ABSTRACT
In general, Network attack should be prohibited and information security technology should contribute to the improvement for trust of network communication. Network communication is based on IP packets which are standardized by international organization. Therefore, Network attack does not function without following the standardized manner. Hence, Network attack also leaks adversaries’ information in their IP packets. In this paper, we propose a new Network attack strategy which counter-attacks adversary. We collect and analyze IP packets from adversary, and derive network topology of adversary. The characteristics of topology can be analyzed by the eigenvalue of topology matrix. We observe the influence by which the attack to topology gives it to changes of characteristic, and choose most suitable network attack strategy. In this paper, we propose two kinds of attack scenarios and three types of tactics. And we show an example attack using actual data of adversary.

KEYWORDS

1 INTRODUCTION
Network attack is not special threat today, and its purpose and technologies evolve complicatedly. APT (Advanced Persistent Threat) is seen frequency now a days, and organization of adversaries is becoming normality. The organization of adversary disperses worldwide or is maldistributed in a specific area (such as country). The former has a possibility that it belongs to the worldwide terrorism organization. On the other hand, the latter has a high possibility that the organization gets the government support. In this paper, we focus on the activity of adversaries who exist in specific country.

In general, we believe that Network attack should be prohibited action. However, Network attack also uses IP packet which is determined by the international standardized group (ISO and IETF[1]). as the result, Network attack leaks the information concerning to the action of adversary at the same time. So, there are Honey pot project[2] and Darknet Monitoring[13] in the security technology based on the fact. These are used for an analysis of Network attack technologies and observation of large scale attacks. So we can see these security technologies as passive observation of Network attack trend. On the other hand, in this paper, we also use the information brought by IP packets, from adversaries to make strategy for counter-attack.

As already mentioned above, we focus on the activity of adversaries who exist in specific country. The IP packets from adversaries have information of network infrastructure (such as topology) in the specific country. Therefore, we analyze the topology of specific country by collecting and analyzing IP packets from there. The characteristic of topology can be analyzed by the eigenvalue of matrix which is derived from the topology. The analysis method using eigenvalue of topology is developing as Network Dynamics. By using these eigenvalues, we propose a method of choice of the most suitable strategy of counter-attack. In addition, we focus on the fact that Network attack changes the topology and its characteristics. In this paper, we propose two kinds of attack scenarios and three types of tactics, and show an example attack. The example attack is demonstrated using actual results of our Darknet Monitoring. Since our proposal scheme and method have some sensitive topics, note that the some details of example attack are omitted. Some topological analysis
were applied to Network security in previous studies. But, for example paper[3], all of them refers to defense technology and there is no result applied to attack technology. In this point, our paper is very epoch-making one since we focus on the counter-attack using topological analysis.

2 PRELIMINARIES

The characteristics of network can be estimated by topological analysis. The topology can be expressed by some methods. In this paper, we take two kinds of matrices; Adjacency matrix[4] and Laplacian matrix[5]. The eigenvalue of each matrix shows the characteristic of topology. In this paper, we focus on two types of characteristics; “Spread speed” and “Convergence”. “Spread speed” denotes the characteristic which shows easiness of communication. “Convergence” denotes the characteristic which shows easiness of settling of information. As an example of previous works using eigenvalues of topology, there is a chain-reaction bankruptcy analysis of bank-transaction [14]. In this work, They derived some topologies of bank-transactions and calculate their eigenvalues. Using these eigenvalues, they made it clear that only bankruptcy of megabank is not always the cause of the financial crisis.

2.1 Adjacency matrix

Let $G$ be undirected topology with $n$ nodes. Then $G$ can be expressed as $n \times n$ Adjacency matrix $A$. Let $A_{i,j} (1 \leq i, j \leq n)$ be an element of matrix $A$ as follows.

$$A_{i,j} = \begin{cases} 1 & \text{if } i \text{ is adjacent to } j, \\ 0 & \text{if } i \text{ is not adjacent to } j. \end{cases}$$

(1)

Since characteristic equation is $n$-th degree, eigenvalue can have different $m(1 \leq m \leq n)$ values. Let $\lambda_{\text{max}}(A)$ be the maximum value of $\lambda$. The value of $\lambda_{\text{max}}(A)$ shows the characteristic of the connection density among hub-nodes. Thus it indicates the characteristic of “Spread speed” of topology.

