Communications and Network, **2011, 3, 225-228**
doi:10.4236/cn.2011.34026 Published Online November 2011 (http://www.SciRP.org/journal/cn)

An Enhanced Secure Heuristic-Stochastic Routing Arithmetic in MPLS Network

Ying Zheng
Wuhan Maritime Communication Research Institute, Wuhan, China
E-mail: *phoolcee*2004*@yahoo.com.cn*
Received July 2, 2011; *revised September* 20, 2011; *accepted September* 30, 2011

Abstract

To improve routing security in MPLS network, base on the stochastic routing algorithm, we propose a proactive mechanism we call enhanced secure heuristic-stochastic routing (ESHSR), which brings to bear Bayesian principle, explores the existence of multiple routes and forces packets to take alternate paths probabilistically. In this paper, we investigate game theoretic techniques to develop routing policies which make interception and eavesdropping maximally difficult. Through simulations, we validate our theoretical results and show how the resulting routing algorithms perform in terms of the security/delay/drop-rate, and we contrast them with the mechanism, secure stochastic routing (SSR). We observed that our scheme makes routing more secure than traditional secure stochastic routing, as they make use of the information of detecting the other side's behavior.

Keywords: MPLS Network, Routing Security, Game Theory, Bayesian Principle, Stochastic Routing

1. Introduction

The purpose of traffic engineering (TE) [1-8] is to improve network performance through the optimization of network resources. 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. Hence it is possible to balance the traffic through the network, thus improving the network utilization and minimizing the congestion. However, 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. In "traditional" shortest-path routing protocols, the path over which a data packet travels is fairly predictable and easy to determine. Even if several paths with the same number of hops exist, routing algorithms typically select one of the possible options and utilize that same path for all packets. Indeed, a study by Zhang *et al.* [9] reveals that Internet routes are fairly persistent (e.g., often the same route between a source-destination pair persists for days; only 10% of the routes persist for a few hours or less). This makes IP networks vulnerable to packet interception and/or eavesdropping attacks. Notable exceptions to single-path routing schemes are Equal-Cost Multi-Path (ECMP) [10] and OSPF Optimized Multi-Path (OSPF-OMP) [11]. However, these algorithms were developed to increase throughput and not to make routing robust to attacks. In practice, they do not introduce unpredictability and therefore packet interception is fairly easy to achieve.

In this paper, we describe enhanced secure heuristic-stochastic routing, or ESHSR, whose main goal is to make packet interception maximally difficult. These algorithms explore the existence of multiple paths between two network nodes and route packets to minimize predictability. Routers compute all possible paths between a source-destination pair and, according to a given probability distribution, assign some probability to each next-hop. The net effect is that data packets traverse random paths on their way from the source to the destination. We should point out that, unlike the secure stochastic routing, SSR [12], we take a proactive and heuristic approach to making routing less vulnerable to attacks. In other words, according to partially detecting attacker's behavior, packets are always sent along multiple paths according to some probability.

2. Enhanced Heuristic-Stochastic Routing

We consider a MPLS network where multiple parallel LSPs exist between any given ingress LSR and egress LSR pair. The main objective is to distribute the traffic at each ingress LSR among the multiple LSPs so as to balance the load through the network and thus improving the network performance. Take the routing problem as a game between the network designer that specifies the routing algorithm and an adversary that attempt to intercept data in the network. We consider here a zero-sum game in which the designer wants to minimize the time it takes for a packet to be sent from node 1 to node n, and the adversary wants to maximize this time. To accomplish this, the adversary attempts to intercept the packet at particular links in the network. For short we say that the adversary scans link $l \in L$ when she attempts to intercept the packet at that link.

We start by considering an on-line game in which the adversary selects a new link to be scanned every time the packet arrives at a new node and makes the selection knowing where the packet is, and the player determines a new path to forward data and makes the selection knowing the link to be scanned in the previous time. For generality, we take the probability of intercepting a packet to be link dependent and denote by p_l the probability of intercepting a packet traveling in link $l \in L$, given that link l is being scanned by the adversary.

