Defense against DoS attacks by multipath routing using the ACO algorithm

Takuya Shindo$^{1a)}$, Tomotaka Kimura$^{2b)}$ and Takefumi Hiraguri$^{1c)}$

$^1$ Department of Electrical and Electronics Engineering, Nippon Institute of Technology
4-1 Gakuendai, Miyashiro-machi, Minami-saitama-gun, Saitama, 345-8501, Japan

$^2$ Faculty of Science and Engineering, Doshisha University
1-3 Tatara Miyakodani, Kyotanabe-shi, Kyoto 610-0394, Japan

$^{a)}$ t-shindo@nit.ac.jp, $^{b)}$ tomkimur@mail.doshisha.ac.jp, $^{c)}$ hira@nit.ac.jp

Abstract: In recent years, the number of malicious denial-of-service (DoS) attacks on network servers has increased. Malicious traffic reaches the server through multiple routers, which results in heavy load on many links; thus, load suppression of malicious traffic is important. Therefore, we propose a throughput suppression control scheme using multiple communication routes obtained by ant colony optimization (ACO). The ACO algorithm is used to distribute the routing path. The effectiveness of this proposed scheme is confirmed through computer simulations, which shows that the throughput can be adjusted by the selection probability of the longest route and the number of available routes.

Keywords: Optimization problem, Dijkstra’s algorithm, Ant colony optimization, Routing, Software-defined Network

Classification: Network system

References

[1] H. Muto and N. Sato, “Active DoS attack measures by bandwidth control,” IPSJ SIG Technical Report, Nov. 2008.

[2] Z. Chao-Yang, “DoS attack analysis and study of new measures to prevent,” Proc. of 2011 International Conference on Intelligence Science and Information Engineering, 2011.

[3] M. Dorigo and L. M. Gambardella, “Ant colony system: a cooperative learning approach to the traveling salesman problem,” IEEE Transactions on Evolutionary Computation, vol. 1, no. 1, pp. 53–66, Apr. 1997.

[4] S. Ihara and T. Imaizumi “Consideration of Efficient Multipath Routing under Software Defined Networking,” The Institute of Electronics, vol. 17, L–13, 2014.

[5] H. Sswai, “Emegence and Analysis of a New Small – World Network,” JSAI Technical Report SIG–DOCMAS–B101 –1.

[6] A.-L. Barabási and R. Albert, “Emergence of Scaling in Random Networks,” Science, vol. 286, no. 5439, pp.509–512, Oct. 1999.
1 Introduction
With the widespread use of the Internet, traffic volume has increased tenfold in the last five years, which includes malicious traffic, such as denial-of-service (DoS) attacks [1][2]. In DoS attacks, attackers send excessive connection requests to a server to crash the server. In addition to crashing the server, DoS attacks can also deplete network resources because of the large amount of traffic flow into the network. Specifically, malicious traffic reaches the server through multiple routers, which results in heavy load on many links. Therefore, load suppression of malicious traffic is a serious technical challenge.

In this study, to solve the problem of DoS attacks, we propose a throughput suppression control scheme using multiple paths searched by the ant colony optimization (ACO) algorithm [3]. The ACO algorithm is an optimal path search method based on the foraging behavior of ants; it is generally used for shortest path optimization problems in networks. However, in the proposed method, multiple long paths are searched by reversing the heuristic information. Malicious users with heavy load flows are assigned the obtained long paths. Thus, the proposed method mitigates network congestion due to DoS attacks. Computer simulations are performed to verify the effectiveness of the proposed scheme.

2 Conventional route selection issues and the proposed method
The proposed method requires dynamic changes in the communication path. Therefore, a software-defined network (SDN) [4] is chosen as the operating environment. An SDN switch and SDN controller can communicate in an SDN. An SDN switch sends statistical information, such as amount of bandwidth being used by each IP address, to the SDN controller and can detect malicious users on the SDN controller. This requires no new software or special equipment to be installed on the server.