2.2 Laplacian matrix

The topology $G$ also can be expressed by Laplacian matrix $L$. Let $L_{i,j}(1 \leq i, j \leq n)$ be an element of matrix $L$.

$$L_{i,j} = \begin{cases} d_i & \text{if } i = j, \\ -1 & \text{if } i \text{ is adjacent to } j, \\ 0 & \text{if } i \text{ is not adjacent to } j. \end{cases}$$

(3)

where $d_i$ denotes the degree of $i$-th node. The eigenvalues of $L$ is also derived by the same way of Adjacency matrix shown as eq.(2). So we have $m(1 \leq m \leq n)$ different values for $L$ as follows.

$$0 = \lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_m$$

(4)

The minimum value $\lambda_1$ is always equals to zero. The second minimum value $\lambda_2 > 0$ is determined as algebraic connectivity. When $\lambda_2$ has large value, the topology has high connectivity. The maximum value $\lambda_m$ shows the difficulty caused the connection delay. The synchronization of topology can be evaluated by the ratio $R = \lambda_2/\lambda_m$. When $R$ has large value, it indicates the characteristic of “Convergence” of topology.

2.3 Example analysis

We show an example analysis using seven nodes topology shown in Fig1. From this fig-
The Adjacency matrix $A$ is:

$$A = \begin{pmatrix}
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0
\end{pmatrix} \quad (5)$$

By using eq. (2), we have the following:

$$\lambda_1(A) = -2.358 \quad \lambda_5(A) = 0.000$$
$$\lambda_2(A) = -1.199 \quad \lambda_6(A) = 1.199$$
$$\lambda_3(A) = 0.000 \quad \lambda_7(A) = 2.358$$
$$\lambda_4(A) = 0.000$$

As the result, we have $\lambda_{\text{max}}(A) = 2.358$. In the same way, from Eq1, we have the following Laplacian matrix $L$.

$$L = \begin{pmatrix}
1 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 1 & -1 & 0 & 0 & 0 & 0 \\
-1 & -1 & 4 & -1 & 0 & -1 & 0 \\
0 & 0 & -1 & 2 & -1 & 0 & 0 \\
0 & 0 & 0 & -1 & 3 & -1 & -1 \\
0 & 0 & -1 & 0 & -1 & 2 & 0 \\
0 & 0 & 0 & 0 & -1 & 0 & 1
\end{pmatrix} \quad (6)$$

From this matrix, we have the following eigenvalues:

$$\lambda_1(L) = 0.000 \quad \lambda_5(L) = 2.000$$
$$\lambda_2(L) = 0.514 \quad \lambda_6(L) = 3.836$$
$$\lambda_3(L) = 1.000 \quad \lambda_7(L) = 5.314$$
$$\lambda_4(L) = 1.336$$

Then we have $R = \lambda_2(L)/\lambda_7(L) = 0.1237$.

3 BASIC IDEA

3.1 Background

“Darknet Monitoring” is one of analysis methods for Network attacks. Darknet is the unused IP address-space among global IP address that the organization holds. It is abnormal situation that there are accesses to Darknet from outside, because the IP address of Darknet does not execute any network services. So we can see the access to Darknet as malicious act. Therefore the analysis of Darknet access (Darknet Monitoring) is regarded as the detection method for network attacks. There are many projects of world scale Darknet Monitoring, such as Norse[6], Nicter[7], and so on.

All network attack is based on IP packets. Each IP packet has many information in its header; protocol, source IP address, destination IP address, timeout, the parameters decided by OS and so on[1]. Since the packets arrived Darknet also has such information, we can get information of adversary by analyzing them. The actual attacks are executed via springboard PCs, it is difficult to specify the adversary’s true IP address. However, even if springboard PC is intentional or accidental, in this paper, we suppose that springboard PCs which execute persistent access to Darknet are adversaries. Note that there are many methods which detect springboard PCs[15][16][17].