We start by considering the case in which intercepting a packet simply results in a fixed extra delay T. The routing of the packet over the network can then be regarded as a stationary Markov chain whose state $q_t \in N$ is a random variable denoting the node where the packet is before the hop $t \in \{1,2,\cdots\}$. Denoting by $a_t \in L$ the next link as determined by the routing algorithms and by $b_t \in L$ the link scanned by the adversary, we have the following transition probability function for the Markov chain:

$$P\left(q_{t+1} = q' \middle| q_t = q, a_t = \overline{qa}, b_t = l\right) = \delta_{q'a},$$
$$q \in N/\{n\}, q' \in N, \overline{qa}, l \in L, t \in \{1,2,\cdots\}.$$

The state *n* is an absorbing state, *i.e.*,

$$P\left(q_{t+1} = q' \middle| q_t = n, a_t = l_1, b_t = l_2\right) = \delta_{q'n},$$
$$q' \in N, l_1, l_2 \in L, t \in \{1,2,\cdots\}.$$

The cost to be optimized is the average time it takes to send the package from node 1 to node n and can be written as:

$$J = E\left[\sum_{t=1}^{\infty} l\left(q_t, a_t, b_t\right)\right]$$

where

$$l(q,a,b) = \begin{cases} 0, q = n \\ \tau_{\overline{qa}}, a \neq b, q \neq n \\ \tau_{\overline{qa}} + p_{\overline{qa}} T, a = b, q \neq n \end{cases}$$

To optimize this cost, for each node $\mathrm{i} \in N/\{n\}$, the player that designs the routing chooses the distribution $a(\mathrm{i}) := \{a_k : \overline{\mathrm{i}k} \in L\}$ of links to route the packet out of node i and the adversary chooses the distribution $b(\mathrm{i}) := \{b_l : l \in L\}$ of links to be scanned.

The two-person zero-sum game just defined falls in the class of stochastic shortest path games considered in [12]. In [12], it has been proved that the game exists a saddle solution point, however, In [13], the player just selects the stochastic next hop, it's too blind to do like this, and even if we do like this, it's still possible that the data can be Interception or eavesdropping by the adversary, and it's very possible to give birth to the routing loop. In our scheme, SHSR, we adjust every p_l based Bayesian principle termly, and then adjusts routing strategy to make the transmission more secure. People uses *Bayesian principle* to modify the prior probability, and get the new posterior probability constantly, here, we suppose the adversary has K types, here, the type means which link the adversary will attack, and has H possible actions, uses θ^k to represent a given type of the adversary, and a^h represents a specifically action, let $p\left(a^h \mid \theta^k\right)$ represents the prior probability that the adversary belongs to θ^k, and then, we can get:

$$\begin{aligned} \mathrm{Pr}ob\left\{a^h\right\} &= p\left(a^h \mid \theta^1\right) p\left(\theta^1\right) \\ &\quad +,\cdots,+ p\left(a^h \mid \theta^K\right) p\left(\theta^K\right) \\ &= \sum_{k=1}^{K} p\left(a^h \mid \theta^k\right) p\left(\theta^k\right) \end{aligned}$$

according to the probability formula:

$$\begin{aligned} \mathrm{Pr}ob\left(a^h, \theta^k\right) &\equiv p\left(a^h \mid \theta^k\right) p\left(\theta^k\right) \\ &\equiv \mathrm{Pr}ob\left\{\theta^k \mid a^h\right\} \mathrm{Pr}ob\left\{a^h\right\} \end{aligned}$$

now, if we observe the adversary's action a^h, we can forecast the new posterior probability that the adversary belongs to θ^k:

