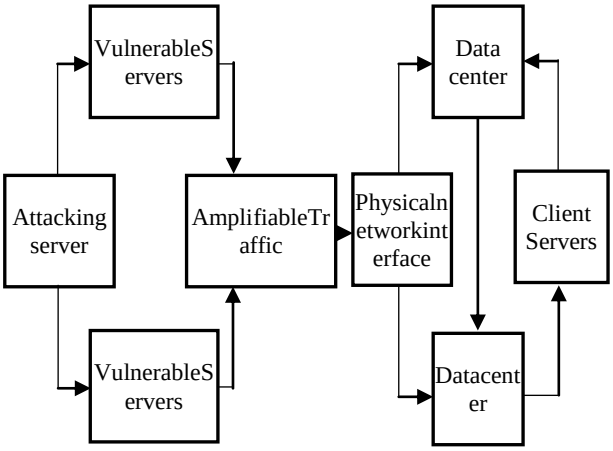

Figure 2 -The scheme of detection of attacks with a physical interface

3. Software systems for detecting attacks. These solutions are standard firewalls implemented by various corporations in operating systems. The operation scheme of standard firewalls is shown in Figure 3.

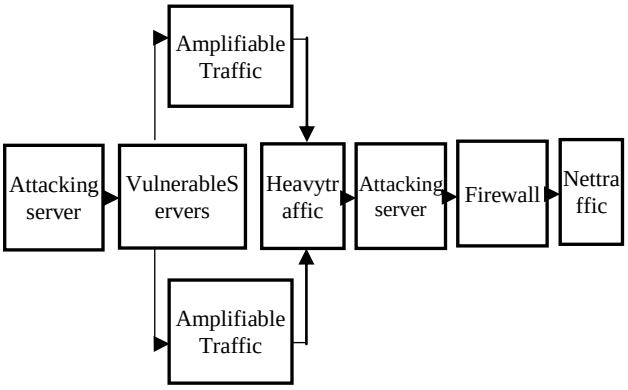

Figure 3 -The operation scheme of standard firewalls

Network Attack Recognition Scheme

The network attack recognition scheme is shown in Figure 4.

An attacker's computer distributes an amplification algorithm to search for vulnerable servers in order to increase the power of network attacks. Next, the cluster head server accepts the attack and distributes it among the physical servers. After starting the algorithm based on Markov chains, network load control and distribution of network traffic filtering rules are implemented [1-2]. After sending data to the kernel of the operating system, the number of incoming network packets is determined, data is received from the system core of each server, and network attack speed is determined.