General users use the shortest route, as shown in Fig. 1a. In the proposed method, multiple routes, including long routes, are assigned to malicious users using a lot of bandwidth, as shown in Fig. 1b. Multiple routes result in different packet arrival times, which may result in lost packets or discrepancies in the order of packets. In other words, throughput can be suppressed by route control in which several routes are combined. The proposed method does not distinguish between users who launch DoS attacks and heavy users who use a lot of bandwidth. Therefore, the proposed method can be applied to all users who are using a lot of bandwidth; such users are assigned multiple routes.

Multiple paths are generated by ACO, which is one of the optimal solution search methods. The ACO algorithm is typically used to probabilistically search for the shortest path based on the foraging behavior of ants. However, in the proposed method, ACO is used to search for multiple longest paths. The longest path with no loops is a feasible solution. The ACO algorithm can generate routes equivalent to the number of ants in the algorithm. Its characteristics are very useful for generating multiple routes for the proposed scheme.
The outline of the conventional ACO algorithm is described as follows.

1. The ants and pheromones are initialized. \( t = 0 \).
2. Initial pheromone information is provided to all edges.
3. Using pheromone information \( \tau_{i,j} \) and heuristic information \( \eta_{i,j} \), when ant \( k \) stays at node \( v_i \) at time \( t \), the probability of selecting node \( v_j \) at time \( t + 1 \) is calculated as follows.

\[
p_{i,j}^k(t + 1) = \frac{\tau_{i,j}^a \eta_{i,j}^b}{\sum_{l \in \mathcal{N}_{ik}} \tau_{i,l}^a \eta_{i,l}^b},
\]

where \( \mathcal{N}_{ik} \) denotes the set of non-visited nodes that are adjacent to node \( v_i \), and \( \alpha \) and \( \beta \) denote the importance of pheromone information and heuristic information, respectively \((\alpha, \beta > 0)\). \( \eta_{i,j} \) is set to \( 1/d_{i,j} \), where \( d_{i,j} \) denotes the distance between node \( v_i \) and node \( v_j \).

4. The pheromone secreted by each ant in step 3 is calculated using Eqs. (2) and (3), and pheromone information is added to the network.

\[
\tau_{i,j} = (1 - \rho)\tau_{i,j} + \sum_{k=1}^{M} \Delta \tau_{i,j}^k,
\]

\[
\Delta \tau_{i,j}^k = \begin{cases} 1/L^k, & \text{if } (v_i, v_j) \in T^k \\ 0, & \text{otherwise} \end{cases}
\]

**Fig. 1:** General methods and proposed methods of routing.
where \( T^k \) is the route created by the ant \( k \), \( L^k \) represents the route length, \( M \) denotes the total number of ants, and \( \rho \) is the parameter representing pheromone evaporation.

5. The pheromones in the network are evaporated according to \( \rho \).

6. \( t := t + 1 \). Return to step 3 if the end condition is not met.

Figure 1c illustrates an example of selecting multiple routes to use from generated routes by 10 ants. For example, when using one route, the shortest route is selected. When using two routes, the shortest and the longest route are selected. In the case of using three or more routes, routes with a large cost differences are selected. When sending packets through multiple routes, the route to be used is determined stochastically. If a malicious user’s throughput is still high when the routes are assigned, additional routes are added. Packet arrival times are distributed by such stochastic selection.

3 Evaluation conditions

In general, the packet arrival time is almost constant when the same route is being used; in addition, the variance is almost zero. When multiple routes are used, the packet sent earlier uses the longest route and the packet sent later uses the shortest route, which leads to packet loss. In the proposed method, throughput is controlled by intentionally causing packet loss. For the proposed method, the time required for arrival is desired to be uniformly distributed for general users. On the other hand, the packet arrival time is distributed for malicious users. After the packets are sent to multiple assigned routes, the variations in time taken for each packet to be received are checked. Moreover, the order of packet arrival is disturbed when multiple routes with large cost differences are used. Therefore, packet loss occurs and throughput decreases. The experiment verifies the effect of the probability of the selection of the longest route and the number of multiple routes on throughput.

In this study, simulations were performed using two types of networks: the Watts-Strogatz (WS) model [5] and Barabási-Albert (BA) model [6]. The WS model is a random graph generation model with small-world properties. On the other hand, the BA model is a random graph generation model with scale-free properties. A small-world network is based on the phenomenon that the diameter of the network becomes smaller when a small number of random links are introduced into the lattice network. In small-world network, several nodes can be reached from other nodes in a small number of hops or steps. A scale-free network is a network whose degree of distribution follows a power law, at least asymptotically.

In the experimental scenario, there was one DoS attack source and four general users accessing one node. The DoS attack source used the user data-gram protocol (UDP), typically used in DoS attacks, and a bandwidth of 100 Mbps. General users used the transmission control protocol (TCP). The number of nodes was 1000, each node’s buffer was 500, \( P = 0.1 \) for the WS
model, and the perfect graph $n = 10$ for the BA model. $P = 0.1$ indicates a 10% probability of changing the edge. $n$ represents the initial number of nodes in network generation by the BA model. The starting and goal nodes were randomly selected for communication. The shortest route was generated by the Dijkstra’s algorithm and the remaining routes were generated by ACO. The network parameters are listed in Table Ia. The parameters for ACO are shown in Table Ib. In ACO, $\alpha$ is set to be larger than $\beta$ to find a long route quickly. In the experiment, simulations for 3, 5, 10, and 20 routes were performed.

4 Simulation results

Figure 2 shows the result of probabilistic selection of several routes including the longest route. The horizontal axis represents the probability that the longest route will be selected; the vertical axis represents the throughput. Figures 2a and 2c show the throughput of the DoS attack source. The throughput of the DoS attack source can be suppressed by the number of routes to be used and the selection probability of the longest route regardless of the network characteristics. In addition, stable throughput for general users is confirmed as shown in Fig. 2b and Fig. 2d.

Figures 2e and 2f show an example of the bandwidth utilization of each node, where 10 routes are used and the probability of selecting the longest route is 50%; the horizontal axis represents degree. Because there are no hub nodes in the WS model, the degree is smaller than that in the BA model.

From these results, the route utilization of the low degree node is confirmed. Therefore, diverse routes have been generated and selected with distributed packet arrival times.

5 Conclusions

In this study, we proposed a method to control the throughput using multiple communication routes to solve the problem of DoS attacks. The proposed throughput control was verified by numerical experiments. In the experiments, the probability of the selection of the longest route was changed and that of using each node was confirmed. Experimental results showed that the throughput changes if the probability of the route selection is changed.

---

Table I: Simulation conditions

| (a) Network Parameters | (b) ACO Parameters |
|------------------------|--------------------|
| Number of packets | 1000 |
| Packet size | 1500 bits |
| Number of nodes | 1000 |
| Bandwidth | 100 Mbps |
| Packet loss rate | 0.001 % |
| Number of trials | 10 times |
| Buffer | 500 |
| Number of routes | 3, 5, 10, 20 |
| Time to live | 64 hops |
| Window size | 32000 bytes |
| Distance between nodes | 100 - 300km |
| Number of ants | 20 |
| Evaporation rate | 0.8 |
| $\alpha$ | 1.0 |
| $\beta$ | 0.7 |
When the probability of the longest route is changed, the throughput changes depending on the number of routes. Therefore, throughput can be adjusted by the selection probability of the longest route and the number of available routes. When the probability of using the longest route increases, the usage rate of nodes in multiple routes increases. Therefore, increasing the probability of using the longest route may increase the load on the network. Accordingly, the probability of using the longest route should preferably be 50%. In future work, we will tackle the problem of implementing this in real machines.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number 20H04184.