3.2 Our strategy

“traceroute” is the command which shows the route to given IP address[8][18][9]. As shown above, IP address and packet have many information of adversary. Our purpose is to derive network topology attacking us. In our strategy, malicious IP addresses monitored in Darknet are classified adversary group by analyzing their packets. As a result, we can collect different malicious IP addresses from same country. Then we execute “traceroute” them, we estimate the topology of the target country. We call such topology malicious topology. However, the results of “traceroute” do not show all IP address on the route. Fig2. shows an example result of “traceroute”. In this figure, “* * *” denotes unknown IP address. It is occurred when the server exists, but it does not open its IP address. To estimate the malicious topology, we treat such unknown IP address as they are, and make temporary topology. Fig3.(upper) shows an example of tem-
Fig 2. Example result of "traceroute"

<table>
<thead>
<tr>
<th>IP Address</th>
<th>RTT (ms)</th>
<th>RTT (ms)</th>
<th>RTT (ms)</th>
<th>RTT (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXX.XXX.XXX</td>
<td>0.819</td>
<td>0.821</td>
<td>1.140</td>
<td></td>
</tr>
<tr>
<td>YYY.ZZZ.ZZZ</td>
<td>4.779</td>
<td>4.797</td>
<td>4.767</td>
<td></td>
</tr>
<tr>
<td>AAA.BBB.CCC.DDD</td>
<td>13.249</td>
<td>13.249</td>
<td>13.249</td>
<td></td>
</tr>
<tr>
<td>BBB.CCC.DDD</td>
<td>13.247</td>
<td>13.240</td>
<td>13.245</td>
<td></td>
</tr>
<tr>
<td>AAA.BBB.CCC.DDD</td>
<td>125.808</td>
<td>125.808</td>
<td>125.808</td>
<td></td>
</tr>
<tr>
<td>XXX.XXX.XXX</td>
<td>135.318</td>
<td>135.318</td>
<td>135.318</td>
<td></td>
</tr>
<tr>
<td>XXX.XXX.XXX</td>
<td>135.407</td>
<td>135.394</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fig 3. Driving malicious topology

3.3 Outline of attack strategy

The threat scenario of Network attack is complicated and various, in this paper, we focus on following two.

Scenario-1. Spread of malware and disinformation

Scenario-2. Concentration and confusion of information sharing

Scenario-1 is generally easy to understand and typical case of Network attack, so we omit the details. The purpose of Scenario-2 is to generate the differentials in information sharing between target area and others and make confusion. This scenario is also based on the one of important characteristics of Internet technology such as immediacy of information sharing. By using this characteristics, we can generate a threshold of diffusion of information. This scenario is similar to spreads of rumor (and malware such as Scenario-1), but it is different from these scenarios in the point that the difference in the spread of different informations are generated.
The effectiveness of these attack scenarios can be decided by the characteristics of target network topology. Therefore the effectiveness of Scenario-1 is related to the characteristic of “Spread of speed” and Scenario-2 is related to “Convergence” respectively. In the simple way, the attacker chooses whether attack scenario is more effective by the analysis of target topology.

On the other hand, Network attack has various tactics such as DDoS attack, XSS, down of services constructing rogue servers, and so on. These tactics have influence on the topology and can change its characteristics. Therefore the attacker can choose attack scenario and discuss its effectiveness by selecting tactics.

In this paper, we consider following three tactics and its effectiveness against change of topological characteristics.

Tactics-1. Down of server
Tactics-2. Construction of agent server
Tactics-3. Combination of Tactics-1 and Tactics-2

Tactics-1 can be achieved by the well-know attack such as DDoS attack. Tactics-2 can be achieved by using IP address which are not well-managed.

There are some problems such as slow down of communication speed and feasibility with attack execution. These problems influence effectiveness and feasibility of strategy, however, they are individual problems every actual target topology, so we omitted them in this paper. And the choice and location of server have big influence on effectiveness of strategy. In this paper, we analyze the optimal attack effectiveness by brute force search, so, we limits the size of target topology with in our computer can analyze (maximum 100 nodes).