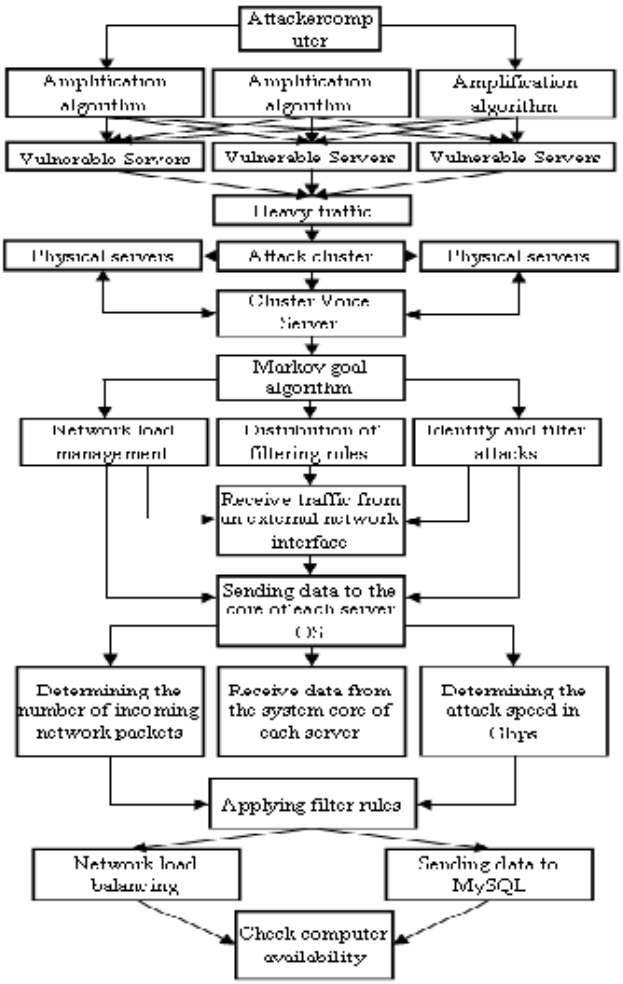

Figure 4 -The network attack recognition scheme

Ultimately, it all comes down to increased protection for the availability of information. An effective solution is to use Markov chains as the basis for recognizing network attacks. Network load management occurs through the processing of incoming applications:

$$\lambda = K * N, K = \frac{\frac{M}{J}}{\sum_{p=0}^{m} \left(\frac{M}{J}\right)^{K}}, \quad (1)$$

where

λ –network load management;

K –number of cores of the attacked server;

N –real time attack probability;

M –total number of cluster cores;

J – current computing load.

This is necessary for uniform distribution of network packets across a physical server / cluster in order to reduce the load on computer systems. The following applies the distribution of filtering rules with a successful probability:

$$P = \frac{N * B}{M * J}, \quad (2)$$

where

P −probability distribution of filtering rules;

N −real time attack probability;

B −probability of successful traffic processing;

M −total number of cluster cores;

J −current computing load.

This is necessary to filter out unauthorized network traffic. The types and types of attacks are also determined by the contents of network packets:

$$P_w = \frac{S_p}{1 - \frac{J_p}{M_K}}, \quad (3)$$

where

P_w −probability of determining the type and type of attacks by the contents of network packets;

S_p −packet content analysis;

J_p −possible types of attacks;

M_K −number of cores in a cluster.

Network attack filtering is performed on all physical servers in the cluster with a uniform load distribution across the cores:

$$= \frac{\sum_{j=0}^{M} K * H + (N * B)}{t_h + t_{min} + t_{av} + t_{max}} \quad (4)$$

where

T −likelihood of successfully filtering network attacks;

K −number of cores of the attacked server;

H −number of physical servers in the cluster;

N −real time attack probability;

B −real time attack probability;

t_h −incoming network packet time;

t_{min} −minimum duration of network attack;

t_{av} −average network attack duration;

t_{max} −maximum network attack duration.

Determining the duration of network attacks is necessary for applying restrictive limits on the processing of external network traffic in the filtering rules [3]. Thus, the proposed scheme for recognizing network attacks allows high-quality filtering of external network traffic.

III. CONSTRUCTION A NETWORK ATTACK DETECTION MODEL BASED ON SECURITY POLICY

Intrusion detection attacks are widely used as one of the most popular means of protecting modern information systems (IS). The increasing sophistication of network attack technology, which is currently observed, requires the discovery of the most dangerous complex attacks, consisting of several stages, during which the attacker carries out malicious actions using various methods. Thus, network attacks should be considered as attempts to violate the security policy (SP) in the protected IS, and to identify them, means are needed that control many different parameters of the IS.

The detection of complex attacks is difficult due to the need to analyze heterogeneous sources of information and search for the relationship between the identified simple attacks. Intrusion detection systems A should have at its disposal a database of signs of detectable ontology attacks. In order to detect network attacks, it is inexpedient to single out common features common to all IS, since in general the attack intensity is different for each IS, since it depends on the characteristics of the system the attack is directed at. In particular, the formation of detection signs should take into account the characteristics of the goals, structure and functioning of the IS. As the basis for the formation of signs of detection of network attacks, IS SP can be used. The SP takes into account the features and characteristics of IS, in particular, describes a model of an internal intruder and internal threats. It also includes information external to IS - a model of external threats, as well as information about the role of IS in the outside world.

The structure of the SP includes private policies that describe the parameters and security criteria for classes of protected IS resources. These policies determine what is an anomaly and normal behavior for various system and network parameters, and contain an assessment of the criticality of deviations from normal behavior scenarios. Thus, the SP can provide the information necessary for the formation of signs of the detection of simple attacks, taking into account the characteristics of IS. However, the SP is a document and almost does not contain quantitative characteristics of various criteria and parameters.