$$\begin{aligned} \mathrm{Pr}ob\left\{\theta^k \mid a^h\right\} &\equiv \frac{p\left(a^h \mid \theta^k\right) p\left(\theta^k\right)}{\mathrm{Pr}ob\left\{a^h\right\}} \\ &\equiv \frac{p\left(a^h \mid \theta^k\right) p\left(\theta^k\right)}{\sum_{k=1}^{K} p\left(a^h \mid \theta^k\right) p\left(\theta^k\right)} \end{aligned}$$

so the stationary Markov chain above can be re-written as:

$$J = E\left[\sum_{t=1}^{\infty} l\left(q_t, a_t, b_t\right)\right]$$

where

$$l(q,a,b) = \begin{cases} 0, q = n \\ \tau_{\overline{qa}}, a \neq b, q \neq n \\ \tau_{\overline{qa}} + p_{\overline{qa}} T, a = b, q \neq n \\ p_{\overline{qa}}(t+1) \leftarrow \dfrac{p\left(a^{h(t)} \mid \theta^{\overline{qa}}\right) p\left(\theta^{\overline{qa}}\right)}{\sum_{k=1}^{K} p\left(a^{h(t)} \mid \theta^{\overline{qa}}\right) p\left(\theta^{\overline{qa}}\right)} \end{cases}$$

$$\frac{p\left(a^{h(t)} \mid \theta^{\overline{qa}}\right) p\left(\theta^{\overline{qa}}\right)}{\sum_{k=1}^{K} p\left(a^{h(t)} \mid \theta^{\overline{qa}}\right) p\left(\theta^{\overline{qa}}\right)} = \frac{\left(p(t)\right)^{\phi}}{k + \left(p(t)\right)^{\phi}}, \phi > 0, k > 0;$$

and **Figure 1** (T represents $p(t)$, and P represents $p(t+1)$) show the relationship between $p(t)$ and $p(t+1)$, the player will detect the link that the adversary has attacked continually, and adjusts his faith about the probability that the adversary attacks every link, sequentially changes his routing strategy. It's very possible that the adversary also will adopt similar attack strategy with the player, the process that the player and the adversary change their faith about each other and strategy makes up of the game between them.

3. Simulation Results

To evaluate the routing algorithm proposed in Section 3, we simulated the network in **Figure 2**, data were transmitted from the blue point to the red point, using the ns-2 network simulator [13]. In the simulations presented, all links have propagation delay of 25 ms and bandwidth of 2Mbps. Each queue implements drop-tail queuing discipline with maximum queue size set to 100 packets for the case of the CBR simulations. All packets are 400 bytes long. The simulation time for each trial was 20 seconds. Experiments data were performed using CBR according to TCP connecting.

Similar to SSR in [14], we were interested in determining the effect of ESHSR on security, drop-rate, and packet transmission delay. We assumed here that the attacker chooses the set of links that maximizes the percentage of packets seen, *i.e.*, the worst-case scenario. Base on the on-line game, we evaluate the routing algorithm SSR and ESHSR (red line represents ESHSR, blue line represents SSR), and **Figure 3** shows the simulation results of the percentage of packets seen of them respectively. As expected, ESHSR is most secure than SSR, since according as the adversary's behavior in history, packets will be transmitted in the more secure path, not

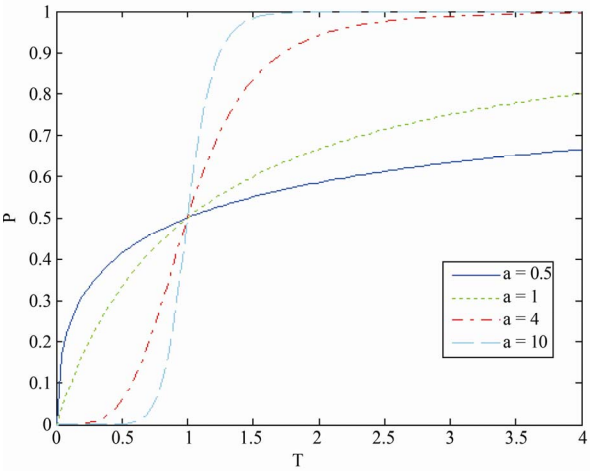

Figure 1. Relationship of (p,t).

