

Multi-path Based Link-state Routing Mechanism

Jing Tao, Xianming Gao, Baosheng Wang, Xiaozhe Zhang, Shicong Ma

School of Computer, National University of Defense Technology, Changsha China

ellen5702@aliyun.com

Abstract—End-to-end communication usually adopts a single path to transmit interactive packets in traditional routing mechanisms, so attackers can easily snoop into the whole communication trace to analyze users' typical features and to predict users' next-behaviors, which can severely decrease the security of users' information. Thus, this paper puts forward a multi-path based link-state routing mechanism, which can achieve packet transmission via multiple paths for end-to-end communication. It's a distributed system, which can make each node attain the whole network status by using notification of link-status. Besides, this mechanism uses two key parameters: path length (refers to length of path carrying end-to-end communication) and path reliability (refers to security degree of path) to calculate optional path-set that can be used to transmit packets. On the basis, we further use "exponential penalty" method and "exponential reward" method to calculate distribution ratio of data-flow via each path of optional path-set. Our experimental results show that our routing mechanism can effectively achieve tasks of packet transmission in end-to-end communication by using multiple paths with high reliability and short length.

Keywords—routing mechanism; link-status; multi-path; path length; path reliability; system robustness

I. INTRODUCTION

With the rapid development of information technology, the Internet has become an important information infrastructure for human society, such as Internet surfing, e-commerce and so on [1]. Its openness makes it face with a variety of security issues, such as data snooping, and information leakage .etc. In order to address above problems, research scholars put forward an idea to establish trusted network, which is a safe, controllable and reliable environment [2-3]. Trusted network is a kind of security system framework, which needs to monitor and evaluate network behavior and to control abnormal network behavior. In addition to authentication and authorization mechanism to ensure the security of access network equipment (e.g. terminals, routers, and switches .etc.) [4], it still needs to ensure that users' information isn't intercepted or tampered by any attacker. Currently, data encryption is usually used to ensure data

security, which can hinder information leakage [5]. But attackers can still capture users' traces in the processing of end-to-end communication, such as interactive time, times of communication, and certain related content .etc. These users' traces are likely to be intercepted by attackers, while users are unaware of the situation where they are in a state of insecurity. So there are two questions: first, why can attackers attain users' typical features? Second, how can we do to hinder attackers and protect our information?

For the first question, it's mainly related to traditional routing mechanisms adopted in the Internet. The existing routing mechanisms mainly include OSPF protocol (open shortest path first) [6], RIP protocol (routing information protocol) [7] and BGP protocol (border gateway protocol) [8]. Take OSPF protocol as an example, it uses the shortest path algorithm to calculate paths for packet transmission, and end-to-end communication usually adopts a single path to transmit interactive packets at most time. Similarly, path for end-to-end communication in RIP protocol is also the sole. Thus, an attacker can easily attack one important node in network topology to snoop into users' communication traces, such as interactive time, searching content and so on, and to further analyze users' typical features by using big-data technology [9-10]. Even if some nodes support ECMP protocol (Equal Cost Multipath Routing) [11], attackers are also able to calculate these equivalent multiple paths and to intercept users' traces. Thus, it's difficult for traditional routing mechanisms to prevent attackers snooping into users' traces.

In order to address the second question, we should change traditional routing mechanisms which using a single path to transmit packets for end-to-end communication. We need to use multiple paths to achieve end-to-end

communication to increase attack difficulty for attackers. So this paper proposes a multi-path based link-status routing mechanism, which can use multiple paths to transmit packets and effectively avoid the whole users' traces intercepted by attackers. This mechanism adopts distributed system to ensure that routing mechanism has high robustness. Nodes usually notify their link-status to others and receive others' link-status to obtain the whole network status. Besides, two key parameters of path length and link reliability in our proposed routing mechanism are used to determine optional path-set for end-to-end communication. At the same time, we further put forward "exponential penalty" way and "exponential reward" way to calculate distribution ratio of data-flow transmitted by each path in optional path-set. In this way, end-to-end communication can achieve packet transmission via multiple paths with high transmission performance and high security degree. Our experimental results prove that this mechanism not only can effectively solve these key challenges, such as optional path-set which are used to achieve end-to-end communication and the distribution ratio of data-flow transmitted by each path, but also can reduce the probability of information leakage and increase attack difficulty for attackers.

The remainder of this paper is organized as follow. Section 2 discusses and illustrates the features of basic idea behind multi-path based link-status routing mechanism. Section 3 presents a mathematic model for our proposed routing mechanism including key features and important parameters. Section 4 mainly exhibits work procedure of our proposed routing mechanism. Section 5 presents our experimental results, and analyzes its advantages and disadvantages. Section 6 concludes this paper with a summary of our studies and discusses next works in the future.

