How to Cite:
Mohammed, M. H. (2022). Autonomous security assessment model using genetic algorithm in cyber-security domain for healthcare documents. *International Journal of Health Sciences*, *6*(S1), 1073-1087. https://doi.org/10.53730/ijhs.v6nS1.4862

Autonomous Security Assessment Model using Genetic Algorithm in Cyber-Security Domain for Healthcare Documents

Muzammil H Mohammed
Associate Professor Department of Information Technology College of Computers and Information Technology Taif University, Taif, Saudi Arabia

***Abstract*---**In this article, an organization data security appraisal model dependent on abreast hypothesis was considered and advanced. Based on completely considering the data security issues evaluation interaction and components, the degree and mischief of the assault were broke down, and information sources and the particular techniques for incorporating circumstance factors and key hubs were applied to plan the general model, in this way guaranteeing the precision of healthcare documents through cyber-security approaches. The use of hereditary calculation in the dependability investigation of PC correspondence networks is of extraordinary importance. In this paper, the dependability examination and utilization of PC correspondence network dependent on hereditary calculation were considered. The primary substances of hereditary calculation were presented. Simultaneously, the primary substance and exploration techniques for the unwavering quality investigation of PC correspondence network were talked about. Finally, the exploration results were examined and talked about. The outcomes show that the use of hereditary calculation in PC correspondence network dependability investigation is acceptable, which gives a positive evaluation to attain better efficiency of PC correspondence network.

***Keywords*---**Network information, security assessment model, genetic algorithm, security risk assessment.

Introduction

With the ceaseless improvement of data innovation, network security dangers are expanding. In the day by day interaction of utilizing the organization, individuals are confronting the danger of organization security consistently and second [1]. As the current organization security dangers bit by bit show the qualities of scale and disguise, evaluation, discovery and guard method of the customary

International Journal of Health Sciences ISSN 2550-6978 E-ISSN 2550-696X © 2022.
***Corresponding author**: Mohammed, M.H.*
Manuscript submitted: 27 Nov 2021, Manuscript revised: 18 Feb 2022, Accepted for publication: 09 March 2022

organization security can't meet the necessities. Joined with data combination and other new scientific methods, the foundation of a more dependable organization security circumstance evaluation model have turned into an intriguing issue in related fields [2]. In the domestic, with the universal application of the Internet, the traditional Internet technology can't meet people's requirements for network diversification; the Internet with its fast, efficient, service performance advantages occupies an important position in the construction of various industries [3]. However, in the process of using the Internet, there are more and more attacks on the network. Most of the security measures, such as encryption, firewalls, have been unable to adapt to modern borderless network security requirements. Therefore, how to effectively and quantitatively evaluate the security performance of the Internet has become the main task to be solved in the Internet field [4]. Mathematical modeling method for quantitative assessments of Internet security performance can use packet loss rate as a performance index to measure network security performance, the establishment of an Internet security assessment model is the fundamental way to solve these problems, which attracts the attention of many scholars, but also appears a good way.

Related Works

The specific steps of the implementation of information security risk assessment are as follows: building a security framework, carrying out information asset assessment, identifying threats, conducting vulnerability assessment, and establishing correlation of threat and vulnerability [5]. A risk assessment method is utilized to evaluate the information system and determine the size of the risk. Risk Management: appropriate security measures are taken to reduce risk and implement risk management on the system [6]. The main contents and classification of information security risk assessment are shown in Table 1.

Table 1
The main content and classification of information security risk assessment

Classification	Contents	Purpose
Assets assessment	Assets assessment includes two steps of "asset identification" and "value estimation"	Assets are a valuable entity, in the field of network security, assets are computers or systems that take the key task in the enterprise
Threat recognition	Threat assessment is the analysis of the risk that assets may suffer in the system	A threat is an integral part of a risk that can stem from a direct or indirect attack on the system, or accidental or deliberate events, threats generally require the use of vulnerabilities in systems or servers in the network that could cause damage to assets

Vulnerability assessment	Vulnerability assessment is to find flaws in assets through various testing methods, and vulnerability identification and acquisition can be carried out by means of tool scanning, manual analysis and penetration testing	Vulnerability is the weakness in the information assets that may be exploited by attackers and cause damage to the system, including physical environment, institutions, personnel, management, configuration, hardware, software and information
Risk determination	Risk is the direct or indirect damage to the assets caused by loopholes that threaten assets employed	Risk is directly related to asset value, threat and vulnerability

Methodology

Delay Model of Safety Measures

Management decisions are often accompanied by delays in the execution process, that is, there is a delay when decisions affect the system. The result of the delay is that the effect of the decision will not appear immediately, but will appear after the delay time τ[7]. In the fields of economy, biology, engineering and other fields, the delay equation model is widely used to study the delay phenomenon. The delay equation is an equation that describes the relationship between change rate and function value of the unknown function x (t) and the current time t.