### 3.4 Example attack

In this section, we show an example attack against the topology shown in Fig.1. The initial values are $\lambda_{max}(A) = 2.358$ and $R = 0.1237$ (see Section 2.2). The conditions of each Tactics are as follows.

Tactics-1: The number of attack target server is one.

Tactics-2: The number of agent server is one. And the number of links from agent server is not restricted.

Tactics-3: The number of attack target node and agent server is each one. And the number of links from agent server is two.

Fig4. shows the result of Scenario-1. From these results, we can find that Tactics-2 is most effective but it is obviously worthless. Tactics-3 is the most realistic case. Tactics-1 shows a little unexpected result. The value of $\lambda_{max}(A)$ of Tactics-1 is smaller than initial value, we can conclude that Tactics-1 is useless in the attack Scenario-1 against the topology shown in Fig1. In Scenario-1, the best results are decided uniquely without Tactics-3. In Tactics-3, ten kinds of best result are derived (total 28 patterns). Another three of them are shown in Fig5, but all of them has same attack target. Fig6. shows the results of Scenario-2. From these results, we can find that Tactics-3 is most effective and realistic case. Tactics-2 which is expected as most powerful attack is lesser effect than Tactics-3. Tactics-1 can expect more effective compared with Scenario-1. Note that all result is decided uniquely.

### 4 PROPOSAL ATTACK METHOD

The purpose of our proposal attack method is to derive the most effective attack strategy or to estimate the effectiveness each attack strategy. The attack strategy is defined as the combination of scenario and tactics shown in Section 3.3. Since we have two kinds of scenario and three types of tactics (we have six patterns of attack strategy). The flow of our proposal method is as follows.

1. Collect IP addresses from the target area (target IP group).
2. Execute `traceroute` command for target IP group.
3. Estimate the topology of target area.
Step-4. Execute simulation of Tactics-1 ~ Tactics-3.

Step-5. Choice the scenario and tactics (strategy).

In our experiment (see Section 5), we use Darknet Monitoring for Step-1. It is desirable to execute Step-2 from more than one different place. And for even same IP address, it is desirable to execute Step-2 changing time and a day of week sometimes. Because the network traffic will change by time and a day of week, so there is possibility that network routing also changes. As a result, it is possible to get more new different IP address, so deriving of more precise topology is helped. In Step-3, we take the method shown in Section 3.2. An example execution of Step-4 and Step-5 are shown in Section 3.4. The computational complexity of Step-4 is determined by the number of nodes in target topology ($N$), the number of attack target nodes ($n$), the number of agent servers ($m$) and the number of links from each agent server ($\ell$). Thus we can calculate computational com-
complexity for each tactics as follows.

\begin{align*}
\text{Tactics-1:} & \quad C_1 &= N C_n m \quad \text{\normalfont (7)} \\
\text{Tactics-2:} & \quad C_2 &= \sum_{i=1}^{m} (N+i-1) C_\ell \quad \text{\normalfont (8)} \\
\text{Tactics-3:} & \quad C_3 &= N C_n \times \sum_{i=1}^{m} (N+i-1) C_\ell \quad \text{\normalfont (9)}
\end{align*}

Note that we derive computational complexity as the number of calculation of eigenvalues.

5 EXPERIMENTS

In this section, we show our proposal method based on the Darknet Monitoring in our organization while March 1st ~ 21st, 2013.

5.1 Step-1: Darknet Monitoring

In the monitoring period, we recorded total 1,654,925 of malicious access for our Darknet. Among these access, there are 1,093,859 different IP addresses. Using the country information of IP address, the access numbers of each countries are summarized as Table.1. In this paper, we focus on Country-Q. By our Darknet Monitoring, 3,674 different IP address are recorded.

\begin{table}[h]
\centering
\caption{Access numbers of each countries}
\begin{tabular}{|l|c|c|}
\hline
Country & access number & IP addresses \\
\hline
Total & 1,654,925 & 1,093,859 \\
Country-A & 757,775 & 553,689 \\
Country-B & 75,785 & 53,390 \\
Country-C & 3,896 & 2,089 \\
Country-Q & 8,728 & 3,674 \\
\hline
\end{tabular}
\end{table}

5.2 Step-2: Traceroute

We executed \texttt{traceroute} for 3,674 different IP addresses. The parameter of \texttt{traceroute} is as follows.

