Communications and Network, **2009, 1, 101-107**
doi:10.4236/cn.2009.12016 Published Online November 2009 (http://www.scirp.org/journal/cn).

Scientific Research

A Novel Mechanism in MPLS Network under Adversarial Uncertainty

Ying ZHENG
Wuhan Maritime Communication Research Institute, Wuhan, China
E-mail: *phoolcee*2004@yahoo.com.cn
Received October 11, 2009; *accepted November* 9, 2009

Abstract

The advantage of multi-protocol label switching (MPLS) is its capability to route the packets through explicit paths. But the nodes in the paths may be possibly attacked by the adversarial uncertainty. Aiming at this problem in MPLS Network, in this paper, we propose a novel mechanism in MPLS network under adversarial uncertainty, making use of the theory of artificial intelligence, at first, we find the initialized label switching paths (LSPs) using the A* arithmetic, and secondly, during the process of data transmission, we switch the transmission path duly by taking advantage of the non-monotone reasoning mechanism. Compared to the traditional route mechanism, the experimental results show that it improves the security if data transmission remarkably under our novel mechanism in MPLS network.

Keywords: A* Arithmetic, Non-Monotone Reasoning Mechanism, Data Transmission, MPLS Network

1. Introduction

The purpose of traffic engineering (TE) is to improve network performance through the optimization of network resources [1]. The emerging Multi-Protocol Label Switching (MPLS) technology has introduced an attractive solution to TE in IP networks. MPLS can efficiently support the explicit routes setup through the use of Label Switched Paths (LSPs) between the ingress Label Switched Router (LSR) and the egress LSR [2]. Hence it is possible to balance the traffic through the network, thus improving the network utilization and minimizing the congestion. many researchers have proposed all kinds of arithmetic about the traffic engineering in MPLS network. Several researchers have proposed some solutions to balance the load in MPLS networks. An analytical framework is presented in [3] where different models with different objective functions for best-effort and expedited-forwarding traffic respectively are established. Another load balancing mechanism called MATE (MPLS adaptive traffic engineering) [4] develops its algorithm based on the gradient project method. MATE is based on a distributed multi path balancing approach. The source routers perform an active measurement of each LSP by sending probing packets and measuring the delay jitter and the loss of the packets. The calculation of the new load distribution relies on the optimal routing with the gradient projection algorithm [5]. The traffic engineering capable routers perform rebalancing actions without coordination. To prevent the system from routing oscillations due to concurrent rebalancing actions, each LSR adapts the load distribution of its LSPs with a limited step size. After each load rebalancing action, the LSPs are measured again. Because the step size decreases with an increasing network size and the load has to be measured after each rebalancing action over a certain period of time, MATE converges slowly in great networks.

Unfortunately, So far, there have few researchers to talk about the security of the process of data transmission in the MPLS network, and it is very possible for the data transmission process to be in face of all kinds of attacks by the adversarial uncertainty. Currently, commercial networks, including the Internet, may carry mission-critical applications. Possibility of a disaster or adversary attack necessitates developing management schemes that balance cost efficiency with robustness. In practical situations some limited (incomplete) statistical information about the operating environment is available. Proper utilization of this incomplete information would allow the network to reduce the safety margin and consequently increase the cost efficiency with respect to the resource utilization. On the other hand, one of the most obvious attacks to a communication network is packet interception which prevents data originating from one (or several) nodes to reach the destination. Eavesdropping

can be thought as a "passive" form of interception, in which packets are "snooped" but not removed from the network, it means that the nodes in the transmission paths (LSPs) may be attacked by the attacker, and it will disturb the normal and security transmission process.

Among the traditional traffic balancing algorithms, the nodes in the MPLS network send the information related to the links to one another termly to make the transmission source know the qos of every transmission path dynamically, and distribute the traffic equably among several transmission paths, it is no problem under normal situation, but once there exists a vicious attack node (or a node has just been controlled by the attacker)in the transmission path, it will be very possible for the transmission source to get wrong information from the nodes in the network ,and make wrong strategy about the traffic distribute, so, obviously, we can not only consider the normal qos parameters, such as throughput ,bandwidth, link delay, and etc, in order to make the process of data transmission in the MPLS network more secure, we also need to consider the security of data, such as the data integrality, the data confidentiality, and so on, and also the security of transmission nodes, for example, the healthy state of nodes, and the time during a given interval period that a node is attacked.