In the research model, this paper adopts the most typical delay equation model, that is, the Logistic equation and Hutchinson equation, so as to study the effect of delay of security measures on information security risk. The Hutchinson equation is an extension model of the Logistic equation. It is a nonlinear delay equation involving the reaction-diffusion. It is often used to study the influence of time delay on the stability of numerical methods under the conditions of given initial values and periodic boundary conditions through linear stability of the fixed point.

The application of genetic algorithm is more and more widely. In the application of genetic algorithm, first of all, the parameters of the problem should be set reasonably and initialized. Then the fitness of each item is calculated and the algorithm is used to calculate the individual. Finally, the crossover and mutation operations are performed, and the optimal solution of the output fitness value is obtained [8]. The exploration on unwavering quality investigation and use of PC correspondence network was used for telecom exchanging network. The connectivity of the network is the main measure to check the reliability of computer communication network. In general, a computer with data exchange requires to be connected by a network. Effective communication network connectivity needs to ensure that there is no system error between network nodes. The continuous development of computer science and technology has promoted the popularization of computer communication network [9]. The

reliability analysis of computer communication networks is of great significance in the fields of industry, commerce, banking, transportation and military affairs. The application and problems of computer communication network will change according to the actual situation. The degree of satisfaction of the user to the network application, the proportion of the user's operation, the reliability of the network software and the network transmission will have different influence on the computer communication network. The factors that affect the communication network are closely related to the reliability of computer communication networks [10].

At the same time, the reliability analysis of computer communication network has a direct influence on the optimal design of communication network. The research of computer communication network in our country can be traced back to the 60s of last century. Computer communication network was first used in the field of our country's space and military. In recent years, there are more and more kinds of algorithms for reliability analysis of computer communication networks [11]. At present, the research of computer communication network reliability analysis in our country has been applied in various fields. However, there are more and more constraints on the reliability analysis of computer communication networks. The network topology design of network reliability can promote the research and development of computer communication network to a certain extent.

In summary, with the popularization and application of computer network in our country, it is of great significance to study the application of genetic algorithm in computer communication network reliability analysis. On the basis of the relevant theories at home and abroad, through the method of simulation experiment, the unwavering quality examination and utilization of PC correspondence network dependent on hereditary calculation are studied in this paper. In the second section, the connotation of genetic algorithm is described. In the third section, the main contents of computer communication network reliability analysis are introduced, and the research methods of computer communication network reliability analysis are described. In the fourth section, the data obtained from the simulation experiments are listed and analyzed. Finally, in the fifth section, the conclusions are drawn.

Genetic algorithm

Hereditary calculation started in nineteenth century, and the primary explanation was that the conventional streamlining calculation can't meet the prerequisites of the advancement of industry and farming around then. The first hereditary calculation was primarily utilized in the field of organic recreation [12]. With the advancement of bionics, hereditary calculation is applied to the investigation of versatility of organic reproduction. With the advancement of the application scope, the hereditary calculation is utilized in the field of recreation. The rise of staggered hereditary calculation makes it assume a more significant part in the field of boundary improvement [13]. The hereditary calculation fundamentally incorporates three essential tasks: determination, hybrid and transformation. The measurement change and the ideal stockpiling methodology are the entirety of the techniques for hereditary calculation. Also, there are a ton of cutting edge hereditary activities that have little impact and don't adjust to the overall

guideline in the choice cycle. Developmental hunt of hereditary calculations for the most part doesn't include other outer components. It is essentially founded on wellness work, and the utilization of individual contrasts in the populace to look and ascertain the wellness esteem. In this manner, the choice of wellness work is a significant piece of the hereditary calculation, which impacts the combination speed of hereditary calculation and the control of the ideal arrangement. As a rule, the wellness work is gotten from the change of the goal work. The planning of the target work is predictable with the scale change of the wellness work [14]. The accompanying issues generally emerge while choosing an activity: from one viewpoint, in the essential phase of hereditary advancement, some flighty people are normally delivered. On the off chance that the activity is chosen dependent on the scaling strategy, because of the issue of too solid contest, these eccentric encounters will have some antagonistic impacts on the choice activity, thus the worldwide enhancement execution of the calculation can't be successfully applied. Then again, in the later phases of hereditary advancement, the resulting system of hereditary calculations, the individual distinction of populace isn't noticeable, and its streamlining potential is progressively debilitated, which is exceptionally useful to the nearby ideal arrangement.