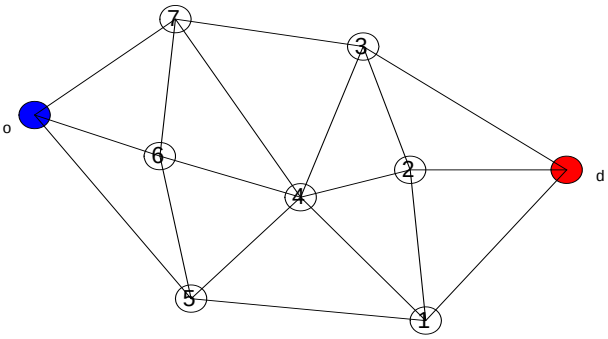

Figure 2. Network topology.

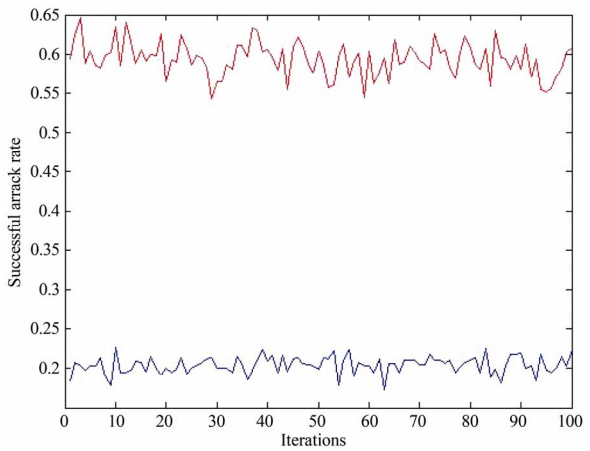

Figure 3. SAR of SSR and ESHSR.

just be transmitted along stochastic path, **Figure 4** shows the simulation results of average delay of SSR and ESHSR respectively, and **Figure 5** shows the simulation results of drop-rate of SSR and ESHSR respectively, because under ESHSR, it's more difficult be seen than under SSR, the average delay and drop-rate under ESHSR are markedly smaller than in SSR.

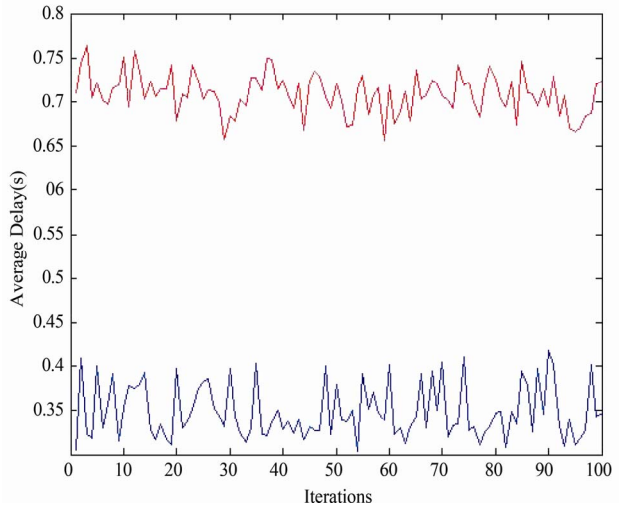

Figure 4. Delay of SSR and ESHSR.