Thus, in the process of achieving the goal, tasks arose of formalizing the signs of detecting network attacks obtained from the provisions of the SP. The possibility of using a combination of fuzzy variables and fuzzy rules to solve this problem is also being investigated.

Let a private security policy indicate that users should not use IS resources after hours. Therefore, the presence of a certain number of users outside working hours should indicate the possibility of penetration into the IS. The simultaneous presence of a large number of active users should signal penetration into the IS and the possibility of an attack propagation stage [4-5]. In turn, the recorded fact of penetration suggests that the risk level for IS is high. In addition, the monitoring policy may indicate the need to analyze the monitoring files at least once every three days. At the same time, a deviation from the monitoring policy with a high possibility of spreading the attack should also indicate that the level of risk for IS is very high. For a formalized description of the above provisions of the SP, it is advisable to write them in the form of the following rules:

R_1:if the users of the system are “few” and the time is “non-working”, then the possibility of penetration is “large”;

R_2: if there are “very many” users of the system, then the penetration possibility is “large” and the spread of the attack is “high”;

R_3:if the time elapsed since the last analysis of the monitoring files is “significant”, then the violation of the monitoring policy is “large”;

R_4:if penetration is “large”, then the risk level is “high”;

R_5:if the spread of the attack is “large” and the violation of the monitoring policy is “large”, then the risk level is “very high”.

In the general case, the premise and conclusion of the rule may consist of an arbitrary nonzero number of atomic formulas connected by various logical operations. A model of the rules that interpret the provisions of the security policy is depicted in Figure 5.

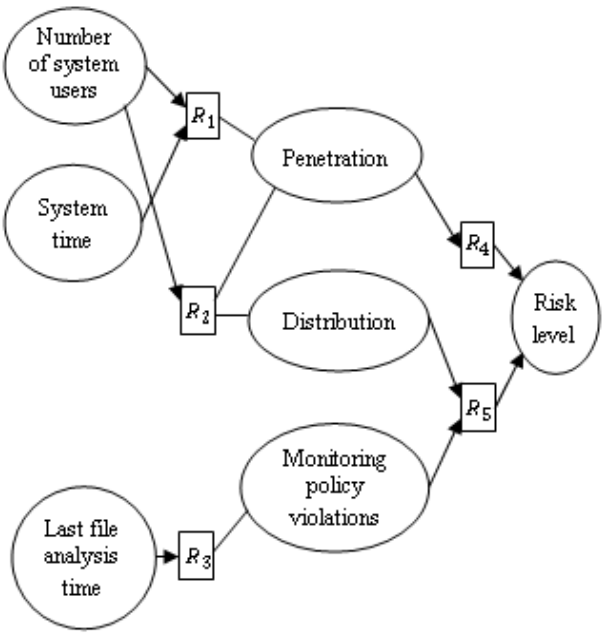

Figure 5 - Model of rules that interpret security policy provisions

To formalize the provisions of the SP, it is proposed to use a fuzzy hierarchical construct. In accordance with the use of fuzzy sets, it is possible to formally define fuzzy and ambiguous concepts, which justifies the use of the apparatus of fuzzy sets and fuzzy logic to formalize the provisions of the IS and to identify deviations from the normal behavior of IP. In the described fragment of the model of rules that interpret the provisions of the SP, linguistic variables are used: "the number of users of the system", "system time", "penetration", "spread", "risk level" and others that take on different values of the form "large", "High", etc. In this case, the input values are the variables "number of users of the system", "system time", "time of the last analysis of monitoring files". The remaining values are obtained by calculations with these fuzzy rules.

Thus, the set of rules obtained by formalizing the provisions of the SP is a hierarchical construct that allows for the detection of network attacks, taking into account the features of IS, expressed in the provisions of its SP. This construct can receive quantitative indicators of IS at the input and, using a qualitative description, evaluate various parameters of IS security, in particular, the current security level of the system described by the linguistic variable "risk level". To describe such a construct and present it in a machine-capable form, we consider the ontology of Intrusion detection attacks as a combination of linguistic variables and fuzzy rules that interpret the provisions of the SP.To form the values of variables in this model, it is proposed to use the method of linguistic terms using statistical data, which allows us to effectively form membership functions of linguistic variables based on statistical data. As statistical data can be used both data obtained from experts, and data obtained by experiment or monitoring the functioning of the components of IS in various conditions and modes.