As a rule, the hereditary calculation isn't restricted by the space condition, and simultaneously, the viable use of the hereditary calculation doesn't require other helper conditions. The use of hereditary calculation in organic advancement has advanced the improvement of hereditary calculation. As of now, rather than being restricted to a solitary subject and innovation, the use of hereditary calculation has been joined with man-made brainpower, measurements, and software engineering and boundary streamlining, etc. In conventional hypothesis, the issues of hereditary calculation primarily incorporate assembly, search, control and improvement. As a rule, the use of hereditary calculation can be known as the misleading issue of hereditary calculation [15]. Ill-advised plan of wellness capacity might prompt the rise of trickery. In this manner, the plan of wellness work is a significant part of hereditary calculation plan. In the plan cycle of hereditary calculation, the size of the populace isn't enormous; however the thing that matters is extremely huge. Consequently, it is of extraordinary importance to change and compute the quantity of individual multiplication. When an unusual individual shows up in gatherings, that is, the individual wellness is altogether higher than the normal wellness esteem, this individual will possess a flat out driving situation in the populace, when the choice is performed by the wellness esteem, subsequently bringing about untimely assembly of hereditary calculations.

On account of untimely union, the strategy for decreasing the individual wellness ought to be taken on to debilitate the intensity of the non-typical people successfully, in order to forestall untimely combination. Furthermore, in the subsequent course of the inquiry, albeit the gathering is absence of certain expansion, the normal wellness worth of the populace has the chance of arriving at the ideal wellness esteem. For this situation, there is no rivalry locally, thus it is hard to further develop the hunt target, and there is a stop marvel. For this situation, the individual wellness ought to be broadened to work on the seriousness of the person. In the conventional hereditary calculation, the spatial data and other helper data can't be looked, yet the wellness work is utilized to

assess the person. Then, at that point on this premise, hereditary tasks are done [16]. Simultaneously, the wellness capacity of hereditary calculation isn't confined by the persistent condition, which enjoys the benefit of setting the definition area deftly. The solitary limitation on the decision of wellness work is that the info data should have the option to get the yield data with high exactness. This element of hereditary calculation makes its application range significantly extended. The underlying arrangement of the hereditary calculation itself contains an enormous number of unessential data, which ought to be sensibly dispensed with by determination, hybrid and transformation activities. The guideline of this cycle is the equal sifting system. Accordingly, the hereditary calculation additionally has high adaptation to non-critical failure capacity [16].

The rate of increase in the number of attacks is a necessary condition for the successful implementation of the threat, which is determined by the number of loopholes in the assets. As time goes by, the number of successful attacks will gradually approach a fixed value: N. When the initial condition $N(0) = 1$ (that is, only one attack was successfully performed on one asset), the differential equation is obtained.

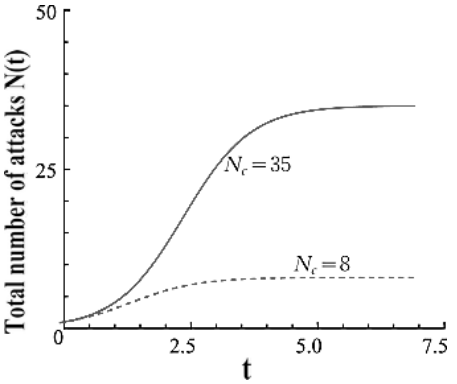

Figure 1. The total number of attacks N (t) with time trend

As shown in Figure. 1, if an information system has 35 assets, in the case of its threat, the increase in the number of attacks with the same type of attack will be shown in the solid line of the graph. If security measures are taken in the network to fix the asset vulnerabilities and thus some of the threats can't be implemented, for example, there are only 8 vulnerable assets, and the increase in the number of attacks with the same type of attack will be shown in the dotted line of the diagram. It can be seen that as long as the safety measures are taken in time, the leak detection hole is processed in time, the logic curve shown by the dotted line will be possible. That is, the number of attacks will be significantly reduced. The delay consists of three stages: (1) incipient stage. The attacker begins to exploit the vulnerability to attack (time interval from 0 to 0.5). (2) Active phase. The attacker gets the confidence to attack at maximum speed (time interval from 0.5 to 6). (3) The saturation phase. The attacker begins to worry about that the attack can be found (time interval from 6 to 7).

