International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 17 (2015) pp 37571-37577
© Research India Publications. http://www.ripublication.com

Quality Restrain Coding in Network Security Using Optimal Attack Graph Modeling

Gouri R Patil
Research Scholar, MJCET, JNTU university, Hyderabad, gourirpatil@gmail.com, India.

Dr.A.Damodaram
Professor, JNTU University, Hyderabad-Telangana damodarama@jntuh.ac.in, India.

Abstract

Attack graphs describe attack scenarios in distributed network, and play important role in analyzing network threats. These attack graphs are able to reveal such potential threats by evaluating the all possible sequences that an attacker can follow to compromise given critical resources or nodes. An Attack graph specifies an attack scenario that results in compromising network values. There are so many methods proposed to evaluate the network security of an attack graph. But no method was proposed to analyze the quality of service for a given text or audio or video file due to the overhead occurred during evaluation of network security at each and every node. This paper addresses the analysis of the quality of service of a network due to its network security evaluation. Mainly the overhead is occurred at each and every node of the network due to its network security evaluation. This overhead reduces the quality of service of the network. The results shown in the paper gives the complete illustration about the quality of service analysis in attack graphs.

Keywords: Attack graphs, network configuration, network security, network security, quality of service

Introduction

Our society has become increasingly dependant on the proper functioning and reliability of a huge number of interconnected information systems. Major issues in nowadays to secure such systems, it is necessary to measure the amount of security provided by various network configurations. Thus it is important to design automatic tools that can analyze the configuration of an enterprise network and find potential security vulnerabilities and the attack paths. In a network with critical resources, certain vulnerabilities may seem to be insignificant when considered in isolation. An attacker may take advantage of it and exploit sequences of related vulnerabilities.Attack graphscan reveal such potential threats by enumerating all possible sequences of exploits that an attacker can follow to compromise given critical resources. An Attack Pathspecifies an attack scenario that results in compromising organization values. It tells us how an attacker gains access to the victim computer; how and which vulnerability attacker can take advantage of and what kind of damage may be done that can impact the organization. Basically networks are designed to perform various information transfer scenarios. These networks tend to get the maximum amount of quality of a data (text, audio, and video) on reception. The various network modeling scenarios are going to be done by aiming this concept. But the performance of the network is getting degraded when the data passing through the overall nodes in a network is suffered from attacks by various attackers at various instants. Attack graphs are able to specify attack scenarios, play important role in analyzing network threats. This evaluation is becoming an overhead to the network. I.e. analyzing each and every node where there is a possibility to attack and mentioning precautionary measures to overcome it, thus providing security in networks. Because of this there is degradation in the quality of service in the information (text, image, audio, and video) transferred in the network. Because the analysis has to be done at each and ever node causes long time delay. As well as with the increment in the evaluation, overhead is increased which indirectly responsible to degradation of quality of service. Thus if we are expecting to send any data through the network having high overhead it definitely suffers from low quality of service.

Related works

Many previous works on attack graphs [1], [2] have been proposed to evaluate network security based on attack graph models, and some further models and examples on network security metric [3], [4] have been constructed. Firstly, previous works encounter the scalability problem in the generation of the attack graphs, with the size of the attack graphs increasing exponentially with that of the network. Although some researchers try to address this problem [5], their result graphs are still too large and complicated to be analyzed efficiently. Secondly, most of previous attack graphs are designed for a single target, and cannot be used to evaluate overall security of networks with several targets. While managing a typical network including multiple critical resources, network administrators would like Corresponding author. To evaluate those resources as a whole rather than reporting each one separately. Thirdly, it is easy to describe outside attackers' threat, but few suggestions have been described to prevent inside malicious attackers from attacking networks. Finally in [6] a new type of attack graph model to detect an intrusion is proposed called as MP (Multiple-prerequisite) attack graphs. Multiple-prerequisite graph (MP graph) is a type of attack graph that has been developed to help defending large scale enterprise network. In this model two stochastic models are mentioned for quantitative security evaluation. These models are constructed based on the use of Markov Decision Process to model the attacker's behaviors. But the problem associated with this model, it is able to evaluate the network security under static conditions only. I.e. there is no any information about the varying conditions of network structure and network content. To address this problem [7] proposed a new attack graph model considering the volatile parameters. In [7] the nodes in the network are considered as dynamic thus the network configuration is not constant. This caused the evaluation overhead to the network. This problem is solved by considering overhead measurements along with network security evaluation in [8]. In [8] first all n-valid attack paths on a particular node in the graph is evaluated and then the complete overhead occurring due to this evaluation is going to be calculated. This paper gives an analysis for the quality of a service degraded due to the overhead occurred in the dynamic network.