\texttt{traceroute -I n -m 30 IP\_address}

Using this command, we can get 30 IP addresses on the route for target IP addresses. Note that we focus on the IP addresses in the Country-Q. For the restriction in our network environment, we execute \texttt{traceroutes} from only single start point, and we did not execute them changing time and a day of week. As the result, we got 2,119 of new IP address in Country-Q. We omit IP address which does not exist in result of \texttt{traceroute} or isolate in resultant of estimation of topology. Thus we have 2,119 nodes which is smaller than initial recorded 3,674 IP addresses. We needed about 2 days for this process.

5.3 Step-3: Estimation of topology

Using the estimation method shown in section 3.2 for the resultants of \texttt{traceroute}, we have the topology of 2,119 nodes with 3,819 links shown in Fig7. But this topology is too large for our computer environment. Therefore, we limited to the topology in the metropolitan area.
in Country-Q using the information of IP locator and whois. As the results, our target topology is derived as Fig8.

5.4 Simulation of Tactics

The initial values of target topology are $\lambda_{\text{max}}(A) = 10.0785$ and $R = 0.005487$. The parameters of each tactics are as follows.

\[ N = 100, \quad n = 100, \quad m = 1 \quad \text{and} \quad \ell = 2 \]

The computational cost and simulation time for the each scenario and tactics are summarized in Table2. And the specification of our computer environment is shown in Table3.

5.5 Results and evaluations

The attack results show in Fig9, Fig10 and Table4. We can find following facts from these results.

5.5.1 A result of no Tactics becomes smaller than the initial value.

We can conclude that our method against Country-Q can guarantee that the attack results do not disadvantageous about attack scenario execution. However, note that Scenario-1 with Tactics-1 can not be expected as effective attack.

On the other hand, for example, when two kinds of attack scenario is executed at once, we can choose the attack target for one scenario which will not disturb another scenario. Therefore, from this fact, we can expect choice of the attack target which can achieve more one attack scenario at the same time.

5.5.2 Tactics-3 is the most powerful.

It is obvious that the condition of Tactics-3 for attacker is most advantageous. More than 10% of improvement is estimated compared with initial value of Scenario-2. However, there are some big problems such as huge computational cost, feasibility for realistic attack and so on. These problems are discussed in Section 7.

5.5.3 Derivation Tactics-3.

Also mentioned above, the computational cost for deriving Tactics-3 is huge. To solve this problem, we try to derive Tactics-3 using the results of Tactics-1 and -2. In Scenario-1, we will be able to derive Tactics-3 using them. Because the target server is same as Tactics-1 and the generated links as same as Tactics-2. Our another computer experiments also show the same results. So we can conclude that Tactics-3 for Scenario-1 can be derived the results of Tactics-1 and -2. But, we can not find out any relations among these
\[ \lambda_{\text{max}}(A) = 10.0785 \]
\[ R = 0.005950 \]

Fig9. [Scenario-1] Spread of malware and disinformation (100 nodes)

\[ \lambda_{\text{max}}(A) = 10.1152 \]
\[ R = 0.006329 \]

Fig10. [Scenario-2] Concentration and confusion of information sharing (100 nodes)

Table 4. \( \lambda_{\text{max}}(A) \) and \( R \) of Initial topology and each Tactics

<table>
<thead>
<tr>
<th>Network</th>
<th>( \lambda_{\text{max}}(A) )</th>
<th>( R )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial topology</td>
<td>10.0785</td>
<td>0.005487</td>
</tr>
<tr>
<td>Tactics-1</td>
<td>10.0785</td>
<td>0.005950</td>
</tr>
<tr>
<td>Tactics-2</td>
<td>10.1152</td>
<td>0.006329</td>
</tr>
<tr>
<td>Tactics-3</td>
<td>10.1152</td>
<td>0.007122</td>
</tr>
</tbody>
</table>

results in Scenario-2.
We conclude that it is efficient to execute separately in Scenario-2. Development of the method to reduce the necessary computational cost for Tactics-3 in Scenario-2 is our future work.