Reliability analysis of computer communication network based on genetic algorithm

As a system engineering science, the concept of reliability of computer communication network has been developed for more than half a century, and has formed a relatively complete and sound system. Figure 1 is the application of genetic algorithm in computer communication network. Researchers at home and abroad have summarized the dependability of PC correspondence network into four classes: the availability of the PC correspondence organization, the survivability of the PC correspondence organization, the ruinous tendency of the PC correspondence organization, and the legitimacy of the PC correspondence network in the multi-mode. If the computer communication network works properly, the basic nodes and components in the network must provide reliable connection conditions for each user terminal [17]. Therefore, the connectivity of computer communication network is the most widely studied in the field of reliability. The connectivity of computer communication networks is generally measured by computer communication network reliability. Traditional genetic algorithms for computer communication networks are: firstly, the computer network model is analyzed and simplified through the relevant theory. Then the mathematical algorithm is used to calculate the theory. Finally, the results of genetic algorithm are obtained. Compared with the traditional algorithm, the accuracy of the results of reliability analysis of computer communication networks based on genetic algorithms is higher.

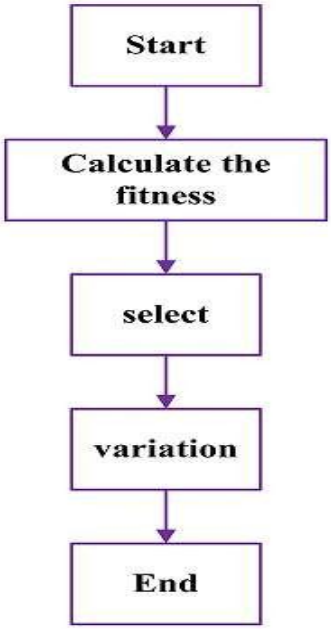

Figure 2. The flow chart of genetic algorithm

The application of genetic algorithm to reliability analysis of computer communication network is a kind of intelligent genetic algorithm. This algorithm is usually used in computer communication networks with more network nodes. The main contents of intelligent genetic algorithm include coding structure,

selection operation and genetic operation, objective function and fitness function and condition selection. The control parameters of the genetic algorithm used in the reliability analysis of computer communication networks mainly include the population size, the selection ratio and the number of iterations. The selection and optimization of these parameters are very important for the reliability analysis of computer communication networks. Reasonable control parameters can improve the accuracy of genetic algorithm. Intelligent genetic algorithm (GA) has a specific operational object, which can largely avoid the inherent limitations of traditional algorithms, so that its application is more and more widely. At the same time, the search method of genetic algorithm is parallel search, which can improve the effectiveness of search behavior to a large extent. In addition, the evaluation method and the objective function of the intelligent genetic algorithm do not need other information and conditions, thus greatly improving the simplicity of algorithm analysis. This algorithm also has non-deterministic rules, which can be used to optimize the structure of genetic algorithm.

Analysis of the factors affecting the reliability of communication network

In the process of reliability analysis of computer communication network, there are three factors of network equipment, network management and network structure. Figure 2 is a comprehensive representation of computer communication networks. The user terminal is a direct user oriented device. Its reliability is very important, and it is also the key to the reliability of computer communication network [18]. The higher the interaction ability of the user terminal, the higher the reliability of the network will be. For example, the installation of two network cards, connected to different LAN segments, is much higher than the reliability of a network card. At the same time, the transmission switching equipment will also have a certain impact on the reliability of computer communication networks. This is mainly because the terminals in the computer network need to realize the transmission of data through the exchange equipment. However, the problems of the data transmission equipment, such as hubs, will lead to the failure of computer network communication. It can be seen that the stability of the transmission and exchange equipment is the basic guarantee of the reliability of the computer communication network.

