Multiobjective Optimal Secure Routing Algorithm Using NSGA-Ⅱ

Dan.Han, Hu Guang-min, Cai Lu
School of Communication and Information Engineering
University of Electronic Science and Technology of China
Chengdu, Sichuan, China

***Abstract*—Integrating security metric into QoS framework is a new strategy in secure routing. Existing QoS framework use only one security metric to describe the link security. Aiming at the deficiency of existing secure routing, we propose a novel strategy which employs multi-security metrics as QoS parameters to achieve more secure route. In our strategy, security metric is combined with other general QoS parameters in differentiated service and then form a multiobjective, multiconstraint secure model. Since the model will be known as a NP complete problem, we introduce nondominated sorting genetic algorithm II to solve the problem. We call the proposed strategy as MOSRA (Multiobjective Optimal Secure Routing Algorithm). Finally, the simulation results demonstrate that the performance of our proposed algorithm.**

***Keywords*—nondominated sorting genetic algorithm-Ⅱ (NSGA-Ⅱ), differentiated service, multiobjective optimization, secure routing**

I. INTRODUCTION

Since the Internet has significantly and rapidly growing, routing attack has becoming popularly, which threaten confidentiality of the data transmission. Researches on secure routing become one of the most important issues in network society. Integrating security metric as a QoS parameter is novel strategy in secure routing research. Sandrine Duflos has suggested that security mechanisms need to be negotiated at that time when sensible multimedia information is exchanged, and the negotiation needs some security services with confidentiality, integrity and authentication [1]. Sandrine Duflos has suggested that integrating security metric into application layer of distributing system will improve Qos management obviously [2]. Stefan Lindskoge has figured out that the big problem of adding security to Qos framework is that security, which has broad meaning, is so difficult to be quantified [3].

The difficulty of integrating security to QoS framework is how security can be quantified. Syed Naqvi has figured out some measurable entities to simplify the security metrics tree with optimal granularity [4]. These entities serve as probes for the evaluation of the overall security assurance of the system. Joseph Pamula has suggested a security metric measures the security strength of a network in terms of the strength of the weakest adversary who can successfully penetrate the network [5]. Abdullah M. S has appointed some random value as the link degree, and defines a path security degree by multiplying those link degrees [6]. All these methods emphasize security particularly only on one policy or objective, which lacks a composition quantification for security metric. A single security strategy can not characterize the network routing security accurately, for there are a lot of issues that contribute to it.

For the unilateral problem that integrating only one kind of security metric into QoS framework, we propose a novel multi-security metric strategy for QoS-based routing. Based on the main target of network security, we used access control, authentication and cryptography [7] to define security metrics, and integrating these security metrics to QoS parameter system. The QoS parameter system is selected for a very diverse mix of applications in IP networks, for QoS itself is taking on a much broader meaning .For example , IP standards have dealt with packet delay and losses, session set up times, session success rates, etc. In this paper, we select some normal QoS parameters, such as time delay, bandwidth utilization ratio, and with security metrics. With all these parameters, the problem becomes a multiobjective routing problem. We use non-dominated sorting genetic algorithm II [8] to solve the NP complete problem. Finally we propose a algorithm named MOSRA (Multiobjective Optimal Secure Routing Algorithm) based on differentiated service model. The simulation results show that the algorithm can provide better security performance, and satisfy other service requirements.

II. MULTIOBJECTIVE SECURE ROUTING MODEL

A. *Multi-security metric definition*

Generally, the need for information security and trust in computer systems is described in terms of three fundamental goals: Confidentiality, integrity and availability (or access).In this paper, we apply three mainly security techniques to define link security metric, that is, router authentication, encryption and access control. These metrics are believed to be good, reasonable and practical [9]. Since authentication is regarded as the first line of defense, cryptography is the key tool that ensures secure transmission of data across a network and access control systems help in guaranteeing the availability of services delivered by the information system. Each metric thus demonstrates the level of achievement in preserving the three goals of security.

A-1 Security metric definition based on Neighbor router authentication

S^1 denotes the first quantifiable security metric we proposed. Here either router authentication on that router is configured or not. When routers need to exchange information

TABLE I. SECURITY METRICS CONFIGURED BY AUTHENTICATION ALGORITHMS

diverse authentication algorithm	Security metric
DES (Data Encryption Standard)	7
SHA (Secure Hash Algorithm)	6
AES (Advanced Encryption Standard)	5
MD5(Message Digest Algorithm 5)	4

between each other, it is configured to authenticate other peer routers. The key can be encrypted in different kinds of authentication algorithm, such as DES、RSA、SHA、AES, MD5. However, when MD5 is used for exchange keys, that link between the routers is considered to be secure. In our network model, we define a link security S_i^1 by the diverse authentication algorithm the peer routers use. The stronger the intensity of algorithm is, the lower security metric values are. The security metric values can be configured, which shows in table1.We suggested this metric be additive composition rule, so a path security metric value can be configured as $S_p^1 = S_1 + S_2 + S_3 + ... + S_n$

A-2 Security metric definition based on Access control

S^2 denotes the second quantifiable security metric we proposed. In actual networks, each node uses intrusion detection/prevention systems (IDS/IPS) or firewalls to enhance the overall level of network security [10]. Either configuration can prevent a subset of the whole set of known attacks. For example firewalls can protect the network from routing based attacks, like source routing and path redirecting. Intrusion detection systems, on the other hand, detect with high accuracy those attacks with known patterns only, like denial of service. The link security metric value of all links leaving that node is given by the equation $S_i = P_{fw}^i + P_{IDS}^i - (P_{fw}^i \times P_{IDS}^i)$, where P_{fw}^i and P_{IDS}^i respectively are the probability that the firewall will prevent and the IDS will detect the attack. We proposed that this metric follows a multiplicative composition rule and the path's security metric value can be calculated via following equation: $S_p^2 = (1 - S_1)\times \quad (1 - S_2)\times(1 - S_3)\times....\times(1 - S_n)$ .Because multiplicative composition rule has some inconvenience, we made a slightly change, $S_p^{'2} = -\log_{10}(S_p^2)$.

A-3 Security metric definition based on Encryption

S^3 denotes the third quantifiable security metric we proposed. Encryption is the technique that mostly used on data communication systems to enhance the security and privacy of information. It is the process of transforming the original message (plain-text) to a scrambled data format (cipher-text) so that authorized people only can have access to the information. A path is considered to be as secure as the weakest link amongst those links allows for forming the path [11]. So it is a bottleneck characteristic and it will follow the concave composition rule. The security metric defined based on the key length used in the encryption/decryption process ,carries a value between zero and one, where zero denotes secure link and vice versa. Precisely, if the data sent over a link is encrypted using a key that is not breakable for the next 30 years, that link is considered as a secure link ,that is, S_i^3 equals 0.0 .On the other hand, if the key used is below the recommended size, the S_i^3 will be 1.0. Between the two extremes the path metric value is given by the following statement.

$$S_p^3 = Max\left[S_1, S_2, S_3 \cdots, S_n\right]$$

$$S_i = \begin{cases} 1, \text{the used key is below the recommended size} \\ 0.99 - 0.033 \times Y, \end{cases}$$

Where Y is the time span in years the key used guarantees acceptable level of data security.

B. The network model and glossary

According to the diverse quantifiable security metric we mentioned before, we proposed to integrate security metric into QoS routing. Based on Russian Dolls Model, we suggested a multiple objectives and multiple constraints optimization model. Russian Dolls Model is one of the Diff-Serv-aware MPLS Traffic Engineering models, in which, services are classified as K class types, and each of them have a bandwidth allocation proportion of $P_1, P_2, ...P_k (\sum P_k = 1)$ .Each allocation of band- width is divided into two parts, that is, the minimum reservable bandwidth n_i and sharing buffer pool m_i . b is a proportion of minimum reservable bandwidth of each service, that is $n_i = P_i * b * C_{ij}$, $m_i = P_i * (1 - b) * C_{ij}$, as shown in Fig.1, where C_{ij} denotes the bandwidth of link (i, j) .For the i^{th} traffic load, the reservable bandwidth n_i is appointed to offer the service; if n_i is not enough, it is consented to make a requisition from sharing buffer pool m_i . Either preemption within a class-type or across class-types is allowed, that is, higher class type traffic can make a requisition for lower class' sharing buffer pool. This strategy can be used in conjunction with preemption to simultaneously achieve isolation across class-types (so that each class-type is guaranteed its share of bandwidth no matter the level of contention by other classes), resulting in bandwidth usage efficiency and protection against QoS degradation.

The network is modeled as topology $G=(V,E,D,C)$, where V is the set of vertexes or nodes and E is the set of directed edges or links in the domain. For any $(i, j) \in E$, D_{ij} denotes the time delay of link (i, j) , C_{ij} denotes the bandwidth of link (i, j) . λ_k denotes the allocation of bandwidth for K^{th} arriving traffic .

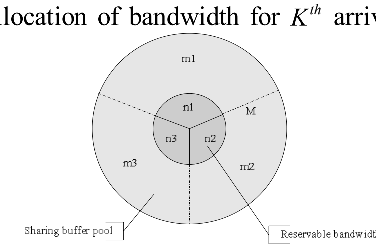

Figure 1. RDM bandwidth allocation model

The network is modeled as topology $G=(V,E,D,C)$, where V is the set of vertexes or nodes and E is the set of directed edges or links in the domain. For any $(i,j)\in E$, D_{ij} denotes the time delay of link (i,j) , C_{ij} denotes the bandwidth of link (i,j) . λ_k denotes the allocation of bandwidth for K^{th} arriving traffic flow. f_{ij}^k denotes the allocation of bandwidth for K^{th} existing traffic on link (i,j) . r_{ij} denotes the existing load on link (i,j) . Therefore, $\alpha = (r_{ij} + \lambda_k) / C_{ij}$ denotes the ratio of the sum of existing load and the allocation of bandwidth for K^{th} arriving traffic flow to bandwidth of link (i,j) , that is, the bandwidth utilization ratio of link (i,j) ; $\lambda_k + f_{ij}^k$ denotes the bandwidth of the K^{th} traffic flow on link (i,j) , both existing and arriving. $P_k * C_{ij}$ denotes the allocation of bandwidth of K^{th} traffic flow . $\beta = \max_{(i,j)\in P_{d_i \to s}} (\lambda_k + f_{ij}^k - P_k * C_{ij})/ C_{ij}$ denotes the max ratio of the K^{th} traffic flow preempted the sharing buffer pool of lower class to the bandwidth of certain link ,that means, a path's ratio for bandwidth preemption of lower class. For different traffic class, each class have a maximum allocation of bandwidth value $\lambda_{k\max}$ (we suppose that there are three class, then $\lambda_{1\max} = P_1 * C_{ij} + (1-b)*(P_2 + P_3)*C_{ij}$, $\lambda_{2\max} = P_2 * C_{ij} + (1-b)*P_3 * C_{ij}$, $\lambda_{3\max} = P_3 * C_{ij}$, the allocation of bandwidth of each class can't exceed this limit).Besides, $(r_{ij} + \lambda_k) \in [0, \min(\lambda_{k\max}, C_{ij} - r_{ij})]$ must be satisfied ,for traffic of lower class can not preempt the sharing buffer pool of higher class [12].

C The multiobjectives optimization model

This paper has proposed an optimal model as below:

$$Min(\sum_{i,j\in P} D_{ij} / P(count)) \tag{1}$$

$$Min(S_1 + S_2 + S_3 + ... + S_n) \tag{2}$$

$$Min[-\log_{10}(1-S_1)\times(1-S_2)\times(1-S_3)\times....\times(1-S_n)] \tag{3}$$

$$Min[\max(S_1, S_2, S_3.....S_n)] \tag{4}$$

$$Min(\max_{i,j\in P_{d_i \to s}} (r_{ij} + \lambda_k) / C_{ij}) \tag{5}$$

$$Min(\max_{(i,j)\in P_{d_i \to s}} (\lambda_k + f_{ij}^k - P_k * C_{ij})/ C_{ij}) \tag{6}$$

$$S_p^1 < S_{p\max}^1 ,\ S_p^{'2} < S_{p\max}^{'2} ,\ S_p^3 < S_{p\max}^3 \tag{7}$$

$$\lambda_k + r_{ij} < C_{ij} \quad (i,j)\in E \tag{8}$$

$P(count)$ denotes the count of a path. Equation (1) means to minimize the average time delay of a path. Equation (2) (3) (4) denotes minimizing of three different security metrics. Equation (5) denotes minimizing the maximum of the bandwidth utilization ratio, which means to minimize a path's bandwidth utilization ratio. Equation (6) denotes minimizing a path's ratio for bandwidth preemption of lower class. Following two equations are some constraints. Equation (7) denotes some threshold of each security metric, which illustrates a route must satisfy some security requirements. Equation (8) illustrates the sum of existing and arriving traffic flow can not exceed the bandwidth of link, and this avoids congestion.

III. ALGORITHM DESIGN

The presence of multi-objectives in a problem, in principle, gives rise to a set of optimal solutions (largely known as Pareto-optimal solutions), instead of a single optimal solution. In the absence of any further information, one of these Pareto-optimal solutions cannot be said to be better than the other. This demands a user to find as many Pareto-optimal solutions as possible. Classical optimization methods (including the multicriterion decision-making methods) suggest converting the multiobjective optimization problem to a single-objective optimization problem by emphasizing one particular Pareto-optimal solution at a time. When such a method is to be used for finding multiple solutions, it has to be applied many times, hopefully finding a different solution at each simulation run. Over the past decade, a number of multiobjective evolutionary algorithms (MOEAs) have been suggested [13], and NSGA-II has been regarded as a fast and elitist strategy. A lot of experiments encourage the application of NSGA-II to more complex and real-world multiobjective optimization problems. In this paper, we proposed MOSRA (Multi-Object Optimal Secure Routing Algorithm) based on NSGA-II, for a purpose of solving multiobjective (security, time delay, ect) QoS routing problem.

A. Coding method

A path from the source to the destination can be coded as a chromosome. As shown in Fig.2, $(S,1,2,5,6,D)$ can be coded as a chromosome. The initial chromosome complex P_0 is a collection of all different paths form source and destination.

B. Genetic operator

Select operator: when initial chromosome complex P_0 forms, we select two chromosomes stochastically, find out which one is dominated to the other one, and give them each a rank. By doing this until all chromosomes in P_0 have a rank, this new chromosome complex is ready for aberrance.

Intercross operator: Intercross operation depicts to exchange the route between two chromosomes which have intersection point, as shown in Fig.3 .This is for preserving diversity among solutions of the same nondominated front.

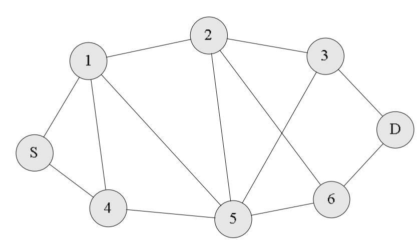

Figure 2. A simple network topology

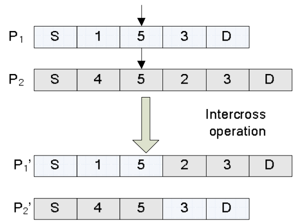

Figure 3. Intercross operation

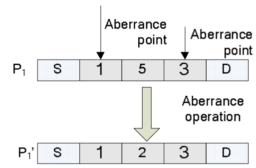

Figure 4. Aberrance operation

Aberrance operator: Aberrance operation depicts to choose a new route between node i and j, as shown in Fig.4, also for preserving diversity and getting multiple nondominated solutions.

Renovation operator: Renovation operation means to eliminate the path loop in a chromosome.

C. Multiobjective Optimal Secure Routing Algorithm

For sake of clarity, we describe our algorithm in five steps:

Step 1. Form initial chromosome complex P_0 with population size N . Then use fast nondominated sorting approach to give a rank for each chromosome.

Step 2. Do select, intercross, aberrance and renovation operation to form a new chromosome complex Q_t (t=0 is the first generation).

Step 3. Combine the old and new chromosome complex R_t , $R_t = P_t \bigcup Q_t$,then apply fast nondominated sorting approach to Rt, find solution with different rank $F_i, i = 1, 2\ldots$

Step 4. Set P_{t+1} as 0, and a count number ***i***=1. When $|P_{t+1}|+|F_i|<N$, do $P_{t+1}=P_{t+1}\bigcup F_i, i=i+1$.

Use a crowding-distance calculation to immediate F_i and give a rank. When the last F_i add to P_{t+1}, we choose ($N-|P_{t+1}|$) solutions. Then turn back to step2 until the generation reaches the limit.

IV. SIMULATION RESULTS

A. Simulation Background

We use the models generated by GT-ITM, the transit-stub networks model [14]. In this model, nodes, which represent routers on the network, are organized into logical domains, or collections of nodes. Nodes within a domain tend to be fairly interconnected within the domain, but rarely connect to nodes outside of the domain.

B. Simulation result

We simulate our algorithm comparing with Widest Shortest Path (WSP) algorithm and Bandwidth-inversion Shortest Path (BSP) algorithm. WSP selects a feasible path with minimum hop count and, if there are multiple paths, choose the one with the largest residual bandwidth. BSP selects a feasible path with minimum hop count, if there are multiple paths, the one with largest bandwidth inversion sum. In following simulation, the arriving traffic flow has highest level, and every link has initial load.

As shows in Fig.5, varying with arriving of traffic flow, the route MOSRA selected has a lower average time delay in

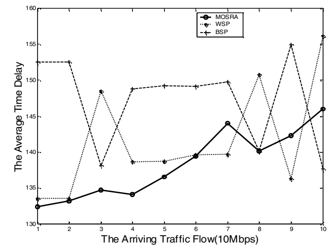

Figure 5. The comparison of average time delay

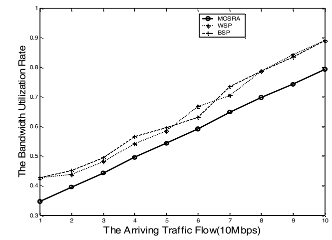

Figure 6. The comparison of bandwidth utilization ratio

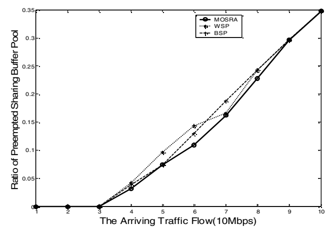

Figure 7. The comparison of ratio of preempted the sharing buffer pool

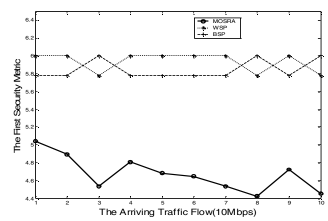

Figure 8. The comparison of First security metric

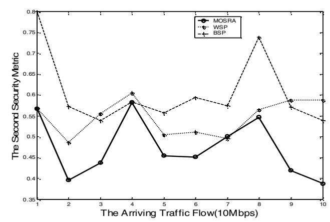

Figure 9. The comparison of Second security metric

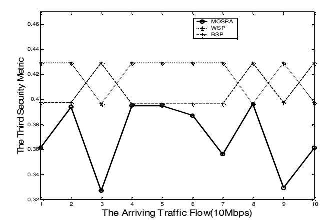

Figure 10. The comparison of Third security metric

contrast to the route selected by WSP 、BSP most of the time. Abnormity occurs because adding security to quality of service increases the resource consumption and the time of exchange. In Fig.6, it shows as traffic flow grows, the bandwidth utilization ratio of the route selected by three algorithms all grows, but MOSRA has a lower value. This illustrates that MOSRA perform better in Network Load Balancing. In Fig.7, when the traffic of higher class arrives, the route selected by MOSRA has a lower ratio value of preempted the sharing buffer pool of lower class, this illustrates MOSRA use the network resource much more fairly. Fig.8, 9, 10 show that, for different security metric, the route selected by MOSRA have lower value, and this demonstrate our algorithm choose more secure route. In conclusion, under multiobjective and multiconstraint circumstance, our algorithm get a better balance of network load, and have less congestion. Furthermore, it has much better security performance.

V. CONCULSION

Secure routing is a challenge topic, and integrating security metric as a QoS parameter is novel strategy in research of present network secure routing. For the unilateral problem that integrating only one kind of security metric into QoS framework, we propose a novel multi-security metric strategy for QoS-based routing. With other normal QoS parameters, we form a multiobjective, multiconstraint model; we also propose a algorithm named MOSRA(Multiobjective Optimal Secure Routing Algorithm)based on nondominated sorting genetic algorithm II .The simulation shows that the algorithm can provide better security performance, satisfy different class service requirements, give a better bandwidth utilization, and reduce the network congestion.

REFERENCES

[1] Sandrine Duflos, Valerie Gay, Brigitte Kervella, Eric Horlait.Integration of Security Parameters in the Service Level Specification to Improve QoS Management of Secure Distributed Multimedia Services[C]. Proceedings of the 19th International Conference on Advanced Information Networking and Applications, Mar. 2005, Vol. 2 : 145 – 148

[2] Sakarindr, P. Ansari, N. Rojas-Cessa, R. Papavassiliou.S. Security-enhanced quality of service (SQoS): a network analysis[C]. Military Communications Conference, 17-20 Oct. 2005. Vol. 4:2165- 2171.

[3] Stefan Lindskog and Erland Jonsson.Adding Security to Quality of Service Architectures[C]. Proceedings of the SSGRR Conference, Aug. 2002.

[4] Syed Naqvi, Michel Riguidel. Quantifiable Security Metrics for Large Scale Heterogeneous Systems[C]. Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International, Oct. 2006 . p209-215.

[5] Joseph Pamula,, Paul Ammann. A Weakest–Adversary Security Metric for Network Configuration Security Analysis[C], Proceedings of the 2nd ACM workshop on Quality of protection, Alexandria, Virginia, USA, 2006, 31 – 38.

[6] Alkahtmi, M. E. Woodward, The Analytic Hierarchy Process Applied to Best Effort QoS Routing with Multiple Metrics: a Comparative Evaluation[C], Personal Mobile Communications Conference, 2003. 5th European (Conf. Publ. No. 492),p539- 544.

[7] I. A. Almerhag , M. E. Woodward. Security as a quality of service routing problem[C], Proceedings of the 2005 ACM conference on Emerging network experiment and technology,p 222 – 223.

[8] Kalyanmoy Deb. A fast and elitist multiobjective genetic algorithm: NSGA-II [J]. IEEE Transactions on Computation, 2002, 6(2): p182-197.

[9] Madalina Baltatu, Antonio Lioy, Fabio Maino, Security Issues in Control, Management[C],TERENA Networking Conference, May 22-25, 2000.

[10] M. Goncalves.Firewalls Complete, McGraw-Hill, 2002[EB/OL], URL: http://www.secinf.net/firewalls_and_VPN/Firewalls_Complete/.

[11] I.A. Almerhag and M.E. Woodward.Key Length as a QoS Routing Metric[C]. Sixth informatics workshop, pp. 23–24 , March 2005.

[12] Le Faucheur, F., Wu, L., Davie, B., Davari, S., Vaananen, P.,Krishnan, R., Cheval, P., Heinanen, J., "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services", IETFRFC 3270, 2002.

[13] J. Horn, N. Nafploitis, and D. E. Goldberg, "A niched Pareto genetic algorithm for multiobjective optimization," in Proceedings of the First IEEE Conference on Evolutionary Computation, Z. Michalewicz,Ed. Piscataway, NJ: IEEE Press, 1994, pp. 82–87.

[14] Zegura EW, Calvert KL, Donahoo MJ. A quantitative comparison of graph-based models for Internet topology[J].IEEE/ACM Trans. on Networking, 1997,5(6):770~783.