The ontology of the model for detecting network attacks should contain a linguistic variable "risk level", the value of which is an assessment of the risk of a security event corresponding to the identified attack. When detecting various attacks, other variables can be used that correspond to the stages of complex attacks, for example, "reconnaissance", "penetration", "spread" and others, showing the level of confidence of the system that the attack passes the corresponding stage. The described variables are marked as "interesting" in the ontology. A set of rules and linguistic variables can be represented as a directed graph, its vertices are fuzzy rules, and an arc between two rules exists if there is a linguistic variable that is involved in simultaneously concluding the first and second rule conditions.

In the aggregate of ontology rules, there should not be a cycle of rules, i.e., a sequence of rules of the form $R_1, R_2, \dots, R_n$ such that there is a linguistic variable that occurs simultaneously in the condition of the rule R_{i+1} and in the conclusion of the rule R_i, for $i = 1, \dots, n-1$and $R_1 = R_n$, otherwise the values of some linguistic variables will remain undefined [6]. This condition is equivalent to the fact that in the specified directed graph there should not be contours. In ontologies of the described model, fuzzy rules form not a linear one, as in the classical fuzzy inference algorithm, but a hierarchical structure. It is proposed that the stages of fuzzy implication and fuzzy composition of the fuzzy inference algorithm be carried out not in an arbitrary, but in such a way that the linguistic variables that make up the rule's conditions are already determined either on the basis of fuzzification or on the basis of the rules already used. This order can be achieved if the rules are processed in the order corresponding to the topologically sorted rule column, which will lead to the correct calculation of each subsequent linguistic variable. Since the digraph corresponding to the structure of the rules is a digraph without contours, it allows topological sorting in accordance with the algorithm.

The steps to Intrusion detection attack in the proposed model of Intrusion detection systems are as follows:

1. Processing of used fuzzy ontologies, for each ontology ordering of rules in accordance with the topological sorting algorithm. Specifies the parameters that agents need to collect in accordance with the ontology input parameters.
2. Getting input parameter values. Passing the received parameters to the input of the modified fuzzy logic inference algorithm.
3. Processing the obtained parameters by performing a modified fuzzy inference algorithm.
4. Assessment of the obtained values of "interesting" linguistic variables, assessment of the resulting risk level of the event. In the case when the numerical values of "interesting" linguistic variables exceed a certain threshold value, a decision is made about the possibility of a particular attack.
5. Repeat steps 2, 3, and 4 until an external signal is received.

Thus, the task of formalizing the detection signs obtained from the provisions of the SP is solved by presenting the ontology of the Intrusion detection attacks as a combination of linguistic variables and fuzzy rules suitable for machine processing. The presented model of a network attack detection system is used as signs of detecting the position of a security policy, formalized by means of hierarchical fuzzy systems.

IV. Construction of the Model of Intrusion Detection Attacks Based on Time Series Analysis

The main network protocols generate chaotic structures revealed during the measurement of network traffic, and can be described on the basis of the theory of dynamic systems (DS). For most network protocols used in global computer networks, nonlinear behavior is embedded in their algorithms.Dynamic processes in computer networks can be described by a system of equations:

$$\frac{dx}{dt} = F(x,t) \quad (6)$$

where

x −IS characteristics vector;

t − time.

The difficult moment of modeling is the task of the right part. Determining the form of the function $F(x,t)$ is the main task in the study of DS. As one of the effective methods for obtaining $F(x,t)$, the method of reconstructing the DS from time series, in our case, from network traffic, is used.

Traditionally, the initial stage is a statistical analysis of network traffic. Of the methods of statistical analysis, the main attention is paid to smoothing problems, trends, autocorrelation, spectral analysis, auto regression, etc. Building a smoothing procedure based on the moving average method allows you to evaluate the trend and build a simplified forecast model. However, it must be remembered that this model is linear and cannot be used for critical conditions.