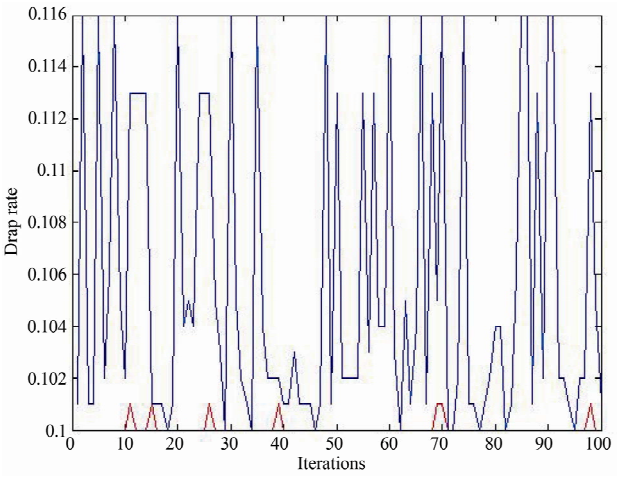

Figure 5. Drop-rate of SSR and ESHSR.

4. Conclusions

We investigated the use of ESHSR and demonstrated through simulations that it improves security. By proactively detecting the adversary's behavior in history, and in the same time, forcing packets to probabilistically take alternate paths, ESHSR mitigates the effects of interception, eavesdropping, and traffic analysis attacks. The routing policies proposed also proved efficient in average package transmission delay and drop-rate. We experimented to contrast the performance of ESHSR with SSR in [14], and the simulation Results shows that our scheme is more secure.

5. References

[1] V. Sbarma, B. Crane, K. Owens, *et al.* "Framework for MPLS-Based Recovery," *IETF RFC* 3469, February 2003.

[2] D. O. Awduche, A. Chiu, A. Elwalid, *et al.* "A Framework for Internet Traffic Engineering," *Computer Physics Communications*, Vol. 153, No. 3, 2003, pp. 52-58.

[3] I. Hussain, "Overview of MPLS Technology and Traffic Engineering Applications," *Networking and Communication*, INCC204.

[4] R. Guerin, A. Orda and D. Williams, "QoS Routing Mechanisms and OSPF Extensions [EB/OL]," 2003, pp. 12-25.

[5] Z.-H. Zhao, Y.-T. Shu and L.-F. Zhang, "Flow-Level Multipath Load Balancing in MPLS Network, Communications," *IEEE International Conference*, Vol. 2, 2004, pp. 1222-1226.

[6] F. Ricciato, U. Monaco and D. Ali, "Distributed Schemes for Diverse Path Computation in Multidomain MPLS Networks," *Communications Magazine*, *IEEE*, Vol. 43, No. 6, June 2005, pp. 138-146. doi:10.1109/MCOM.2005.1452842

[7] N. M. Din and N. Fisal, "Dynamic Resource Allocation of IP Traffic for a DiffServ-MPLS Interface Using Fuzzy Logic, Communications, APCC 2003," *The* 9*th Asia-Pacific Conference*, Vol. 1, 2003, pp. 339-343.

[8] M. Huerta and X. Hesselbach, "Application of the Theory of the Multicommodity for the Flows Distribution in MPLS Networks," *Local and Metropolitan Area Networks*, 2004, pp. 119-124.

[9] Y. Zhang, V. Paxson and S. Shenker, "The Stationarity of Internet Path Properties: Routing, Loss and Throughput," *Technical Representative*, ACIRI, May 2000.

[10] C. Hopps, "Analysis of an Equal-Cost Multi-Path Agorithmn," *RFC* 2992, 2000.

[11] C. Villamizar, "Ospf Optimized Multipath (Ospf-Omp)," *Draft-Ietf-Ospfomp*-03, June 1999, p. 46.

[12] S. Bohacek, J. P. Hespanha, K. Obraczka, Lee Junsoo and L. Chansook, "Enhancing Security via Stochastic Routing, Computer Communications and Networks," *Proceedings of the* 11*th International Conference*, 14-16 October 2002, pp. 58-62.

[13] J. P. Hespanha and S. Bohacek, "Preliminary Results in Routing Games," *Proceedings of the* 2001 *American Control Conference*, June 2001.

[14] 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