In immune processes, to derive a antigen, antibodies carries out a cycle of clonal selection, crossover and mutation, to reach to the fittest antigens. In synonym to the human immune system, immune algorithm (IA) was developed in recent years. IA has been widely applied in data clustering [9], function optimization [10], and network intrusion detection [11]. In optimization, objective problem is taken as antigen, and the corresponding set of solutions as antibodies. To optimize the performance of Immune algorithm, fast convergence algorithm based on multi-objective is defined in [7]. However developed approaches of multi objective convergence are developed with the focus of security concern. It is however observed that, such approaches define the security concern, but doesnot consider the network operational perform e with respect to delivered service. In the approach of providing better service in such network, this paper focus on the objective to get minimal delay and maximum traffic throughput for given network resource. To achieve the objective of immune system with constraint QoS in network performance, in this paper a modified multi objective immune algorithm (MO-IA) is proposed, with the objective constraint of Service quality in addition to security metric.

Evaluation system model

For the evaluation of the proposing system, an evaluation model is developed, and the interaction between security and QoS is evaluated. The interface of the evaluation model is described as follows: there is one kind of input interfaces, i.e., input interface of network state parameters. In addition, there are also two kinds of output interfaces, i.e., output interface of optimal QoS parameters and output interface of optimal security parameters. These interfaces can be physical or logistic in practical systems. The process of evaluation model includes parameters collecting, parameters evaluating and parameters outputting.

(a) *Parameters collecting*: the current network status such as transmission delay, throughput, call dropping probability and so on, are transmitted to the evaluation model.

b) *Parameters evaluating*: The model consists of two segments: Table unit and Evaluation unit. The Table unit is used to store optimal parameters on security and QoS. The Evaluation unit calculates optimal values according to the input parameters with special algorithms, policies or manual configuration. When the evaluation model receives the parameters of network status, it will firstly look up the table in Table unit to find the corresponding optimal parameters. If the values already exist in the table, they are directly sent to the output interface. Otherwise, the input parameters are sent to the Evaluation unit for calculation. After that, results are sent to output interface for applications and Table unit for storage. With the assistance of Table unit, the optimal parameters can be directly obtained from the Table unit if the same situation occurs again.

c) *Parameters outputting*: the optimal parameters of QoS and security are sent out from the output interface. With the evaluation model, SPs can provide users a series of optimal QoS parameters and optimal security parameters according to current network status. Mostly, the optimal parameters appear as a curve that is composed of various optimal points. Each point represents a vector with elements of security and QoS. According to user's preferences, user can select a suitable point on the curve for a specific service.

Multi objective immune algorithm [7]

To provide the objective of immunity towards network attacks, in [7], a multi objective immune system is presented. In the multi-objective problem, the goal is to seek optimal solutions for several objectives at the same time. In general, it gives rise to a set of optimal solutions, rather than a single solution and one of the solutionscannot be regarded better than others. To achieve the best QoS and the highest SAL (security access level) under certain network delay, it is equal to minimize the delay while maximizing the SAL. When multi-objective immune algorithm is adopted to solve the problems, (*klen*, *ra*) can be considered as antibody, and the antigen is to (T, L). To derive a optimal parameters of SAL the Immune algorithm is as defined in following steps:

*Step 1:*An initial antibodies population *B*with size N is generated, and each antibody (*klen*, *ra*) is created randomly.

Step 2: Based on crowding-distance, the dominant population D from *B*is chosen. If the generation reaches the limit, then output D is selected as optimal solutions. Otherwise, go to Step 3.