Along with the methods of exponential smoothing, polynomial trend approximation is also used, which allows one to select the deterministic component and estimate the daily and seasonal components [7]. The seasonal component of traffic arises from the cyclical nature of human activity. The cyclic component describes irregular ups and downs with varying frequency and intensity. These methods are limited to specified distribution functions that do not always capture critical traffic.

Description of a network attack detection model based on time series analysis

Changing the process behavior at the level of executable code leads to the execution of instructions that are not provided for by the logic of the task to be solved, which entails changes in the nature of access to IS resources and can be fixed by analyzing the processes that occur in the system interfaces. A study of the operation of IS in the “normal” mode, as well as under the influence of an attack, allows us to state that the distribution of the frequencies of access to different resources on the same time interval is different [8-9]. In this regard, it becomes necessary to describe the functioning of the system on the basis of information flows circulating inside the IS. The data exchange between the IS subsystems can be described using the information model, which will allow to describe the data exchange within a single interface in which the information system S can be represented:

$$S = \langle Struct, Fun \rangle \quad (7)$$

The structural components of IS can be represented as $Struct = (C, F, Z, T)$.

where

C − many subsystems included in$S$;

F − many information flows circulating between IS subsystems;

Z −many events generated by information flows;

T −time / set of time intervals.

Then the execution of a set of Fun functions can be considered as an exchange of information flows between the components of IS. Moreover, each function of the subsystem provides another subsystem with an interface for presenting the results of the function, in which time T is spent on information processing. The information stream itself $(f_i \in F(i = 1, \dots M)$where M is the number of streams) is considered as a one-dimensional data array in the form numerical series $\{f_{ij}\}$given at discrete time instants $t_j(j = 1 \dots N)$ −interval between separate observations, N − is the number of observations). This allows you to get a set of time series characterizing the behavior of the IP in the "normal" state during and after the attack on the IS.

To monitor the operation of the IP, we introduce a vector of state parameters$Param = (c, f, z, t)$

where

c −the number of subsystems involved in the execution of functionsFun;

f −the number of information flows circulating between IS subsystems;

z −number of events generated by information flows;

t −point in time at which measurements are made.

Then, based on the “anomalous” change in the value of the $Param$ vector, one can judge not only the presence or absence of an attack, but also build an ontology that characterizes the type of attack for various operating modes for a given set of characteristics of subsystems. A certain combination of $Param$ values may indicate abnormal behavior, which allows you to make decisions about the choice of the operating mode. Information processes associated with the attack can be described as:

$$A = (K, Param\} \quad (8)$$

where K − type of attacks.

If it confines ourselves to the simplest characteristic of attack detection, it is enough to use the initial data to construct the threshold value of the characteristics of the IS, i.e. use the estimated average values of the studied temporal characteristics of the subsystems recorded for various modes of operation of the investigated process. For example, for each of the types of attacks K recorded by exceeding the threshold value of the time series of the system S, an anomalous traffic vector is generated.

Modeling the behavior of information flows showed that linear models do not provide an adequate assessment of the ongoing process for critical conditions. Based on the information received, it is possible to envisage the use of appropriate countermeasures aimed at combating a specific attack.

V. CONSTRUCTION OF MATHEMATICAL MODELS OF DETECTION NETWORK ATTACKS IN REAL TIME

Under TCP SYN Flooding conditions, the attacked server does not receive any hardware and software damage; after the attack is over, it quickly restores its normal state with a queue of half-open connections. The real damage is that a legitimate user cannot gain access to the attacked server. Thus, it makes sense to consider in detail the reasons for rejecting the SYN packet.

Actually, packet blocking - the SYN packet is blocked by the server due to the queue overflowing with half-open connections. The probability of blocking p_{BLK}increases with the proposed load, decreases with an increase in capacity by the queue of half-open connections and a decrease in the timeout.

Short timeout - SYN packet is removed from the queue of half-open connections if the corresponding SYN ACK packet is not received before the timeout expires [10-11]. In the normal state, with proper server settings, the probability of this event can be neglected. However, if the timeout decreases under attack conditions, almost all remote users will be blocked.

Filter error - there is a non-zero probability that the SYN packet of a legitimate user will be blocked by the filter (error of the first kind, p_F). This may be due to the inefficiency of the recognition algorithm, the rejection strategy, preserving only repeatedly repeated request, etc.