In this paper, based the active defense model [11], aiming at the problem related to the security of the data transmission process, we propose a novel mechanism in MPLS network under adversarial uncertainty, making use of the theory of artificial intelligence, at first, we find the initialized label switching paths (LSPs) using the A* arithmetic, and secondly, during the process of data transmission, we switch the transmission path duly by taking advantage of the non-monotone reasoning mechanism.

2. A*Algorithm Description

A* algorithm is a typical heuristic searching algorithm in the theory of artificial intelligence ,it mainly aims at the definition and description for the evaluation function, and performs a searching algorithm which possesses the strong heuristic capability ,and at the same time, A* algorithm is also a best preferential algorithm as long as it is attached with some constraint condition, anyway, A* algorithm can settle the searching problem in which it finds a best path from the source to the destination in the state space and its efficiency is the best.

A* algorithm is an acceptable and best preferential algorithm, in which the evaluation function can be denoted as:

$$f^*(n)=g^*(n)+h^*(n)$$

where f*(n) stands for evaluation function, g*(n) denotes the current cost value from the start node to the current node n, and h*(n) denotes the estimated cost value from the current node n to the destination node, it means that f*(n) is a estimated cost value for a special path with some constrains which includes the node n , and in the same time, the value of f*(n) carries out the track in real time to the best path.

From the description of A* algorithm ,we can know that the key point for A* algorithm is how to find the best appropriate evaluation function, and there have two reasons why we use A* algorithm to perform the transmission paths programming in MPLS network:

1) A* algorithm is a heuristic searching and dynamic programming algorithm, we can use this algorithm adjusts our route strategy in real time according to the current network state.

2) combining the non-monotone reasoning mechanism, we can use A* algorithm to perform trace function, it means once we find some nodes in the transmission path have security hidden trouble, we can change our transmission path in good time, and this character can be applied in the rerouting problem in MPLS network.

3. Initial Transmission Paths Programming and the Rerouting Flow

Based the A* algorithm, before starting data transmission, at first we should find the initial transmission paths according to the current network state, here , we not only consider all kinds of network parameters, such as throughput, bandwidth, link delay, and etc, but also some security parameters, they are showed below:

1) link state

Which includes the $delay(l_i)$ on each link l_i in the network under the current state, the bandwidth $bw(l_i)$ that has been consumed on link l_i.

2) node security index

Based the active defense model [11], we separate the whole network topology into N dynamic secure transmission domains, which is denote as $\{d_1, d_2, \cdots d_N\}$, there is a management node $m(d_i)$ in every secure transmission domain, and it chooses K attack forms A_k that may exist during the process of network data transmission, for example , the Dos attack , the confidentiality demolishing, the integrality demolishing, and so on, as the security evaluation criterion, during the every time interval t, $m(d_i)$ will measure the security property of every node $m_j^{'}(d_i)$ in the corresponding secure transmission domain for m times, and record the attack times $n_{km}(m_j^{'}(d_i))$ for every node, and then calculate the probability value $p(A_k, m_j^{'}(d_i))$, which stands for the

attack form A_k is implemented on the node $m_j^{'}(d_i)$ during the *m* times measurement:

$$p\ (A_k, m_j^{'}(d_i)) = \frac{n_{km}\left(m_j^{'}(d_i)\right)}{\sum_{1\le k\le K} n_{km}\left(m_j^{'}(d_i)\right)}$$

$$(1 \le k \le K, 1 \le i \le N)$$

according as different security requirement, we define the destructive index value for every attack form A_k $(1 \le k \le K)$, higher the value is ,and higher the threat of the corresponding attack form is:

$$0 \le w_k \le 1 (1 \le k \le K)$$

now define the threat index that the attack form A_k $(1 \le k \le K)$ gives to the node:

$$F\ (A_k, m_j^{'}(d_i)) = w_k \times p\ (A_k, m_j^{'}(d_i)),$$

$$1 \le k \le K, 1 \le i \le N$$

and then give the form of the node security index:

$$F\ (m_j^{'}(d_i)) = \sum_{1\le k\le K} F\ (A_k, m_j^{'}(d_i)),\quad 1 \le i \le N$$

the current link state value and the he node security index related to every node in the every secure transmission domain will be stored in the local database.