Step 3: Based on crowding-distance, get active population A from D, and implement proportional cloning, recombination and hyper mutation on A.

Step 4: Get the new antibody population B by combining the new antibodies in Step 3 and D. Then go to Step 2.

The final dominant population D is the collection of security parameters. However with the concern of providing security the approach of MO-IA is proposed. Wherein other parametric considerations are as well required to provide service compatibility with security to access. With this objective in this paper, a new modified approach to immunity algorithm is proposed based on the additional consideration of service factor to optimize the Multi-objective problem.

Service Oriented Multi Objective Immune Algorithm (SMOIA)

To achieve the objective of higher service compatibility the network throughput factor is considered. The throughput of the network impacts on the delivered service for the network. The throughput of the network is monitored by the traffic delay, wherein the processing overhead is observed at the process of authentication. During the process of authentication, which is initialized at the beginning of a communication.A challenge/response authentication is used because this method is most widely used in computer network.It is a general agreement that the more the times of authentication is, the higher the SAL of authentication is. Of course, for the same authentication, the SAL is determined by which way it adopts. For example, authentication through Media access control (MAC) address has lower SAL than one through credentials with a shared SA (security association) [7]. To simplify simulation and analysis, we use the most common authentication method in our model. In the case, authentication can be measured by the number of authentication in unit time.Here, $r_a$is defined as arrival rate of authentication request to measure times of authentication in one minute. As the authentication rate changes, the SAL of authentication varies accordingly. For simplicity, it is assumed that authentication rate is proportional to the SAL of authentication, and a linear function is adapted to describe the relationship between authentication and its SAL. The value of SAL is just its relative. When the SAL of authentication is not lager than *lm*, it can be carried out as follow:

$$e = l_m/(r_m - r_{min}), \tag{1}$$

$$l_a = (r_a - r_{min}) \times e. \tag{2}$$

Here, $l_a$is the SAL of authentication with the authentication rate r_a, $e$is proportional coefficient of authentication rate. $r_{min}$is the minimum authentication rate used in simulations and $r_m$is the authentication rate corresponding to l_m. When the SAL is higher than l_m, the additional SAL of authentication can be expressed as:

$$e = (L_{max} - l_m)/(r_{max} - r_m) \tag{3}$$

$$\Delta l_a = (r_a - r_m) \times e \tag{4}$$

Here, $r_{max}$is the maximum of authentication rate.

Once the authentication is implemented successfully, the performance of the application is not basically affected by authentication.

Authentication delay is the time duration from sending an authentication request to receiving the reply. It is proportional to the authentication rate in network scenarios [7]. Here, number of packages for authentication is used to measure the impact of authentication on QoS. The authentication delay $T_a$as well as the authentication delay per package $T_a$can be denoted as follows:

$$T_a = c \times r_a + d \tag{5}$$

$$t_a = r_a \times \frac{T_a}{\frac{1}{T}} = r_a \times T_a \times T \tag{6}$$

Here, the parameter *c* is proportional coefficient, *d* and is a constant that is determined by network status. $ra \times Ta$means time of authentication in one unit. That is to say, how many packets for authentication were sent in one unit. At last, the end-to-end delay can be obtained by substituting (6) into (8), which is expressed by:

$$T = (t_{net} + t_k)/(1 - r_a \times T_a) \tag{7}$$

and we can get the corresponding minimal end-to-end delay and maximum SAL by substituting (*klen*, *ra*) into (7). To observe the impact of authentication process over security operation, an analysis to the security process of encryption and decryption is proposed.

System performance analysis

In the process of security coding, data encryption and authentication are two main security mechanisms used generally in various security protocols. By this means, the evaluating model is setup directly from the two mechanisms. Note that data encryption just refer to the encryption of message in this research, while encryption and key exchange for authentication are all regarded as a part of authentication. In this way, security policy consists of initial authentication and data encryption.Generally, encryption algorithm translates the plain text into cryptograph before transmission according to key used in it, so that users without key cannot know the content of session, except for the valid receiver. It can also be used for data integrity. If the cryptographic text is modified, the receiver end cannot decrypt. Although encryption provides information secrecy and integritycheck, it also takes additional time delay and consumes power due to encryption and decryption [10]. On the other hand, authentication is used as an initial process to authorize a user through secret credentials for communication. By rejecting illegal users, authentication can thus control resource access. At the same time, authentication can not only result in additional delay, but also increases call dropping probability that causes degradation in QoS.