The filter characteristics that affect the listed reasons for the loss of the SYN packet are considered below:

the already mentioned error of the 1st kind can completely cancel the effect of using a filter;

p_Q − the probability of recognizing a fake SYN packet, reducing the likelihoodp_{BLK};

deceleration coefficient, Z −checking the SYN packet for compliance with the rules of legitimacy reduces server performance, reduces the rate of queue release of half-open connections, which also leads to an increasep_{BLK}.

The value of timeout is chosen for reasons that the probability of the event time out in the queue of half-open connections time out" is small in the normal case. Denote the wait timet_w, and the probability of an eventt_w >timeout through$q$.

Then

$$P(t_w > timeout) = 1 - P(t_w, < timeout) = 1 - F(timeout) = \exp(\mu_0 * timeout) = q \quad (9)$$

$$\mu_0 * timeout = \ln q \quad (10)$$

$$timeout = -\frac{\ln q}{\mu_0} \quad (11)$$

It can consider as a characteristic of the filter such a parameter as the delay with the activation of the filter, if the filter was deactivated. But analytical calculations and simulation experiments show its insignificant effect on the effectiveness of protection. As a server model under TCP SYN flooding, it is reasonable to use a Queuing system of the form $M/M/n/n$, where n − is the volume of the queue of half-open connections. The probability of blocking $p_{BLK}$was used as an attack metric. Obviously, when all packets are blocked, $p_{BLK} = 0$and $p_Q = 1$, however, we get an unreasonably high $p_F = 1$, i.e. all legal clients are blocked, the situation is even worse than when the filter is disabled. It was also proposed to consider as a metric the ratio of the number of legal and fake SYN packets recorded in the queue of half-open connections: the higher the value of this parameter, the better the consequences of the attack are transferred. But high values of the mentioned ratio can correspond to high values of p_F. In addition, if a very time-consuming computational procedure is used to verify the packet, it is checked repeatedly over independent channels, guaranteeing

$p_F = 0$, $p_Q = 1$, but significantly slowing down the queue's release of half-open connections, the p_{BLK}value will be unreasonably high. Thus, when simulating TCP SYN flooding, it is necessary to take into account all of the above parameters.Model SYN cookies. If the attacker does not have the ability to intercept and crack cookies, the behavior of a queue of half-open connections can also be described by the process of death and reproduction [12-13]. The corresponding Markov chain has the same states as the Erlang loss model, and another additional state g adjacent to n, which is responsible for generating cookies. In this case, the equilibrium equation for

$$p_g \mu_g = \lambda p_n \quad (12)$$

state$g$has the form

where μ_g −cookie calculation intensity.

The effectiveness of protection is estimated by the formula

$$R = \frac{1}{1 + B(\rho, n)\rho_g}, \rho = \frac{\lambda}{\mu}, \rho_g = \frac{\lambda}{\mu_g} \quad (13)$$

where$B(p, n)$ − B- Erlang formula.

SYN cache model. In the case of using the SYN cache protection mechanism, any incoming SYN packet is not blocked, but can be removed from the semi-open connection queue over time if, before receiving the corresponding ACK packet, n or newer SYN packets arrived. The behavior of a queue of half-open compounds can also be described by a Markov chain with an absorbing state, and a system of differential equations for the probabilities of a state can be obtained. But there is a simpler way. It follows from the initial assumption that the probability of rejecting a legitimate SYN packet is equal to the probability of n or more packets arriving during an exponentially distributed time t, with a mathematical expectation equal to the average time between sending a SYN-ACK packet and receiving an ACK packet $(1/\mu)$. The number of received packets has a Poisson distribution with parameter λ.

From here

$$p_B = \sum_{i=1}^{\infty} \frac{(\lambda t)^i}{i!} e^{-\lambda t} = 1 - e^{-\lambda t} \sum_{n=0}^{n-1} \frac{(\lambda t)^n}{n!} \quad (14)$$

Protection effectiveness indicator:

$$R = 1 - p_B = \sum_{n=0}^{n-1} \frac{\lambda\mu}{n!} \int_0^{\infty} x^n e^{-(\lambda+\mu)x} dx$$

$$= \frac{\mu}{\mu+\lambda} \sum_{n=0}^{n-1} \left(\frac{\lambda}{\lambda+\mu}\right)^n \quad (15)$$

Taking into account the properties of geometric progression, we obtain

$$R = 1 - \left(\frac{\lambda}{\lambda+\mu}\right)^n = 1 - \left(\frac{\rho}{\rho+1}\right)^n \quad (20)$$

Obviously, for the same parameters of the network environment and capacity, the queue of half-open connections, in the conditions of counteracting the SYN flooding attack, is preferable to strengthen the TCP/IP stack than to use the SYN cache mechanism.