Figure 3. Schematic diagram of computer communication network

Network management involves the good running of network state and the troubleshooting of network faults. These problems directly affect the reliability of computer communication networks. In order to ensure the integrity of information transmission, reduce the rate of fault, the loss of information, and the error, and improve the reliability of computer communication network, the advanced network management technology should be used, so as to collect the network operation parameters, analyze the network information in real time, monitor the network running status, and find out the faults and eliminate the faults in time [19]. In the planning and design of computer communication network, the reasonable configuration of network management software must be firstly ensured, including the unification of network management software interface and the standardization of network management protocol [20]. Secondly, it is necessary to ensure the real-time monitoring of the whole communication network by the network management personnel, so as to ensure the effectiveness of network management and improve the stability of the communication network. Finally, on the basis of the network management system, the overall quality of network management staff can be improved. In addition, the effective planning of network structure is a congenital factor affecting the reliability of computer communication network [21]. This is mainly because the reasonable design of network structure is closely related to the network scale and application fields. In general, the structure of computer communication network is topological structure. This structure can effectively avoid the constraint of space and time in the communication network through the reasonable parameter setting and the calculation of connectivity.

Result Analysis and Discussion

The results obtained by the method described above are shown in the following tables:

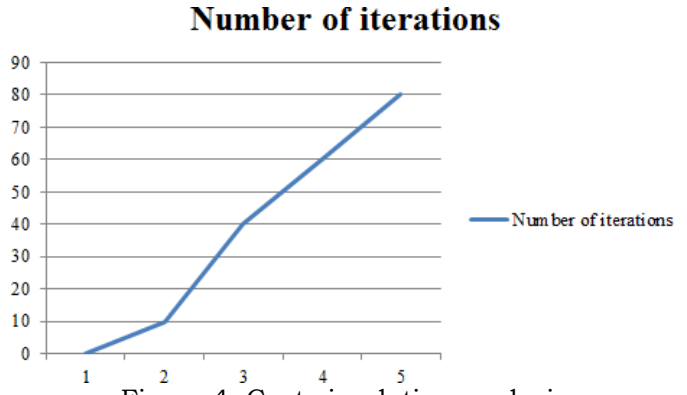

Figure 4. Cost simulation analysis

As can be seen from Figure 3 and Figure 4, the hereditary calculation is utilized to examine the unwavering quality of PC correspondence organization. The information shows that when the quantity of emphasis arrives at 100, the reproduction cycle of PC correspondence network unwavering quality investigation is halted, and simultaneously, the expense of the connection of PC correspondence network is the most minimal. The unwavering quality of PC

correspondence network arrives at the most elevated worth when the recreation interaction is halted and the connection cost is the least. It tends to be seen that the organization cost is adversely corresponded with the unwavering quality of PC correspondence organization, and the quantity of emphasis is decidedly connected with the dependability of PC correspondence organization. As such, the higher the quantity of cycles, the lower the expense of the organization can be taken, and the higher the dependability of PC correspondence organization will be. Subsequently, the utilization of hereditary calculation in PC correspondence network dependability investigation is more practical than the conventional calculation. The outcomes acquired in this paper can be utilized as the fundamental reason for working on the dependability of PC correspondence organizations.