3) using A* algorithm to determine the Initial transmission paths set On the assumption that the MPLS network is denoted by the graph $G=(V,E)$, V presents the nodes set in the network, E stands for the links set, $n=|V|$ presents the nodes number in the graph, and $m=|E|$ presents the links number in the graph, where: $V=\{node_1, node_2, \cdots node_n\}$, $E=\{l(node_1 node_2), \cdots l(node_i ndoe_j)\}, 1 \le i \le n, 1 \le j \le n$, We set the degree of node $node_k$ as $\deg ree(node_k), 1 \le k \le n$, and according to the state values of every node in the network, $F(node_i)$, $delay(l_i)$, $bw(l_i)$, assume that the destination node is *t*, we can calculate the cost function value for every node $m(1 \le m \le n)$ as following formula:

$$\mathrm{f}(m)=\mathrm{g}(m)+\mathrm{h}(m)$$

$$\mathrm{g}(m)=\alpha * delay\left(l\left(node_m node_j\right)\right)+\beta * bw\ \left(l\left(node_m node_j\right)\right), \alpha+\beta=1, 1 \le j \le n, j \ne m$$

$$\mathrm{h}(m)=\alpha^{'} * \left(\deg ree(node_m)/N\right) * F(node_m)+\beta^{'} * hop_{\min}(m,t), \alpha^{'}+\beta^{'}=1, \deg ree(node_m) \ll N$$

where $hop_{\min}(m,t)$ presents the minimum hops from node *m* to node *t* in the graph *G*, and $\alpha^{'} > \beta^{'}$, the function $\mathrm{g}(m)$ mainly focuses on the every node' link state which is a neighbor of node *m*, and on the other hand, the function $\mathrm{h}(m)$ mainly focuses on how to guarantee the node's security, and also how to limit the length of the transmission path to a special range.

After we calculate the value $\mathrm{f}(m)$ for every node *m* in the graph, we can use the A* algorithm to find the corresponding transmission paths, suppose that there are *n* transmission paths need to be found, the step will be:

a) set $i=1$,

b) According to the current source and destination nodes pair (s,t) and the network state, calculate every value $\mathrm{f}(m)$ for every node *m* in the graph *G*.

c) followed by the A* algorithm, find a transmission path (LSP) between the node ***s*** and the node *t*, denote it by $\{node_{i_1}, node_{i_2}, \cdots node_{i_m}\}$, where $m \le n$.

d) update every value $\mathrm{f}(m)$ for every node *m* in the graph *G*, and then set

$$\mathrm{f}(node_{i_k})=+\infty, 1 \le \mathrm{k} \le \mathrm{m}$$

e) set $i=i+1$, go back to step b, until $i=n+1$.

And then, before starting the data transmission process, we can find *n* disconnected transmission paths (LSPs) between the node *s* and the node *t*, which can guarantee the security of the data transmission process in the current network state.

4) the rerouting flow (the non-monotone with credibility reasoning mechanism plus A* algorithm for the rerouting flow)

During the process of the rerouting flow , we take advantage of the non-monotone with credibility reasoning mechanism, which is related to the witness possibility reasoning, and the witness possibility reasoning is one of the forms of the non-monotone reasoning: $A \to B$, where A is a witness for the conclusion B, as the emergence of more and more witnesses, the possibility that the conclusion B is correct will possibly increase ,and also will possibly decrease, so the reasoning process possesses the non-monotone character, and also the reasoning process possesses the credibility, and the witness possibility reasoning can be denoted as:

$$A \to B, \gamma$$

where B denotes conclusion, and A is a witness which supports that is correct, γ is the credibility value for the

reasoning rule $A \to B$, and it means when the witness A happens, the credibility that supports B is correct, and it also means the amount that the witness A contributes to the conclusion that B is correct. When the new witness A' appears, it will contribute to the conclusion B in some extent, this contribution always has three possibilities: to make the credibility that B is correct increased, unchangeable, or decreased, and it always reflects the support degree between the new witness and the old witness, so there has a corresponding version which can be described that the new witness can support the old one with positive manner, and zero manner, and negative manner. The positive manner stands for that the new witness make the possibility that the conclusion is correct increase, the zero manner make the possibility that the conclusion is correct unchangeable ,and the negative manner make the possibility that the conclusion is correct decrease.

Set H as the witness space for the conclusion B, let & denote a binary operation on the H: let A &A ′denotes that witness A and witness A ′appear synchronously, and also the binary operation can be extended to the situation where exists discretional and limited witnesses, such as A 1&A 2&…&A n, which stands for the n witnesses appear synchronously, and

now: $\varepsilon : H \quad X \quad H \to [-1,1]$ denotes the witness support function between two witnesses, which satisfies the axioms below:

a) if witness A ′supports witness A with positive manner, and the information reflected by witness A ′is independent with the information reflected by witness A, then set $\varepsilon(A', A)=1$;

b) if witness A ′supports witness A with positive manner, and the information reflected by witness A ′is not independent with the information reflected by witness A, then set $0 < \varepsilon(A', A) < 1$;

c) if witness A ′supports witness A with negative manner, and the information reflected by witness A ′is not independent with the information reflected by witness A, then set $-1 < \varepsilon(A', A) < 0$;

d) if witness A ′supports witness A with negative manner, and the information reflected by witness A ′is independent with the information reflected by witness A, then set $\varepsilon(A', A) = -1$;

e) if the information reflected by witness A is the origin of the information reflected by witness A ′, then set $\varepsilon(A', A) = 0$;

f) if $\varepsilon(A_i, A_j) = 1$ (i≠j), so, $\varepsilon(A_1 \,\&\, A_2 \,\&\, \cdots \,\&\, A_i \,\&\, A_{i+1}) = 1$;

g) if $\varepsilon(A_i, A_j) = 0$ (i ≠ j), so, $\varepsilon(A_1 \,\&\, A_2 \,\&\, \cdots \,\&\, A_i \,\&\, A_{i+1}) = 0$.

The process of the non-monotone reasoning utilizes the theory of the witness possibility reasoning , aiming at a special conclusion, with the emergence of more and more witnesses ,according to analyzing the relationship of them(using the support function ε) ,and adjusting the credibility value to the conclusion constantly ,and the reasoning step is denoted as follows:

$$
\begin{aligned}
&A_1 \to B, \gamma_1 \\
&A_1 \,\&\, A_2 \to B, \gamma_2 = \eta\left(\gamma_1, \varepsilon\left(A_1, A_2\right)\right) \\
&A_1 \,\&\, A_2 \,\&\, A_3 \to B, \gamma_3 = \eta\left(\gamma_2, \varepsilon\left(A_1 \,\&\, A_2, A_3\right)\right) \\
&\vdots \\
&A_1 \,\&\, A_2 \,\&\, \cdots \,\&\, A_{n-1} \,\&\, A_n \to B, \gamma_n = \eta\left(\gamma_{n-1}, \varepsilon\left(A_1 \,\&\, A_2 \,\&\, \cdots \,\&\, A_{n-1}, A_n\right)\right)
\end{aligned}
$$

where the reasoning function $\varepsilon(x, y)$ must possess the property of the non-monotone reasoning, so we describe it as follows:

$$\varepsilon(x, y) = x\left(1 + y * \frac{1-x}{1+x}\right)$$

The function $\varepsilon(x, y)$ has the properties as follows: it is a linear increased function about y,

when $y = 1$, it gets the maximal value:

$$x * \left(1 + \frac{1-x}{1+x}\right) = \frac{2x}{1+x} \le 1;$$

when $y = -1$, it gets the minimum value:

$$x * \left(1 - \frac{1-x}{1+x}\right) = \frac{2x^2}{1+x} \le x;$$

when $y = 0$, it gets the middle value: 0.

According to the method above, we describe the process of the rerouting flow as a process of the non- monotone with credibility reasoning, where every node in the network has been assigned a credibility value, which will be updated termly by detecting the network state. If the credibility value of a node increases, it means that it's very possible the node will become a part of the transmission path, and on the other hand, every node in the

current transmission path has the credibility value and the evaluation cost value of the next node, according to the detecting network state in real time and the reasoning function $\varepsilon(x,y)$, once the credibility value of a node in the current transmission path decreases and goes beyond a special bound , the transmission path will be re- evaluated using A* algorithm from the previous node, and the process of the rerouting flow step is denoted as follows:

a) before starting the data transmission, we initialize the credibility value of every node in the network $G=(V,E)$ according to the history state of the network, assume the current source node and destination node is denoted as (s,t), the current transmission path is $LSP_c=\{node_{i_1},node_{i_2},\cdots node_{i_p}\}$, and let $\gamma^t(node_{i_k}),1\le k\le p$ denote the credibility value in the current time *t*.

b) in the every time interval τ, according to the reasoning step showed above , treats the new detect network state as the new witness constantly, and takes advantage of the reasoning function $\varepsilon(x,y)$ to update the credibility value $\gamma^t(node_{i_k}),1\le k\le p$ to $\gamma^{t+\tau}(node_{i_k}),1\le k\le p$ of every node which is in the current transmission path.

c) set $k=1$,

d) let $\Delta\gamma_{i_k}=\gamma^{t+\tau}(node_{i_k})-\gamma^t(node_{i_k})$, if $\Delta\gamma_{i_k}\ge 0$, then set $k=k+1$, and go back to step c; if $\Delta\gamma_{i_k}<0$ and $|\Delta\gamma_{i_k}|>\varepsilon$ (where ε stands for the limit value), then detects the previous and followed nodes of $node_{i_k}$ in turn, and set the previous node $node_{i_m}$ which satisfies the condition $\Delta\gamma_{i_m}\ge 0$, and set the followed node $node_{i_n}$ which satisfies the condition $\Delta\gamma_{i_n}\ge 0$, and then re-calculates a new transmission path between the $node_{i_m}$ and $node_{i_n}$ using A* algorithm.

e) let $k=n$, and go back to step d, until $n=p$.

f) go back to step b.

4. Simulation Results

To evaluate the mechanism proposed in Section 3, we simulated the network in Figure 1, data are transmitted from the blue node o to the red node d via the black nodes, using the ns-2 network simulator [12]. In the simulations presented, experiments data are performed using CBR according to TCP connecting, we assume that all the nodes in the network are secure before starting the data transmission, and during the process of data transmission, we also simulate the perturbed behave of attacker to some nodes in the network , the node which is be attacked will discard or tamper the packets that forwarded by it according to a special probability, and in the two experiments we make statistical work about two parameters: drop ratio and mark(tamper)ratio of packets transferred from node o to node d under our mechanism proposed in Section 3 (namely tcs)and the traditional route mechanism in MPLS network(namely static).

In experiment I, we simulate the attacker to attack a fixed node in the network, and we let data transfer from node o to node d under our mechanism proposed in Section 3 (namely tcs) and the traditional route mechanism in MPLS network (namely static) respectively, Figure 2 and Figure 3 show the results about drop ratio and mark ratio, where the green line stands for the transmission performance under tcs, while the red line stands for the transmission performance under static.

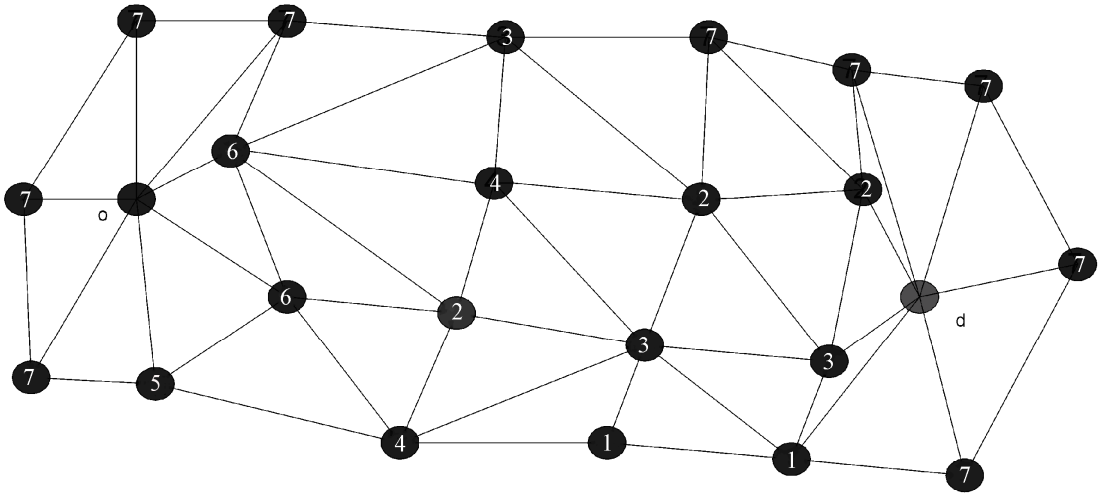

Figure 1. Network topology.

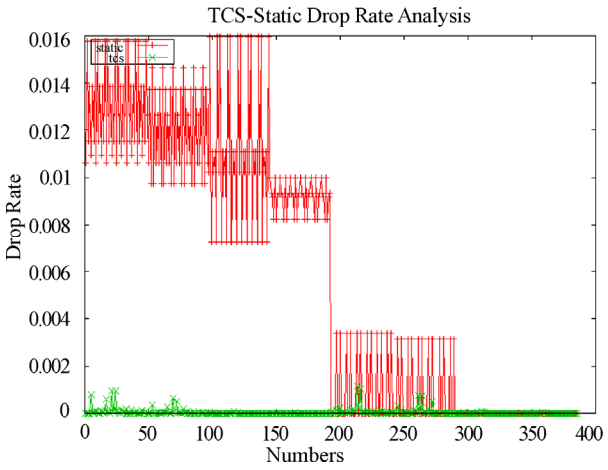

Figure 2. Drop ratio (experiment I).

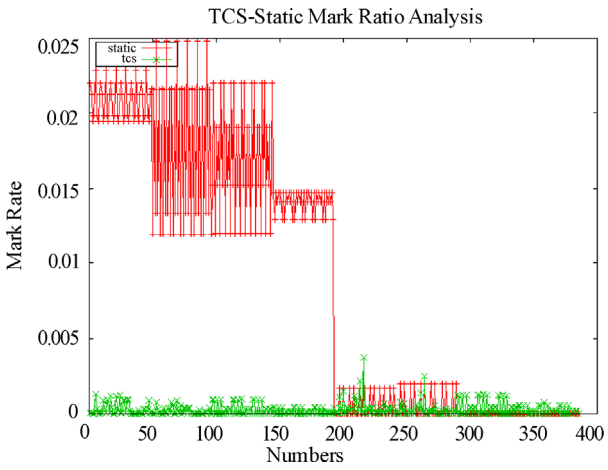

Figure 3. Mark ratio (experiment I).

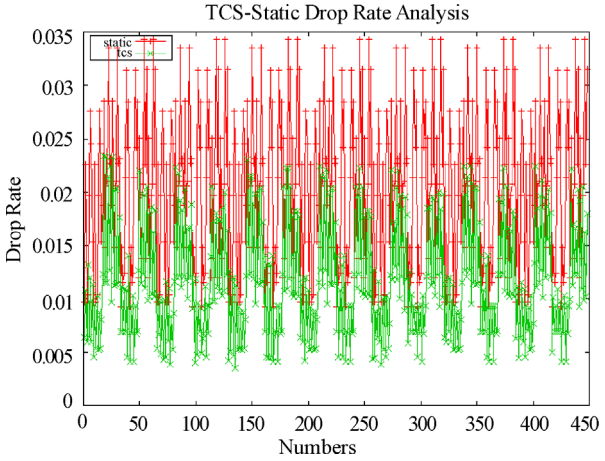

Figure 4. Drop ratio(experiment II).

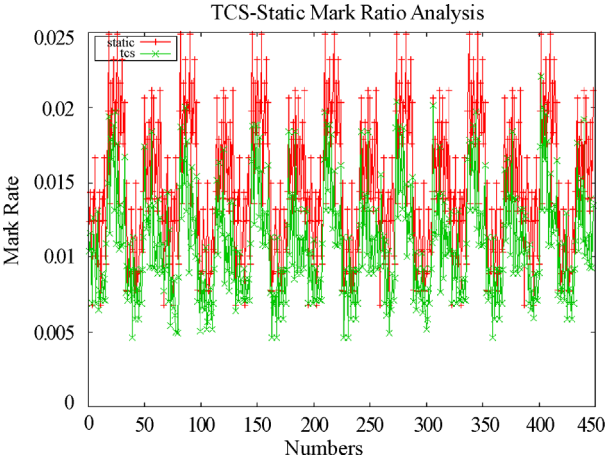

Figure 5. Mark ratio (experiment II).

The statistical data in experiment I are as follows:

route protocol	average drop ratio	average mark ratio
static	0.005844	0.008781
tcs	0.000050	0.000278

In experiment II, not like the experiment I, we simulate the attacker to attack a random node in the network, be similar to the experiment I, the corresponding results can be seen from Figure 4 and Figure 5.

The statistical data in experiment II are as follows:

route protocol	average drop ratio	average mark ratio
static	0.020500	0.014761
tcs	0.011685	0.010927

From the results in the two experiments, according to our proposed mechanism , using A* algorithm to determine the Initial transmission paths set and using the non-monotone with credibility reasoning mechanism for the rerouting flow, the security of data transmission process in the MPLS network improves markedly.

5. Conclusion

In this paper, making use of the theory of artificial intelligence, we propose A Novel Mechanism in MPLS network under adversarial uncertainty: at first, we evaluate the security of every node in the network, and use A* algorithm to determine the initial transmission paths, secondly, use the non-monotone with credibility reasoning mechanism to detect the network state and adjust route strategy constantly and switch the transmission path in good time. Compared to the traditional route mechanism, the experimental results show that it improves the security if data transmission remarkably under our novel mechanism in MPLS network.

6. References

[1] D. Awduche, *et al*., "Requirements for traffic engineering over MPLS," Internet RFC 2702, September 1999.

[2] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol label switching architecture," Internet RFC 3031, January 2001.

[3] E. Dinan, D. Awduche, and B. Jabbari, "Analytical framework for dynamic traffic partitioning in MPLS networks," IEEE ICC'00, NEW ORLEANS, pp. 1604–1608, June 2000.

[4] A. Elwalid, C. Jin, S. Low, and I. Widjaja, "Mate: MPLS adaptive traffic engineering," in Proceedings of IEEE/ INFOCOM, Anchorage, Alaska, April 22–26, 2001.

[5] D. Bertsekas and R. Gallager, Data Networks, Prentice-Hall, 1991.

[6] http://www.ist-tequila.org.

[7] P. Trimintzios, L. Georgiadis, G. Pavlou, D. Griffin, C. F. Cavalcanti, P. Georgatsos, and C. Jacquenet, "Engineering the multi-service internet: MPLS and IP-based techniques," ICT2001.

[8] D. Gao, Y. Shu, and S. Liu, "Delay-based adaptive load balancing in MPLS networks," ICC2002.

[9] E. Dinan, D. Awduche, and B. Jabbari, "Optimal traffic partitioning in MPLS networks," Networking, 2000.

[10] Z. H. Zhao, Y. T. Shu, L. F. Zhang, O. Yang, and H. M. Wang, "Flow-level multipath load balancing in MPLS network," in Proceedings of the IEEE 2004 International Conference on Communications, Paris, France, June 20–24, 2004.

[11] H. P. Hu, B. L. Zhang, and X. Chen, "The transmission model based active defense strategy, network information security," Beijing, pp. 346–353, 2003.

[12] The VINT Project, a collaboration between UC Berkeley, LBL, USC/ISI and Xerox PARC, "The ns manual (formerly ns Notes and Documentation)," October 2000, http://www.isi.edu/nsnam/ns/ns-documentation.html.