VI. FLOWCHARTS OF THE ALGORITHM FOR DETERMINING NETWORK ATTACKS BASED ON THE PROPOSED MODELS FOR DETECTING NETWORK ATTACKS

Figure 6 shows the flowcharts of the algorithm for determining network attacks and the allocation of malicious traffic.

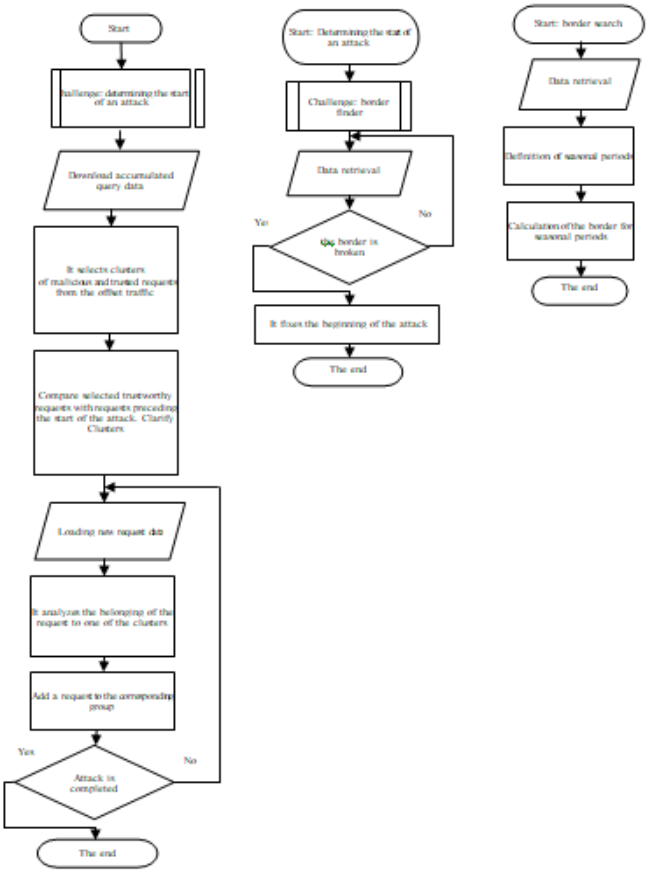

Figure 6 -The flowcharts of the algorithm for determining network attacks

The first flowchart explains the algorithm for allocating malicious traffic; the second and third algorithm for determining the start of an attack. At the first step, subroutines are called to identify seasonal periods, calculate for them the permissible limit of the number of requests, and determine the beginning of the attack.

In the event of an attack, the algorithm splits the mixed traffic into two clusters, one containing malicious requests, the other trustworthy requests. These clusters are being specified. New queries are analyzed for belonging to a particular cluster and, by the result, are added to the corresponding cluster.

VII. CONCLUSION

To sum up, I propose the following outcomes regarding proposal paper:

- A network attack detection model has been developed as an indication of a security policy position, allowing complex attacks to be detected based on these signs.
- Based on the analysis of time series, a network attack detection model has been developed that allows identifying network attacks by a threshold value and determining the classes of attacks used by attacking hosts.
- A mathematical model for recognizing network attacks in real time has beenworked out, which allows calculating the performance of information protection tools designed according to the principle of packet filtering to verify the legality of the packet.
- Based on the proposed models for detecting network attacks, an algorithm has been proposed for detecting and identifying network attacks, which allowto perform not all the enumeration of the possible classification features of network attacks, but limit it to a shortened enumeration.