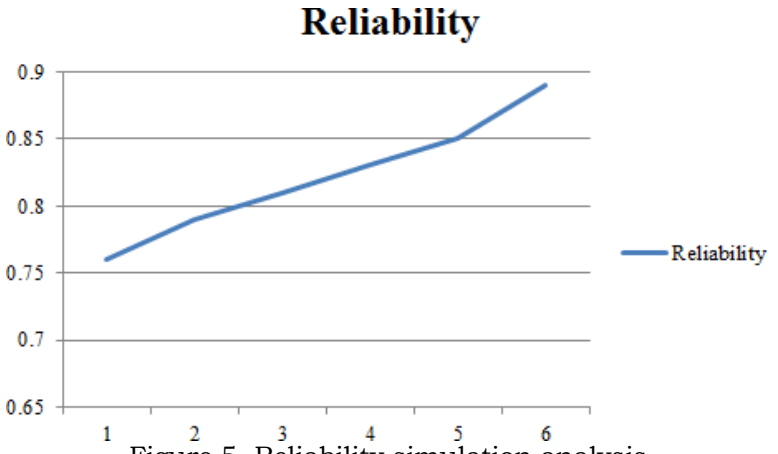

Figure 5. Reliability simulation analysis

Through the simulation experiment of computer communication network reliability analysis, it can be concluded that the application of genetic algorithm in the reliability analysis of computer communication network can get more accurate results, which is beneficial to the improvement of the stability of computer communication network. At the same time, the optimization and improvement of genetic algorithm can improve the accuracy of computer communication network reliability analysis to a great extent. The genetic algorithm optimization design needs to increase the satisfaction of the algorithm analysis. In addition, the optimization and improvement of genetic algorithm can be realized by adjusting the steps and processes of the algorithm. The algorithm steps are as follows: first of all, according to the actual situation of the communication network, the topology of the computer network is redesigned and the network nodes are allocated reasonably. Then, from the perspective of the termination condition, the convergence theory is applied to the iterative number of experiments and the average fitness value is controlled within a reasonable range. Finally, the improved genetic algorithm parameters are input into the simulation software system to carry on the simulation experiment. And the experimental results are obtained. Through the adjustment of the above algorithm, the genetic algorithm can be optimized effectively, so as to provide a more powerful algorithm analysis tool for the reliability analysis of computer communication networks. To sum up, the application of genetic algorithm in

computer communication network reliability analysis is with high feasibility. The optimization design of genetic algorithm is helpful to improve the accuracy of the reliability analysis of computer communication network, which can provide a better basis for the improvement of the stability of computer communication network. Therefore, the optimization of genetic algorithm is of great significance.

It can be seen from the equation that the root cause of the threat is asset loopholes, and the introduction of security measures will lead to changes in asset loopholes. Figure 2 shows the number of vulnerability assets NC=35, when the initial attack number N (0) = 1, the numerical solution in time delay τ = 1.3 and τ = 2 is as follows.

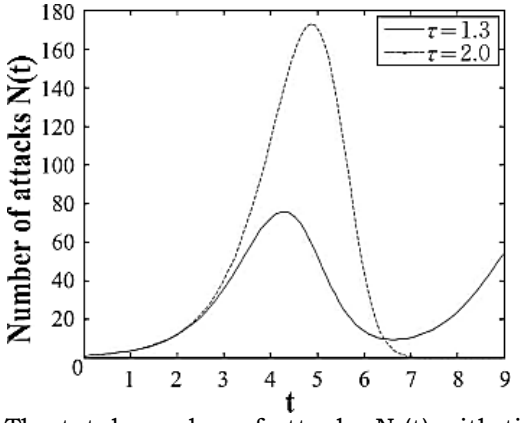

Figure 6. The total number of attacks N (t) with time trend

The scenario of this model is: in an information system consisting of typical assets, a certain amount of assets is threatened. Under a given set of parameters, the solution of Eq. (7) will exhibit periodic oscillatory properties. From the oscillation characteristics of the number of attacks, it can be seen that even if there are only a few attacks, the total number of attacks will increase rapidly without security measures. After a period of time, security measures take effect and the vulnerability is reduced, which will directly lead to a reduction in the threat. The subsequent increase in the number of threats is based on the fact that not all assets in the information system are equipped with security measures or that all security measures are functioning properly; in addition, the same attack may occur repeatedly.

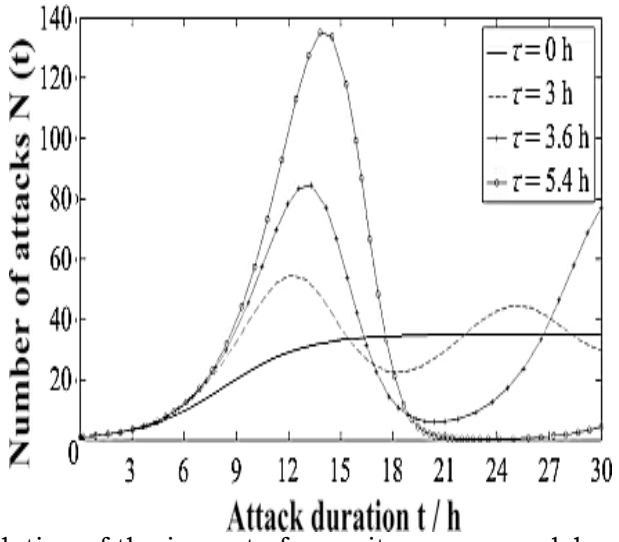

Figure 7. Simulation of the impact of security measures delay on information security risk

Figure 7 shows simulation diagram of the impact of delay in security measures on information security risk. It can be seen from the figure that the emergence of security measures delay τ will result in a significant increase in the number of attacks on the information system, and the more serious the delay in security measures, the higher the increase in the number of attacks, the more obvious the increase in information security risks.

Table 2
Risk scoring criteria table

time delay τ/h	Maximum value of relative risk rr_{max}	Mean value of relative risk rr_C
3.0	1.57	1.08
3.6	2.41	1.25
5.4	3.86	1.97
6.0	1.93	2.39

Table 2. shows the results of simulation experiments, in which rr_{max} is the maximum value of relative risk value, rr_C is the mean value of relative risk value.

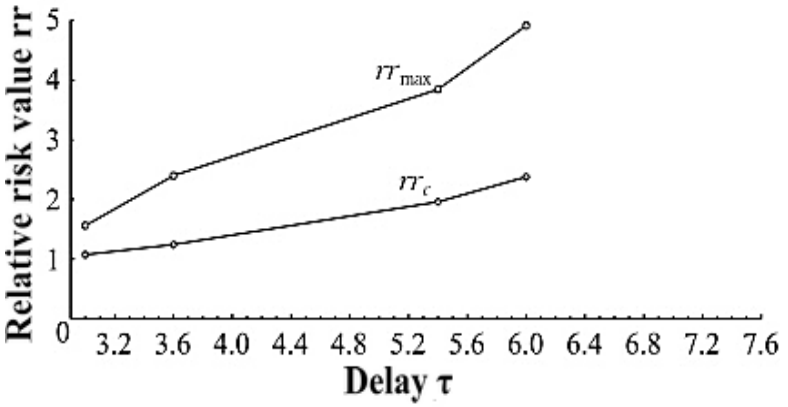

Figure 8. The relationship between the relative risk rr and the delay time τ

Figure 8. shows the results in Table 2, the upper curve is the maximum value rr_{max} of relative risk, and the lower curve is mean value rr_c of relative risk. It can be seen from Figure.4 that the relative risk value after considering the delay is greater than 1, that is, the risk value after considering the delay is greater than the risk value without considering the delay; and with the increase of the time delay τ, the relative risk value also increases. It is also pointed out that in the field of information security, the correct use of Hutchinson equation needs to pay attention to the following problems: (1) the smaller the r value of the vulnerability, the longer it will take for the asset to be attacked. (2) If the attacker threatens the same vulnerability, the delayed timeτ is longer, the negative impact of the enterprise is more serious. (3) The longer the delay time τ, the higher the likelihood of the occurrence of fluctuation (bifurcation), that is, the security personnel who is one of the security mechanisms will not know how to implement the defense, and chaos may occur.

Conclusion

With the popularization of computer and Internet in our country, the subject of computer communication network has gradually become a hot research topic in recent years. Therefore, it is of great significance to study the application of genetic algorithm in the reliability analysis of computer communication networks. In the process of computer communication network reliability analysis, when the number of iterations reaches the maximum value, the simulation process of computer communication network reliability analysis is stopped. At the same time, the cost value of the link of the computer communication network is the lowest. When the simulation process is stopped and the link cost is the lowest, the reliability of the computer communication network reaches the highest value. It can be seen that the network cost is negatively correlated with the reliability of computer communication network, while the number of iterations is positively correlated with the reliability of computer communication networks. Therefore, the higher the number of iterations, the lower the network cost will be taken, and the higher the reliability of computer communication network can be. To sum up, the application of genetic algorithm in computer communication network reliability analysis is good, but there is still some room for improvement.

Therefore, in the future of computer communication network reliability research process, researchers can continue to improve the traditional genetic algorithm from the point of reducing the cost of network link and increasing the number of iterations, so as to improve the accuracy of genetic algorithm analysis and enhance the reliability of computer communication network. With the progress of science and technology and the continuous innovation of information technology, the amount of information on the network is increasing. Therefore, the security of the network faces a severe test. In this paper, a dynamic assessment model for information security risk based on gray system theory was proposed, and the impact of delay in security measures on information security risk was modeled and studied. The model takes into account the threat of assets, asset vulnerabilities, and time delays in taking remedial and security measures. The influence of the delay in security measures on the information security risk was simulated and studied by using the model. The results show that the security measures taken in a timely manner can effectively reduce the risk of information security.