5.5.4 Choice of attack strategy.

From Table 4, we should take Tactics-3 for both Scenarios on the attack to Country-Q. In Section 6, we check the effectiveness of each Tactics by computer simulations.

6 EXPERIMENT OF SPREAD OF MALWARE AND DISINFORMATION

6.1 Relevance between the eigenvalues and the information diffusion.

From the view point of analysis of Network dynamics, the maximum eigenvalue of topology is determined by the total number of nodes and links[19]. Our proposal attack method changes number of nodes and links, therefore, the maximum eigenvalue can be improved to be easy to attack. So, it is necessary to confirm that it becomes advantageous to attack comparing with the Initial topology. Note, when the numbers of nodes and links are not changing, it is clear to become aggressive advantage by our strategy. In the experiments shown in Section5;

- The condition of Tactics-1 decreases the number of nodes one and decrease the number of links more than or equal to one.
- The condition of Tactics-2 increases the number of nodes one, and increases the number of links more than one.
The condition of Tactics-3 is same number of nodes and changes the number of links. In the conditions above, we executed the infection simulation proposed in [19]. The evaluation value $R$ on Scenario-2, each value of Tactics is increased more than 10% to the value of Initial topology. On the other hand, the evaluation value $\lambda_{\text{max}}(A)$ on Scenario-1, the increment is about 1%. Therefore we checked such effectiveness of Scenario-1, using infection simulation following the paper [20]. We observed the number of spread steps with 50% of infection probability. We executed exhaustive search for the start points which makes the least number of steps (best-target) and the maximum ones (worst target). The stop condition of experiment is 90% of infection. In the search, we take average of 100 times of experiment for each node.

6.2 Experimental result

The result of infection simulation is summarized in Table 5. The node 20 is chosen as the best-target by all result of simulation except Tactics-2. In fact, the node 20 has 19 links in Initial topology and Tactics-1, and it is the maximum order node. Note that the same node 20 has 20 links in Tactics-2 and Tactics-3 since the attack of setting of agent server generates one new link on the node 20. From these results, we can confirm that Tactics-3 is the most powerful and the resultant topology of Tactics-3 has the second most number of links. Therefore, we can expect that the resultant topology which has more links is effective for Scenario-1.

In the result of Tactics-2, the resultant topology has most links and nodes among all simulation. It results second best steps (7.10), it has some following interest features.

- Average number of links in Tactics-3 is almost same as Initial topology.
- Node 20 has the most links (20). This is the same result as Tactics-3.
- Best-target is node 19 whose number of links is 17. It is the third node with a lot of links.

From above, we conclude that it is not appropriate to compare the result of Tactics-2 and others simply. Our proposal method conclude that Tactics-3 is the best, however, we need to analyze the relation between evaluation value of $\lambda_{\text{max}}$ and the number of links and nodes. This is our future works.

In the case of worst-target, Tactics-3 is most effective. Thus, the validity of our conclusion could be confirmed.

7 DISCUSSION AND CONCLUSION

In this paper, we propose a Network attack method using topological analysis and show an example derivation of attack strategy using Country-Q. Since Network attack bothers usual operation, we think such action should be stopped complicatedly. However, Network attack also brings adversary’s information, so we should observe them effectively. Our proposal method is based on these facts.

In this paper, we can only derive the choice of attack target and effective attack scenario. Our proposal method does not enable to make an estimation of the actual attack effect. To make proposal method a practical strategy, we need to solve following problems.

Problem 1. Parameterization of attack tolerance of each nodes.