It is well known that security services can influence QoS metrics, such as end-to-end delay, call dropping probability and throughput of communication. In this paper, end-to-end delay is approximately taken as QoS because it is the most important among various QoS factors. We defined the end-to-end delay as the time that a packet is sent from one end to the other. If both encryption and authentication are applied, the time delay *T* can be written as:

$$T = t_{net} + t_k + t_a \tag{8}$$

Here, $t_{net}$is the transmission delay, $t_k$is the encryption and decryption time, and $t_a$is the authentication delay per packet. It is noted that although authentication is just implemented in initial stage of session, to describe its effect on end-to-end delay, we averagely add authentication delay to every packet. By this means, packet transmission takes more time due to authentication. In this way, the effect of security on QoS can be reflected by the end-to-end delay.Security service can provide protection for network and data in communication. We define SAL (security assurance level) to measure the strength of security. If a very strong authentication or encryption algorithm is implemented, security policy can provide better protection, and then the SAL is assigned to a high value. Otherwise, the SAL is assigned to a low value. Since security policy contains authentication and encryption, SAL can be divided as SAL of authentication and SAL of encryption.

In practical application, authentication is used as a general way to protect network resources by rejecting unauthorized users. When the protection of authentication is not strong enough, illegal users can pretend a valid user to communicate with sender without checking correctly.In this case, the illegal user is notified as a valid user, so that data secrecy and integrity cannot guarantee. That is to say, only when the protection of authentication is high enough, data encryption can play its role effectively. On the other hand, authentication does not ensure data integrity and confidentiality [7]. Therefore, the protection of authentication is limited, and cannot satisfy requirements of high SAL. It is necessary to adopt both authentication and cryptographic techniques at relative high SAL.

Based on above discussion, authentication is firstly implemented to identify users, and then cryptographic techniques are used to protect data integrity and data confidentiality at relative high SAL. We defined *lm* as the minimal SAL where the encryption algorithm is deployed. The SAL below *lm* is mainly determined by authentication, while the additional SAL above *lm* is obtained from the minimum of SAL between encryption and authentication. This is because both authentication and encryption can influence security level, and weak protection from either side can degrade the SAL performance. By this means, the final SAL *L* can be expressed as:

$$L = \begin{cases} l_a l_a \leq l_m \\ l_m + \min(\Delta l_a, l_k)\, l_a \leq l_m \end{cases} \qquad (9)$$

Where *lk*and*la* are the SAL of encryption and the SAL of authentication respectively, Δ*la* is the additional SAL of authentication that will be described in equation (4), *min(lk,* Δ*la)* is the minimum value between *lk*andΔ*la*.

In this paper, we consider the evaluation model in wireless network from two aspects. One is the limited, shared, unpredictable wireless network resources, leading to QoS to be a more critical issue. The other is the open medium of the wireless network. Both aspects require security to protect data in transmission. It is urgent to optimize the QoS and security in wireless network. Our evaluation model is to provide optimal configurations of security and QoS based on the current network state to facilitate user decision.

Data encryption is one of major methods to protect information. It can not only protect user message in communication from leakage, but also guarantee data integrity. Various encryption algorithms are proposed, such as 3DES, RC6, AES to meet different applications. Since the impacts of encryption algorithms on QoS and security are all related to the key size and computational complexity, we simply adopt AES (Advanced Encryption Standard) as encryption algorithm to verify the effectiveness of evaluation model. AES is proclaimed by National Institute of Standards and Technology (NIST) in 2001 and capable to handle key sizes of 128, 192 and 256 bits. It has been widely adopted by suppliers of both network hardware and software.

a) Effect of Encryption on Security

The SAL of encryption is determined by both its algorithm and key length. Assume that the encryption algorithm has enough safety, which means that there is no better way to decipher the cipher system than exhaustive attack, the consumption of computation for exhaustive attack can be got. If the key length is 8 bits, there are 28 =256 possible keys. It needs to try 256 times in worst situation to get correct key. If $k_{len}$is defined as the adapted key length, it needs to try *2klen* times. Therefore, we can conclude that the longer the key length is, the higher the SAL is. It is assumed that without considering the authentication, the additional SAL of encryption is 1 when the shortest key length is used. Then the SAL of encryption *lk*canbe denoted as:

$$l_k = 2^{k_{len}/k_{min}} - 1 \qquad (10)$$

What' more, the SAL of encryption is also related to its computational complexity, we can define the difference of algorithms by assigned a weight *w*.

$$l_k = (2^{k_{len}/k_{min}} - 1)^* w \qquad (11)$$

For example, if 3DES is applied, *w* is set 0.2 due to weak protection, while AES is 0.5 which means relative strong security. In this way, different encryption algorithm and their SALs can be distinguished. In this paper, we only consider AES to check the effectiveness of our model, so *w* is assigned 1. To facilitate discussion, $L_{max}$is defined as the maximum SAL when the strongest authentication and encryption are applied. To ensure that the final SAL is not larger than L_{max}, the equation (10) should be multiplied by $(L_{max} - l_m)/(2^{k_{len}/k_{min}} - 1)$ By this means, $l_k$changes within the range $[\frac{L_{max}-l_m}{2^{k_{len}/k_{min-1}}}, L_{max} - l_m]$. Here, $k_{max}$is the maximum key length, and $l_k$can be further described as

$$l_k = \frac{\left(2^{k_{len}/k_{min-1}}\right) \times (L_{max} - l_m)}{2^{k_{max}/k_{min-1}}} \qquad (12)$$

b) Effect of Encryption on Delay

When AES is used to encrypt and decrypt the same size of message, the encryption and decryption time bears a linear relationship with the key length [10]. Therefore, the encryption and decryption delay $t_k$can be determined by:

$$t_k = a \times k_{len} + b \qquad (13)$$

Here, *a* is proportional coefficient which indicates rate of the time delay; *b* is a constant. Note that these parameters may be different in different scenarios.

In order to protect network resources, authentication is always used as an initial process to validate users' identity and authorize users for establishing and maintaining creditable communications. In this paper, challenge/response authentication in wireless network is used. The process is as follow: when an AP (access point) receives one authentication request from users, it is implemented with shared SA (security association). Meanwhile, session key is generated to provide protection of data integrity and secrecy. It is noteworthy that the process of later encryption in communication is independent to the authentication, and the purpose is to analyze their effects on QoS respectively. To evaluate the network performance a simulation model is developed, the obtained observations are illustrated in following section.

Simulation observations

To evaluate the characteristic analysis of the developed approach, a comparative analysisof the performance evaluation of proposed method in terms of quality of service is developed. The simulation is performed over a distributed network with eight edge attack graph links. The nodes are set in random order and traffic in burst mode is communicated. Each node is considered as an independent node with the possibility of requesting and reception independently. A packet of 1024bits are exchanged in a burst mode over the network to compute the network overhead affecting the offered services. The obtained observation for the developed system is as outlined below.

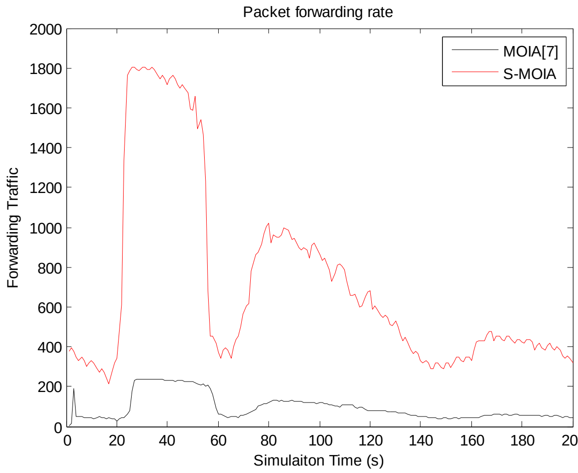

Fig.1. comparison of forwarding traffic between MOIA and S-MOIA

The above figure illustrates the performance of the proposed approach with respect to forwarding traffic. Form the above figure; it was observed that as the simulation time increases the traffic forwarding is varying. For a particular simulation time the amount of traffic forwarding of the proposed S-MOIA is high compared to earlier MOIA, because, in the proposed approach, the overhead occurred due to security evaluation is getting reduced.

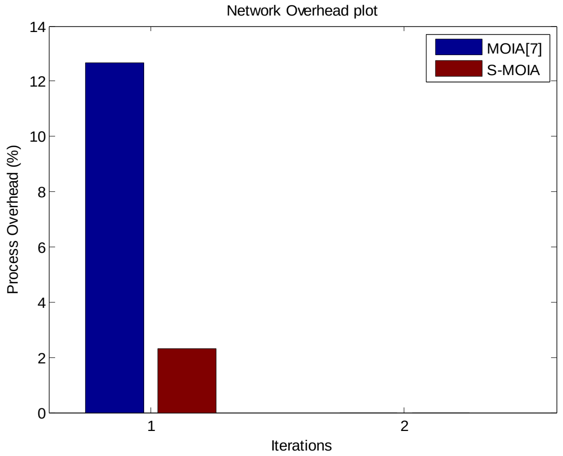

Fig.2. Process overhead

The above illustrates the comparison of process overhead for proposed and previous approaches. The process overhead is mainly due to the security evaluation at each and every node in the network. From the theoretical analysis described above, the proposed approach focused to reduce overhead occurring due to security evaluation, thus the process over head of the proposed S-MOIA should be less compared to MOIA.

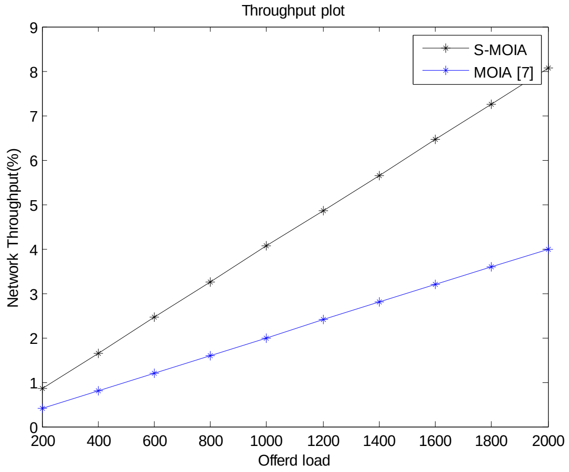

Fig.3. Throughput comparison

As the computational overhead decreases, the data transmission per second can be increased. The above figure illustrates the throughput variation for a varying offered load. Form the above figure it was clear that for a given offered load, the throughput of the proposed approach is high compared to earlier MOIA, because, in the proposed approach the extra computational overhead occurring due to security evaluation is getting decreased. Then the offered entire load can be forwarded through the network intern increases the throughput of the system.

In the next stage, the security access level and network delay were analyzed for both proposed and earlier approaches. The obtained SAL and network delay results are shown in figure.4 and figure.5 respectively.

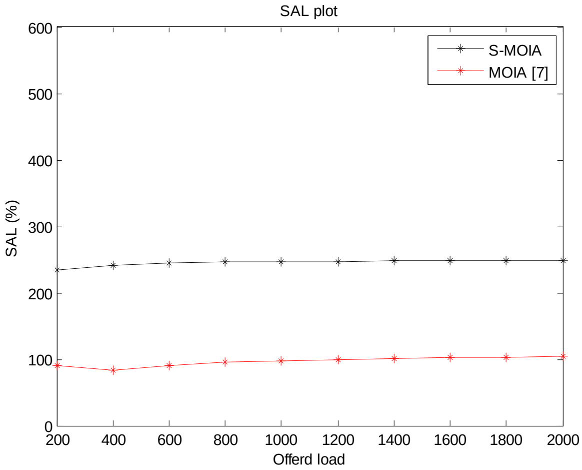

Fig.4. Security Access Level (SAL)

The above figure illustrates the SAL comparison between the proposed S-MOIA and MOIA approaches. From the above figure it was observed that, as the offered load is varying, the SAL of both approaches are almost constant, for a given offered load, the SAL of proposed approach is strictly constant and also high compared to earlier approach.