References

[1] Ibrahim Y K. (2013), A Novel Algorithm to Estimate the Reliability of Hybrid Computer Communication Networks. Journal of Signal & Information Processing, 04(4). 394-399.

[2] Yu J. (2013), Computer Network Reliability Optimization Calculation Based on Genetic Algorithm. Telkomnika, 11(3). 603.

[3] Hasan M M, Xiaodong Huang, Jue J P. (2013), Coordinated Dual. Telecommunication Systems, 54(4). 417-431.

[4] Lim W C, Kanagaraj G, Ponnambalam S G. (2016), A hybrid cuckoo search-genetic algorithm for hole-making sequence optimization. Journal of Intelligent Manufacturing, 27(2). 417-429.

[5] Lin Y K, Yeh C T. (2012), Multi-objective optimization for stochastic computer networks using NSGA-II and TOPSIS. European Journal of Operational Research, 218(218). 735-746.

[6] Varasteh A, Goudarzi M. (2015), Server Consolidation Techniques in Virtualized Data Centers: A Survey. IEEE Systems Journal, 1 - 12.

[7] Frincu M E, Genaud S, Gossa J. (2014), On the efficiency of several VM provisioning strategies for workflows with multi-threaded tasks on clouds. Computing, 96(11). 1059-1086.

[8] Biswas D K, Panja S C, Guha S. (2014), Multi Objective Optimization Method by PSO ☆. Procedia Materials Science, 6 1815-1822.

[9] Ying Liu, Shu Mao, Mingwei Zhang, Guoqi Liu, Zhiliang Zhu, and Jingde Cheng. (2015), Prevention of Fault Propagation in Web Service: a Complex Network Approach, Journal of Web Engineering, 14(1-2). 136-150.

[10] Shill P C, Sarker B, Murase K. (2012), Evolutionary Tuning of Fuzzy Rule Base Systems for Nonlinear System Modelling and Control. International Journal of Computer Science & Information Technology, 4(5). 125-143.

[11] Hamed A Y, Al-Naymat G. (2015), A Genetic Algorithm for Constructing Broadcast Trees with Cost and Delay Constraints in Computer Networks. International Journal of Computer Networks & Communications, 7(1). 35-50.

[12] Liu Z, Liu Y, Wang J, et al. (2016), Modeling and simulating traffic congestion propagation in connected vehicles driven by temporal and spatial preference. Wireless Networks, 22(4). 1-11.
[13] Tahayori H, Livi L, Sadeghian A, et al. (2015), Interval Type-2 Fuzzy Set Reconstruction Based on Fuzzy Information-Theoretic Kernels. IEEE Transactions on Fuzzy Systems, 23(4). 1014-1029.
[14] Wan Y, Cao J, He K, et al. (2014), Node Placement Analysis for Overlay Networks in IoT Applications. International Journal of Distributed Sensor Networks, 2014(1). 1-12.
[15] Bhajantri L B, N. N. (2014), Cluster Based Optimization of Routing in Distributed Sensor Networks Using Bayesian Networks with Tabu Search. International Journal of Electronics & Telecommunications, 60(2). 199-208.
[16] Liu S, Dang Y, Fang Z, et al. (2004), Grey system theory and its application. Science, Beijing, 150-195.
[17] Kayacan E, Ulutas B, Kaynak O. (2010), Grey system theory-based models in time series prediction. Expert systems with applications, 37(2). 1784-1789.
[18] Deschrijver G, Kerre E E. (2003), On the relationship between some extensions of fuzzy set theory. Fuzzy sets and systems, 133(2). 227-235.
[19] Behzadian M, Otaghsara S K, Yazdani M, et al. (2012), A state-of the-art survey of TOPSIS applications. Expert Systems with Applications, 39(17). 13051-13069.
[20] Jiwoon Ha, Duck-Ho Bae, Minsoo Ryu, Sang-Wook Kim, Seok-Chul Baek, Byeong-Soo Jeong, and Jinsoo Cho. (2015), Analyzing Topological Characteristics of The Korean Blogosphere, Journal of Web Engineering, 14(1-2). 151-178.
[21] Ghosh S K, Pal T. (2007), Interparticle coupling effect on the surface plasmon resonance of gold nanoparticles: from theory to applications. Chem. Rev, 107(11). 4797-4862.