In our method, the security level of all nodes is same. In particular, we do not set any attack method (such as DDoS, XSS and so on), so the security level is set zero. But in the real network operation, each node has own role (such as router, Web server, Mail server, clients and so on). Therefore each node has own security level according to its role. In addition, even if same role, the security level is different whether it is located in backborn network or end point. As a result, security level is various and it is not realistic to set in unifying way. To solve this problem, we expect analysis methods of virus infection and Network dynamics[11]. And IP locater and geopolitical...
Table 5. $\lambda_{max}(A)$ and number of spread steps of Initial topology and each Tactics

<table>
<thead>
<tr>
<th>Network</th>
<th>Node</th>
<th>Link</th>
<th>$\lambda_{max}(A)$</th>
<th>step(best-target)</th>
<th>step(worst-target)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial topology</td>
<td>100</td>
<td>187</td>
<td>10.0785</td>
<td>7.13(20)</td>
<td>13.38(64)</td>
</tr>
<tr>
<td>Tactics-1</td>
<td>99</td>
<td>186</td>
<td>10.0785</td>
<td>7.24(20)</td>
<td>12.92(39)</td>
</tr>
<tr>
<td>Tactics-2</td>
<td>101</td>
<td>189</td>
<td>10.1152</td>
<td>7.10(19)</td>
<td>13.39(64)</td>
</tr>
<tr>
<td>Tactics-3</td>
<td>100</td>
<td>188</td>
<td>10.1152</td>
<td>7.05(20)</td>
<td>12.89(75)</td>
</tr>
</tbody>
</table>

Table 6. The number of links of target nodes of Initial topology and each Tactics

<table>
<thead>
<tr>
<th>Network</th>
<th>node(links)</th>
<th>node(links)</th>
<th>average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial topology</td>
<td>20(19)</td>
<td>64(1)</td>
<td>1.870</td>
</tr>
<tr>
<td>Tactics-1</td>
<td>20(19)</td>
<td>39(1)</td>
<td>1.879</td>
</tr>
<tr>
<td>Tactics-2</td>
<td>19(17)</td>
<td>64(1)</td>
<td>1.871</td>
</tr>
<tr>
<td>Tactics-3</td>
<td>20(20)</td>
<td>75(1)</td>
<td>1.880</td>
</tr>
</tbody>
</table>

scheme will help the settings of parameterization of security level of each nodes. These are our future works.

Problem 2. Analysis of actual attack results and optimum values of $\lambda_{max}(A)$ and $R$.

A relation between attack result and value of $\lambda_{max}(A)$ and $R$ should be analyzed. Since the maximum values of them are determined by the number of nodes and links, they decide topology definitely. Thus, we can also derive Tactics from the difference between the Initial topology and resultant topology with maximum values. So we can derive an optimum value of $\lambda_{max}(A)$ and $R$ theoretically, however, there is no realistic meaning. Because, it is easy to see from the result of example analysis shown in Fig4. Tactics-2, to achieve the optimum values is to give the infinite powerful condition for the attacker. So we conclude that the estimation of optimum values of $\lambda_{max}(A)$ and $R$ is useless in realistic network attack. In this paper, we estimate attack effect comparing with the initial value of $\lambda_{max}(A)$ and $R$. But it is not clear how increase from initial value is contributing to the attack result. The analysis of it is also our future work.

Problem 3. Analysis of feasibility of Tactics-2 and -3 in real network environment.

We face two problems in Tactics-2 and -3; 1) setting of agent server and 2) generation of links.

1) Setting of agent server
There are many un-managed IP addresses such as Darknet. In particular, the cases which student group use IP address without notice, and manage phishing servers are reported much at some Universities that has many IP addresses [12]. From this fact, it will be easy to set agent servers if we do not specify the location. Therefore a set at the most effective location may be impossible, but we can conclude that 1) can be solved easily.

2) Generation of links
After the set of agent server, we need to generate links. There are two ways to realize it. One is to establish physical communication lines or construct new network infrastructure. Another is to forge routing tables. The former way is powerful but we can not expect its feasibility. The latter way is realistic. Though we will need to forge many routers and their tables, the feasibility will be high by the same reason of 1). In particular, when attack scenario and tactics are decided beforehand, the execution will be easy.
REFERENCES

[1] Internet Engineering Task Force


[12] Private discussion with security vendors