REFERENCES

1. Borisenko K., Rukavitsyn A., Shorov A., Gurtov A. Detecting the origin of DDOS-attacks in openstack cloud platform using data mining techniques. LNCS. Springer-Verlag GmbH, Heidelberg, 2016, vol. 9870, pp. 303-315.
2. Konovalov A., Korenko I., Shorov A. Simulationbased study of botnets and defense mechanisms against them // J. of Computer and Systems Sciences International. 2013. № 1. C. 45–68.
3. Kotenko I., Konovalov A., Shorov A. Discretevent Simulation of Botnet Protection Mechanisms. Discrete Event Simulations – Development and Applications. Edited by Eldin Wee Chuan Lim. Rijeka, Croatia: InTech, 2012. P. 143–168.
4. Gamer T., Mayer C. Large-scale Evaluation of Distributed Attack Detection // 2nd Intern. Workshop on OMNeT++, Rome, Italy, 2009.
5. Carvalho, L.K., Wu, Y.C., Kwong, R., and Lafortune, S.(2016). Detection and prevention of actuator enablement attacks in supervisory control systems. In Proc. of the 13th Int. Workshop on Discrete Event Systems, 298–305
6. Hoehn, A. and Zhang, P. (2016). Detection of covert attacks and zero dynamics attacks in cyber-physical systems. In Proc. of the 2016 American Control Conference, 302–307.
7. Su, R. (2017). A cyberattack model with bounded sensor reading alterations. In Proc. of the 2017 American Control Conference, 3200–3205. IEEE.
8. Teixeira, A., Shames, I., Sandberg, H., and Johansson, K.H. (2015). A secure control framework for resource-limited adversaries. Automatica, 51, 135–148
9. Ternovoi, O.S., Shatokhin, A.S.: Early Detection of DDoS Attacks by Statistical Methods Taking into Account Seasonality. Mathematical substantiation and theoretical aspects of information security, 1 (25) Volume 1, (2012), PP.104-107
10. Duan Z., Yuan X., Chandrashekar J. Controlling IP Spoofing Through Inter-Domain Packet Filters // IEEE Trans. on Dependable Secur. Computing. 2008. Vol. 5. Is. 1. - P.22–36
11. Chen S., Tang Y., Du W. Stateful DDoS Attacks and Targeted Filtering // Journal of Network and Computer Applications. 2007. Vol. 30. Issue 3. - P.823–840

12. Osanaiye, O., Choo, K.-K.R., Dlodlo, M.: Change-point Cloud DDoS Detection using Packet Inter-arrival Time. In: 8th Computer Science and Electronic Engineering (CEEC), Colchester (2016) pp. 204-209.
13. Alsirhani, A., Sampalli, S., Bodorik, P.: DDoS Attack Detection System: Utilizing Classification Algorithms with Apache Spark. In: 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1-7. Paris (2018)

AUTHORS PROFILE

GulomovSherzod PhD was born in February 26, 1983 in Shakhrisabz city, the Republic of Uzbekistan. In 2009 graduated «Information technology» faculty of Tashkent University of Information Technologies. Has more than 120 published scientific works in the form of articles, journals, theses and tutorials in the field Computer networks and Cyber Security. Currently works of the department «Providing Information Security» at the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi.

AbdullaevDilmurodsenior teacher was born inAugust 21, 1966 in Tashkent city, the Republic of Uzbekistan. Has more than 40 published scientific works in the form of articles, journals, theses and tutorials in the field of Computer networks and Information Security. Currently works of the department «Providing Information Security» at the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi.

MalikovaNodiradeputy dean for Academic Affairs of the faculty "Computer engineering" was bornin May 2, 1974,in Tashkent, the Republic of Uzbekistan. In 2001 graduated "Information Technologies" faculty of Tashkent state technical university. Has more than 28 published scientific works in the form of articles, journals, theses in sphere information systems, Intellectual systems and web technologies. Currently works at the department "Information Technology" of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi.

AkhmedovaKhusniyaassistent teacher was born in May 15, 1986 in Tashkent, the Republic of Uzbekistan. In 2013 graduated "telecommunication technology" faculty of Tashkent University of Information Technologies. Has more than 20 published scientific works in the form of articles, journals, theses in sphere telecommunications. Currently works of the department "Hardware and Software of Control Systems in Telecommunication" at the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi.