Virtual Network with Security Guarantee Embedding Algorithms

Chiqiang Xing
National Digital switching System Engineering & Technological R&D Center, Zhengzhou, China
Email: xingchiqiang@126.com

Julong Lan and Yuxiang Hu
National Digital switching System Engineering & Technological R&D Center, Zhengzhou, China
Email: ndscljl@163.com, chxachxa@126.com

***Abstract*—Network virtualization has been widely concerned as the new technology to remedy the current ossification Internet architecture. Previous virtual network (VN) embedding algorithms focus on optimizing the use of resources with regard to performance with constraints on virtual nodes and links. There are few researches to analyze the security threat to the virtual network. In this paper, we first present two security threats of virtual network and investigate them in depth. Then we propose a novel virtual network with security guarantee that will take the trust value and security protection level as the new security constraints during its embedding. The virtual network with security guarantee embedding algorithm is given at last, and the simulation results show that the algorithm is effective.**

***Index Terms*—virtual network embedding;security guarantee; trust value; security protection level.**

I. INTRODUCTION

The packet switching used by the Internet Protocol (IP) has its own quality characteristics [1], and its simple structure that the network terminals are intelligent makes the Internet an important information infrastructure that supports economic development, social progress and scientific innovation in modern society, while generates some new problems. First, the rigid Internet architecture, the single function of network layer and the excessive separation between the business and network cannot meet the diverse needs of the business; secondly, because the Internet cannot be changed, the implementation and promotion of new technologies, such as IPv6, DiffServ and IntServ are very difficult [2].

In recent years, network virtualization has been widely concerned by the industry and academia [3]. Network virtualization has been propounded as a fundamental diversifying attribute of the future internetworking paradigm that will allow multiple heterogeneous network architectures to coexist on a shared substrate [4]. It also enables researchers to design and evaluation new networking protocols on the heterogeneous experimental architectures [5] [6]. Constructing virtual backbone network in wireless sensor networks also has a wonderful performance in improving the performance of broadcast [7]. Therefore, the network virtualization can support network technology innovations effectively, make it possible to deploy new network architectures, protocols and applications without changing the existing network. It not only provides a feasible evolution way from the current network to the future, but also a key feature of the future Internet [8].

Previous virtual network embedding algorithms are aimed to archive optimization objects, such as the acceptance ratio, the average revenue/cost of the substrate network over time and the load balancing, with constraints on virtual nodes and links. These virtual network embedding (VNE) algorithms can be divided into different kinds: uncoordinated and coordinated, static and dynamic, distributed and centralized, concise and redundant. Minlan Yu[9] designed a virtual link mapping algorithm and path migration algorithm based on the multi-commodity flow (MCF)under the condition that the substrate network support division and migration, improved the link mapping phase of the baseline algorithm to get higher substrate network resource utilization. In literature [10], the main objective of the virtual network embedding algorithm based on traffic constraint was to find a virtual network that can not only meet the traffic demand but also get efficient utilization of the substrate network resource. In literature [11] a virtual network mapping algorithm with QoS guarantees (QoSMap) was proposed, its basic idea is to map a virtual link onto a single link and use a hop relay routing node to provide high quality backup routing path for the virtual link, improving the quality and reliability of the virtual network. Literature [12] presents two algorithms in order to make the substrate network load balanced: virtual network mapping algorithm without reconfiguration and virtual network mapping algorithm with reconfiguration, the first algorithm's basic idea is to map all of the virtual nodes onto the substrate nodes with little load and nearer to the virtual node that have already been mapped, then map the virtual link with the shortest path algorithm; the latter cyclically examine the load of the substrate nodes and links. And when the load exceeds a predefined threshold value, the VNs mapped to the node or link will be re-mapped to eliminate resource bottlenecks.

doi:10.4304/jcp.8.11.2782-2788

Nowadays, the issues of network security are becoming increasingly serious and attract more attention [13]. These algorithms are proposed to increase the acceptance ratio that map as more as possible VN requests onto specific nodes and paths in the substrate network with constraints on virtual links and nodes resources. However, the security of the substrate hosts in the substrate network is not considered. Because all the virtual nodes of different VN requests are mapped onto the substrate nodes, the VN will be affected if the substrate nodes are under attack or cannot be trusted. In response to these problems, we will consider new security constraints that the substrate nodes need to meet the security requirements of the virtual networks during the mapping to guarantee the security of VN and resist the possible attacks to the substrate hosts.

The remainder of this paper is organized as follows. Section 2 formalizes the Virtual Network with Security guarantee (SVN) model and gives the description and evaluation of the embedding problems. Based on the Section 2, we proposed two algorithms: VN embedding algorithm based on the greedy algorithm (VNE-GA) without security constraints and VN embedding algorithm with security constraints (SVNE-GA), and then compared the both in Section 3. Section 4 presents simulations results that evaluate the proposed algorithms and Section 5 concludes the paper.

II. Virtual Network Model and Embedding Problem

A. *Model of the Virtual Network with Security Guarantee*

The hierarchy architecture of VNs is shown in Figure 1. The substrate nodes that the virtual nodes are mapped onto are called host nodes.

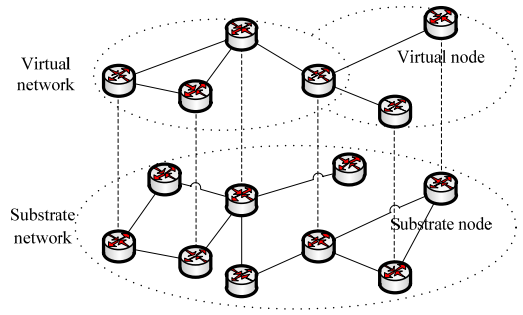

Figure 1. the hierarchy architecture of the virtual network

The security of information is an issue related to information and communication technology and a management issue as well [14]. The risks that the VN introduced can be categorized in two areas:

- A host node attacking one of its virtual nodes. The resources that the virtual node uses are ultimately the resources owned by host nodes. All the computations of the virtual node are carried out by the hardware and software of host nodes. The host nodes can monitor or change any act of the virtual nodes in theory. And virtual nodes have no option to defend themselves. In this case we need to map the virtual nodes onto trusted host nodes.
- Other malicious nodes attacking the host nodes affecting the working of VNs. In this case, host nodes being under attack, the VNs cannot work properly, even causing information leakage. Then we need to consider the anti-attack ability, called security protection level of the substrate nodes. And we can only map the virtual nodes onto the substrate nodes that have a higher level of the security protection.

In the first case, we can use the trust relationship between nodes to get the trust value as one of the security constraints on virtual nodes. Some researchers apply the trust relationship mechanism to the communication network to enable the network with intrusion tolerance and increase the security. Usually, the trust value node A to node B is a decimal between 0 and 1. The higher value indicates the more trust from A to B. Meanwhile, the trust relationship management is a complex process. The trust value will decrease if B does some malicious activities to other nodes that A recognizes. For simple, we will not consider the trust relationship between nodes and set the trust value of each node a unified decimal between 0 and 1 in the whole network.

For the second case, we can introduce the computer information system security protection level of substrate nodes, which is defined in the GB17895-1999 “Classified oriteria for security protection of computer information system”, as another security constraint on virtual nodes. GB17895-1999 provides the computer information system security protection with five levels: the first level of user self-protection level, the second level of system audit protection level, the third level of security token protection level, the fourth level of structural protection level and the fifth level of access authentication protection level. This provision applies to divide level of the computer information system security protection. The security protection capabilities of the computer information system increase as the level increases. The relationships between five levels and security functions are shown in the Table 1:

TABLE 1

THE RELATIONSHIPS BETWEEN FIVE LEVELS AND SECURITY FUNCTIONS

	Level 1	Level 2	Level 3	Level 4	Level 5
Discretionary Access Control	Y	Y	Y	Y	Y
Mandatory Access Control	-	-	Y	Y	Y
Mark			Y	Y	Y

Authentication	Y	Y	Y	Y	Y
Object reuse	-	Y	Y	Y	Y
Audit	-	Y	Y	Y	Y
Data Integrity	Y	Y	Y	Y	Y
Covert channel analysis	-	-	-	Y	Y
Trusted path	-	-	-	Y	Y
Credible analysis	-	-	-	-	Y

So, during the embedding process of SVN, except for the remaining node CPU resources and link bandwidth need to meet the VN request, the trust value and security protection level of substrate nodes should also meet the requirements of VNs.

B. Virtual Network Embedding Problem

Substrate network. For the embedding problem of SVN, the substrate network can be modeled as a weighted undirected graph and denote it by $G_s=(V_s, E_s)$, where V_s is the set of substrate nodes and E_s is the set of substrate links. Each substrate node $v_s \in V_s$ is associated with the CPU capacity weight value $C(v_s)$, trust value $T(v_s)$ and safety protection level $S(v_s)$. Each substrate link $e_s(i, j) \in E_s$ between two substrate nodes i and j is associated with the bandwidth capacity weight value $W(e_s)$ denoting the total amount of bandwidth. The $C(v_s)$, $T(v_s)$, $S(v_s)$ and $W(E_s)$ are non-negative, and $T(v_s) \in [0,1]$, $S(v_s) \in \{1,2,3,4,5\}$.

VN request. Similar to the substrate network, we model VN requests as weighted undirected graphs and denote a VN request by $G_v=(V_v, E_v)$. Likewise, Each virtual node $v_v \in V_v$ is associated with the required CPU weight value $C(v_v)$, trust value $T(v_v)$ and safety protection value $S(v_v)$. Each virtual link $e_v \in E_v$is associated with the required bandwidth weight value $W(e_s)$ denoting the required bandwidth. The $C(v_v)$, $T(v_v)$, $S(v_v)$ and $W(E_v)$ are non-negative, and $T(v_v) \in [0,1]$, $S(v_v) \in \{1,2,3,4,5\}$. Each VN is also associated with the required time and lifetime.

VN Embedding. A virtual network embedding for a VN request can be defined as a mapping: $M : G_v \rightarrow (V_s', P')$, where $V_s' \subseteq V_s$ is a subset of the substrate nodes and $P' \subseteq P$, the mapping result of E_s ,is a subset of the substrate links. The VN embedding can be naturally decomposed into node and link mapping and both the V_s' and P' are required to meet certain constraints. For the node mapping $M^V : V_v \rightarrow V_s'$, mapping virtual nodes onto substrate nodes that all $M^v(v_v) \in V_S$ subject to

$$\begin{cases} RC(M^V(v_v)) \geq C(v_v) \\ T(M^V(v_v)) \geq T(v_v) \\ S(M^V(v_v)) \geq S(v_v) \end{cases} \quad (1)$$

For the link mapping

$$RW(e_s) \geq W(e_v), \forall e_s \in P(M^V(u), M^V(v)) \quad (2)$$

$RC(v_s)$ and $RW(e_s)$ denote the remaining CPU resources of node v_s and the remaining bandwidth of link e_s, where u and v are virtual nodes.

Objectives. Our main interest is to propose an efficient embedding algorithm for the SVN and compare with the VN. Because of the additional security constraints, the security protection level and the trust value on virtual nodes during the embedding process of VN, we redefine the revenue and cost of the substrate network as follows.

Similar to the previous work, we introduce the notion of revenue that corresponds to the economic benefit of accepting the VN request. We denote by $R(G_v, t)$ the revenue of serving the VN request at time t. Revenue gives an insight into how much an InP will gain by accepting a VN request.

$$\begin{aligned} R(G_v, t) &= \alpha_1 \cdot \sum_{e_v \in E_v} W(e_v) + \alpha_2 \cdot \sum_{v_v \in V_v} C(v_v) \\ &+ \alpha_3 \cdot \sum_{v_v \in V_v} (k_1 \cdot T(v_v) + k_2 \cdot S(v_v)) \end{aligned} \quad (3)$$

We also redefine the cost of accepting a VN request as the sum of total substrate resources allocated to the VN.

$$\begin{aligned} C(G_v, t) &= \alpha_1 \sum_{e_s \in P'} W(e_v) + \alpha_2 \sum_{v_s \in V_s'} C(v_v) \\ &+ \alpha_3 \cdot \sum_{v_s \in V_s'} (k_1 \cdot T(v_v) + k_2 \cdot S(v_v)) \end{aligned} \quad (4)$$

And the following three evaluations can be given:

1) Average Revenue Over Time:

$$R/T = \lim_{T \to \infty} \frac{\sum_{t=0}^{T} R(G_v, t)}{T} \quad (5)$$

2) Acceptance Ratio:

$$\lim_{T \to \infty} \frac{\sum_{t=0}^{T} V_S}{\sum_{t=0}^{T} V} \quad (6)$$

3) Average Revenue/Cost:

$$\lim_{T \to \infty} \frac{\sum_{t=0}^{T} R(G_v, t)}{\sum_{t=0}^{T} C(G_v, t)} \quad (7)$$

III. VIRTUAL NETWORK WITH SECURITY GUARANTEE EMBEDDING ALGORITHM

We employ a node mapping algorithm based on greedy, since it is computational too expensive to employ other strategies. In order to map virtual nodes onto substrate nodes based on the greedy algorithm, we gives the following definition to evaluate the remaining bandwidth of substrate nodes and the demand bandwidth of virtual nodes:

From the substrate node's point of view, we denote by $PR(t, v_s)$ the potential remaining bandwidth of the substrate node at time t as the sum of the remaining bandwidth of all the links that connect node v_s:

$$PR(t, v_s) = \sum_{e_s \in L(v_s)} RW(t, e_s) \quad (8)$$

We also define by $PR(t,v_v)$ the potential required bandwidth of the virtual node at time t as the sum of the required bandwidth of all the virtual links that connect to v_v:

$$PR(t, v_v) = \sum_{e_v \in L(v_v)} W(t, e_v) \quad (9)$$

Algorithm 1 VN Embedding Algorithm based on Greedy Algorithm, VNE-GA

Step 1: Sort the virtual nodes according to the $PR(t, v_v)$ and the substrate nodes according to the $AR(t, v_s)$ in descending order when the VN request arrives. Define N_v and N_s as the number of virtual nodes and substrate nodes respectively;

Step 2: for i=1:N_v , j=1: N_s, if $RC(v_s)_j \geq RC(v_v)_i$, map the virtual node v_{vi} onto the substrate node v_{sj}. If all the virtual nodes are mapped successfully, go to Step 3; otherwise go to Step 5, the request fails;

Step 3: $\forall e_v \in E_v$, find the shortest path that meets the bandwidth requirement with the shortest path algorithm to complete the link mapping. If all the virtual links are mapped successfully, go to Step 4; otherwise go to Step 5, the request fails;

Step 4: Update the substrate network with the node CPU resources and link bandwidth resources;

Step 5: Waiting for the next VN request arrives and then go to Step 1.

In the SVN embedding algorithm, because of the additional security constraints we first need to remove the substrate nodes that does not meet the needs of the SVN request, and then perform the above VNE-GA algorithm. Meanwhile, due to the "bucket effect" of the security, we let the security protection level S and the trust value T of the virtual nodes to be same in the same SVN. We can give the SVN embedding algorithm based on greedy.

Algorithm 2 SVN Embedding Algorithm based on Greedy Algorithm, SVNE-GA

Step 1: Remove the substrate nodes that cannot meet the security constraints S,T when the SVN request arrives, getting an available set of substrate nodes. Define N_v and N_s as the number of virtual nodes and available substrate nodes respectively. If $N_s > N_v$, go to Step 2; otherwise go to Step 5, the request fails;

Step 2: for i=1: N_v , j=1: N_s, if $RC(v_s)_j \geq RC(v_v)_i$, then map the virtual node v_{vi} onto substrate node v_{sj}. If all the virtual nodes are mapped successfully, go to Step 3; otherwise go to Step 5, the request fails;

Step 3: $\forall e_v \in E_v$ find the shortest path that meets the bandwidth requirement with the shortest path algorithm to complete the link mapping. If all the virtual links are mapped successfully, go to Step 4; otherwise go to Step 5, the request fails;

Step 4: Update the substrate network with the node CPU resources and link bandwidth resources;

Step 5: Waiting for the next SVN request arrives and then go to Step 1.

Compared with the VNE-GA , the SVNE-GA algorithm will lead to lower acceptance ratio as the available substrate nodes decrease because of the security constraints on virtual nodes. The following simulation experiments and results also verified this situation.

IV. PERFORMANCE EVALUATION

In this section, we first describe the performance evaluation environment, and then present our main evaluation results. Our evaluation focuses primarily on comparing the acceptance ratio, revenue and cost of substrate network in the above two algorithms.

A. Evaluation Environment

We implement a VN embedding simulator to evaluate our algorithms.

Substrate network. We use the GT-ITM tool [15] to generate the substrate network topology. The substrate network is configured to have 100 nodes and around 500 links, a scale that corresponds to a medium-sized ISP. The CPU resources at nodes and the link bandwidths at links follow a uniform distribution from 50 to 100 units. The trust value and the security protection level follow a uniform distribution from 0 to1 and 1to 5 (integer) separately.

VN request. The arrivals of VN requests are modeled by a Poisson process with mean five requests per 100 time units. The duration of the requests follows an exponential distribution with 500 time units on average. In one VN request, the number of VN nodes is randomly determined by a uniform distribution between 2 and 20. Each pair of virtual nodes are randomly connected with probability 0.5. As well, the CPU requirements of the virtual nodes and the bandwidth requirements of the virtual links are uniformly distributed between 0 and 50. The required trust value and the security protection level follow a uniform distribution from 0 to1 and 1to 5 (integer) separately.

In VNE-GA and G-SP [11], because there are no security constraints, we set α_1=α_2=0.5, α_3=0 in (3) (4). In SVNE-GA, we set α_1=α_2=α_3=1/3, and considering the values of T and S, set k_1=25, k_2=5.We run all of simulations for 50000 time units, which correspond to about 2500 requests on average in an instance of simulation.

B. Evaluation Results

We used several metrics in our evaluations to measure the performances of our algorithms against the G-SP and compare the VN and SVN. The metrics conclude the acceptance ratio, average revenue(R) and cost (C) over time. We also evaluated and compared the acceptance ratio by changing the distributions that the trust value and security protection level of substrate nodes follow. In all cases we plot the performance metrics against time to show how each of these algorithms actually perform in the long run. We summarize our key observations in the following.

(1) VNE-GA leads to higher acceptance ratio than G-SP and because of additional security constraints, SVNE-GA leads to lower acceptance ratio than VNE-GA. Fig.2 depict that without the security

constraints, the acceptance ratio of VNE-GA is 65%, achieving about 10% increases over the G-SP. And the acceptance ratio of SVNE-GA is about 53%, 12% decreasing over the VNE-GA. This is because that VNE-SC takes the trust value and security protection level as the additional constraints on virtual nodes, the available substrate nodes decrease for each VN request.

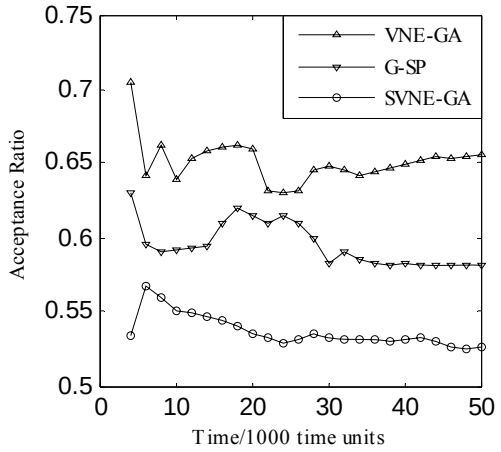

Figure 2. VN request acceptance ratio.

(2)VNE-SC leads to higher revenue/cost than VNE-GA. Figure 3 shows the result. Because of the additional components (trust value and security protection level in (3) (4))in the revue and cost, the substrate network can provide customized services and security guarantee, making the revenue increase significantly and the cost increase slightly, leading significantly improvement of the R/C. Fig.3 and Fig.4 give the average revenue and cost over time separately. We can see that because of the security constraints, the acceptance ratio decreased, as the cost and revenue.

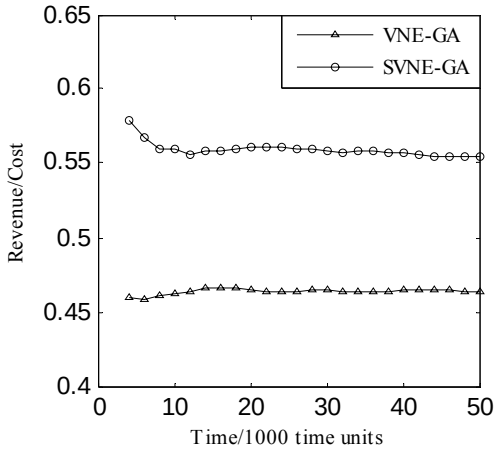

Figure 3. Time average of revenue/cost

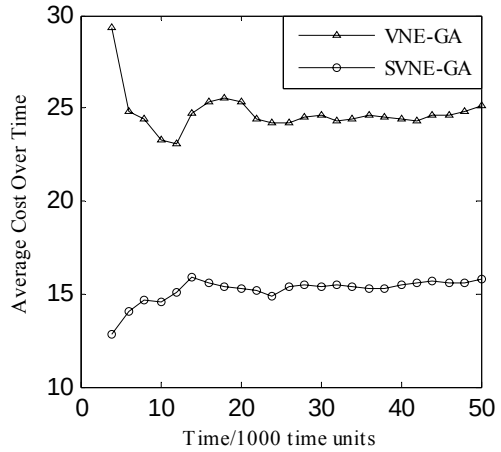

Figure 4. Average cost over time

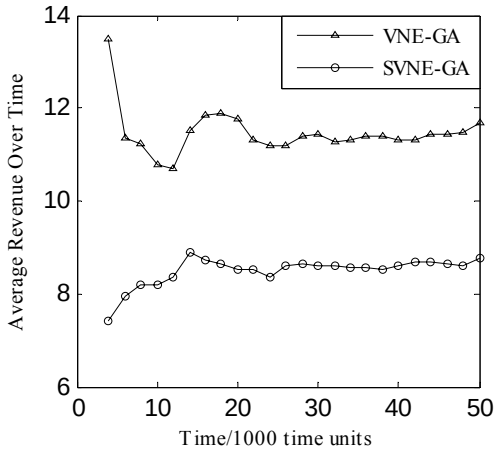

Figure 5. Average revenue over time

(3) The substrate network with higher trust value and security protection level will lead to higher acceptance ratio. From the results above we can see that the acceptance ratio decreased due to additional constraints of the security protection level and trust value on virtual nodes. Therefore, the different distributions of the trust value and security protection level (called as the "ability") of the substrate network will lead to different acceptance ratio. The following simulation shows this situation too. The different distributions of the trust value and security protection level of the substrate network are shown in Table 2. We can see that the "ability" of substrate nodes in Distribution 2 is stronger than Distribution 1.

TABLE 2
DIFFERENT DISTRIBUTIONS OF THE TRUST VALUE AND SECURITY PROTECTION LEVEL

Security protection level	Trust value	Distribution1	Distribution2
Level 1	[0,0.2)	0.2	0.1
Level 2	[0.2,0.4)	0.2	0.15

Level 3	[0.4,0.6)	0.2	0.2
Level 4	[0.6,0.8)	0.2	0.25
Level 5	[0.8,1]	0.2	0.3

The result of acceptance ratio is shown in Fig.5. The acceptance of Distribution 2 is 57%, 4% (about 100 SVN requests) increase over Distribution 1. This is because the "ability" of substrate nodes in Distribution 2 is stronger than Distribution 1, leading the number of available substrate nodes increasing for each VN request, and the higher acceptance ratio.

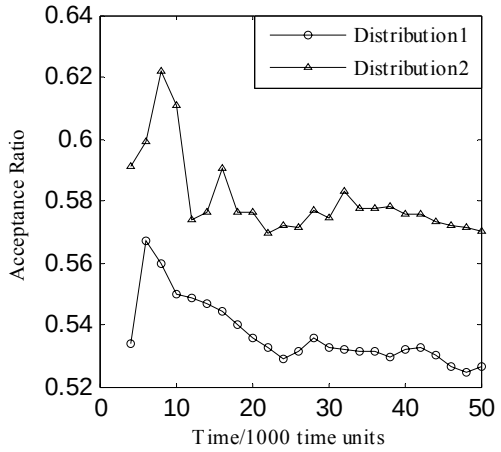

Figure 6. SVN request acceptance ratio

V. CONCLUSION

Network virtualization has been propounded as a fundamental diversifying attribute of the future internetworking paradigm that will allow multiple heterogeneous network architectures to coexist on a shared substrate. However, being the foundation critical infrastructure, VN must strive to ensure a certain level of security. In this paper we first analyzes two security risks that the network virtualization introduced and then proposes a new virtual network model with security guarantee that take the trust value and security protection level of substrate nodes as new constraints. Finally, the virtual network with security guarantee embedding algorithm based on greedy algorithm is given and the simulation results show that the algorithm is effective and validate. We also proved that the substrate nodes with higher security "ability" can increase the acceptance ratio.