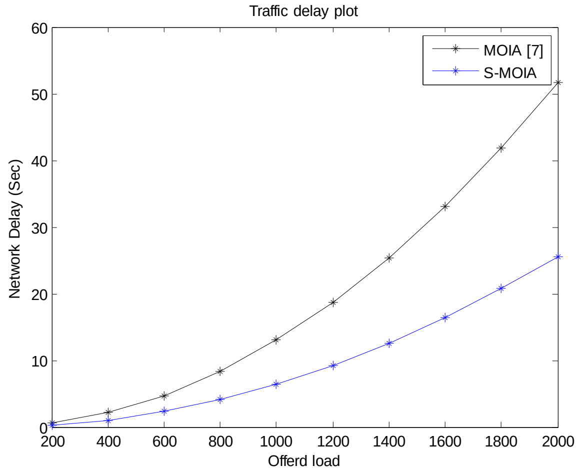

Fig.5. Network delay

In the attack graph, the delay is generally getting increased due to the evaluation of security at each and every node. From the above figure, it is clear that, as the load offered increased, the network delay is also getting increased, when compared to earlier approach, the increment in the network delay of the proposed approach less. Because, the overhead occurred due to the security evaluation for the MOIA is very high compared to S-MOIA.

Conclusion

This paper presents an approach to optimize the attack graph coding for demanded service. The approach developed present an modeling approach to achieve quality metrics of lower traffic overhead and higher network throughput by the allocation of multi objective algorithm. The immune logic is developed to issue or block the acceptance of requested data packet in distributed network. This approach shows a comparative improvement in delivered quality of service in distributed network with the objective of retaining higher quality of service. The simulation results represented in the above section also revealed that the QoS of the network with the proposed S-MOIA algorithm is efficient.

References

[1] K.Ingols, R.Lippmann and K.piwowarski, "Practical attack graph generation for network defense", in proceedings of the 22nd annual computer security Applications conference, December, 2006.

[2] O. Sheyner, J. W. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs, " in IEEE Symposium on Security and Privacy, 2002, pp. 273–284.

[3] L. Wang, A. Singhal, and S. Jajodia, "Toward measuring network security using attack graphs, " in *QoP*, G. Karjoth and K. Stølen, Eds. ACM, 2007, pp. 49–54.

[4] S. Noel, S. Jajodia, B. O'Berry, and M. Jacobs, "Efficient minimum-cost network hardening via exploit dependency graphs, " in ACSAC. IEEE Computer Society, 2003, pp. 86–95.

[5] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graph-based network vulnerability analysis, " in *CCS '02:* Proceedings of the 9th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2002, pp. 217–224.

[6] Yinqian Zhang, Xun Fan, ZhiXue, HaoXu, "Two Stochastic Models for Security Evaluation Based on Attack Graph", the 9th International Conference for Young Computer Scientists.

[7] Maoguo Gong, Licheng Jiao, Haifeng Du, and Liefen Bo, Multi-objective immune algorithm with nondominated neighbor-based selection, Evolutionary Computation (MIT Press), 2008, Vol. 16, No. 2, pp.225-25.

[8] Lei Wu and Lei Peng, A dynamic immune algorithm with immune network for data clustering, ICCCAS on Communications, Circuits and Systems, 2007, pp.919 –923.

[9] Chunhua Li, Yanfei Zhu, and Zongyuan Mao, A novel artificial immune algorithm applied to solve optimization problems, ICARCV on Control, Automation, Robotics and Vision, 2004, Vol 1 , pp.232 - 237.

[10] Ge Hong and Mao Zong-Yuan, Immune algorithm, World Congress on Intelligent Control and Automation, 2002, Vol 3, pp.1784 – 1788.

[11] Zhu Kai, MengXiangru, and Ma Zhiqiang, “Research on intrusion detection technology based on immune algorithm”, International Symposium on Knowledge Acquisition and Modeling, 2008, pp.759 – 762.