Meanwhile, the virtual network model with security guarantee in this paper is a new consideration that needs further study in many ways: First, the dynamically management and update of the trust relationships between substrate nodes. Second, the improvement of the SVN embedding algorithm, especially considering how to use the intelligence optimization algorithm to increase the acceptance ratio and make the substrate network load balanced are the future works.

ACKNOWLEDGMENT

This paper is originated from a project numbered as 2012CB315901, which is supported by national 973 foundations, and 2011AA01A103, 2011AA01A101, which is supported by national 863 foundations.

REFERENCES

[1] CHENG Dong-nian, WANG Bin-qiang, WANG Bao-jin, ZHANG Jian-hui. Preliminary study on the connotation of flexibility in dynamically reconfigurable networks[J].*Journal of Communication*, Volume33, Number8, pages 214-222, 2012

[2] Secure virtual network embedding. *Praxis der Information sverarbeiting and Kommunikation*, Volume34, Number4, pages190-193, 2011.

[3] CHENG Xiang, ZHANG Zhong-bao, SU Sen, YANG Fang-chun. Survey of virtual network embedding problem[J]. *Journal of Communication*, Volume32, Number10, pages143-151,2011.

[4] Mosharaf Chowdhury, Muntasir Raihan Rahman, Raouf Boutaba. ViNEYard: Virtual Network Embedding Algorithms With Coordinated Node and Link Mapping. *IEEE/ACM TRANSACTIONS ON NETWORKING*, VOL. 20, NO. 1, FEBRUARY2012.

[5] "GENI:Global environment for network innovations," [Online].Available:http://www.geni.net/

[6] A. Bavier, N. Feamster, M. Huang, L. Peterson, and J. Rexford, "In VINI veritas: Realistic and controlled network experimentation," in *Proc. ACM SIGCOMM*, 2006, pp. 3–14.

[7] Yong Tang, Yu Xiang, et al. Leveraging 1-hop Neighborhood Knowledge for Connected Dominating Set in Wireless Sensor Networks. *Journal of Computers*, 2012, 7(1), 11-18.

[8] FEAMSlER N, GAO L, REXFORD J. How to lease the Interact in your spare time[J]. *ACM SIGCOMM Computer Communication Review* 2007, 37(1):61·64.

[9] YU M, YI Y, REXFORD J, et a1. Rethinking virtual network embedding: substrate support for path splitting and migration[J], *ACMSIGCOMM Computer Communication Review*, 2008, 38(2):17—29.

[10] LU J. TURNER J, Efficient Mapping of Virtual Networks onto a Shared Substrate[R]. *Department of Computer Science and Engineering*, Washington University, 2006.

[11] SHAMSI J, BROCKMEYER M. QoSMap:QoS aware mapping of virtual networks for resiliency and efficiency[A]. *Proceedings of the IEEE GLOBECOM Workshop* [C] Washington. IX, USA, 2007.6.

[12] ZHU Y, AMMAR M. Algorithms for assigning substrate network resources to virtual network components[A]. *Proceedings of the IEEE INFOCOM[C]*. Barcelona, Spain, 2006, pp.1-12.

[13] Ye Du Jiqiang, Liu Ruhui, et al. A Dynamic Security Mechanism for Web Services Based on NDIS Intermediate Drivers. *JOURNAL OF COMPUTERS*. 2011, 6(10), 2021-2028.

[14] Kuo-Hsiung Liao, Hao-En Chueh. Medical Organization Information Security Management Based on ISO27001 Information Security Standard. *Journal of Software*, 2012,7(4), 792-797.

[15] E. W. Zegura, K. L. Calvert, and S. Bhattacharjee. How to model an internetwork. *In Proc. IEEE INFOCOM*, 1996.

Chiqiang Xing is currently a Post-Graduate student at the National Digital switching System Engineering & Technological R&D Center, Zhengzhou, China, supervised by Professor Julong Lan. His research interests include information network, network security and new network architecture.

Julong Lan is currently a professor at the National Digital switching System Engineering & Technological R&D Center, Zhengzhou, China. His research interests include new network architecture and Network modeling.

Yuxiang Hu is currently a lecturer at the National Digital switching System Engineering & Technological R&D Center, Zhengzhou, China. His research interests include new network architecture, routing and switching technologies.