II. BASIC IDEA

Traditional routing mechanisms usually use a single path to transmit packets for end-to-end communication, which allow attackers easily to snoop into users' traces, to analyze users' typical features, and to predict users' behaviors. If end-to-end communication adopts path (e.g. A-B-E-F) to transmit packets, attackers can intercept node E to

get users' traces including time when users establishing connections, end system with which users communication, and times of communication, as shown in Fig.1. Due to vulnerability of traditional routing mechanisms [12], users' information is easily intercepted by attackers, which causing information leakage. Therefore, in order to address above problems, this paper proposes a multi-path based link-status routing mechanism, which mainly uses multiples paths to transmit interactive packets for end-to-end communication.

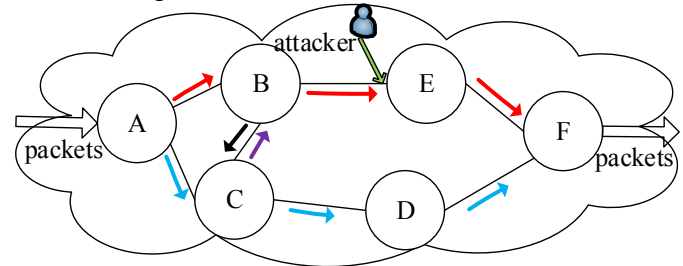


Figure 1. Packet transmission under different routing mechanisms

Compared with traditional routing mechanisms, the idea behind multi-path based link-status routing mechanism is to transmit packets via multiple different paths. For instance, when packets are transmitted from node A to node F, our proposed routing mechanism can use multiple paths to complete packet transmission, as shown in TABLE I. It can achieve tasks of packet transmission via four paths, and only two paths can be intercepted by attackers. Thus, it can reduce the amount of users' information got by attackers, reduce the extent of users' information leakage, and avoid predicting users' next behavior by attackers.

TABLE 1. PATHS OF PACKET TRANSMISSION

path	passed nodes	information leakage
1	A、C、D、F	no
2	A、B、E、F	yes
3	A、B、C、D、F	no
4	A、C、B、E、F	yes

The main challenge of multi-path based link-status routing mechanism is path convergence, because nodes can arbitrarily select multiple paths to transmit packets, and packets may be transmitted to other nodes, rather than the destination node, such as path (A-B-C-A). How to establish a reasonable and efficient mathematical model for multi-path based link-status routing mechanism is the first problem, which should select optional path-

set for end-to-end communication. Secondly, the length of optional path may be unequal, so the transmission performance via different paths may be also different. The shorter the path is, the higher the performance of packet transmission is; otherwise, the performance of packet transmission is relatively lower. Thus, routing mechanism should transmit packets via paths with short length as far as possible. Finally, the security degree of each link in the network is different. In order to ensure the security of end-to-end communication, it should transmit packets via links with high credibility and avoid transmitting packets via links with low credibility. To sum up, multi-path based link-status routing mechanism should address these above challenges: 1) how to calculate optional path-set for end-to-end communication, and 2) the distribution ratio of data-flow via each path in optional path-set.

III. MULTI-PATH BASED LINK-STATUS ROUTING MECHANISM

The multi-path based link-status routing mechanism uses link-state notification to obtain network status, including connectivity relationship between two nodes, link bandwidth, link credibility and so on[13]. Each node transmits its own link-status to other nodes, so that each node can obtain the overall network status including network topology and link credibility .etc. Our proposed mechanism can quickly calculate optional paths of packet transmission to achieve path convergence, which can fundamentally avoid configuration delay in centralized control network [14-15]. For example, data-flow cannot be transmitted in centralized network until SDN controller hasn't completed configuration [16].

OSPF protocol is based on the shortest path algorithm, so the shortest distance between next-hop and destination node is less than the shortest distance between current node and destination node. In our proposed routing mechanism, the shortest distance between next-hop and destination node is independent of the shortest distance between current node and destination node: the former may be either less than or no less than the latter. So it can use multiple paths to transmit packets. Besides, the selection of next-hop relies on path credibility, only paths with high credibility can carry out packet transmission. Therefore, when node chooses next-

hop, optional path needs to meet condition (1), as shown below:

Condition (1): only when path credibility is no less than an acceptable minimum of path reliability, node will choose these paths to transmit packets to avoid packets via links with low reliability.

In order to improve the security of packet transmission, the optional path reliability should be as high as possible. So, the higher the path reliability is, the greater the amount of packets transmitted via this path is. At the same time, in order to ensure that routing mechanism has a good transmission performance, paths with long length may result in high delay of packet transmission, which cannot meet requirements of real-time services. When selecting next-hop, nodes should consider the number of nodes passed through in the processing of packet transmission and the shortest distance between current node and destination node. So it can select paths with short length to achieve packet transmission as far as possible. Thus, when node chooses next-hop, path needs to meet condition (2), as shown below:

Condition (2): the sum of the number of nodes passed through in processing of packet transmission and the shortest distance between current node and destination node doesn't exceed an acceptable maximum of path length. Otherwise, transmission performance may not be able to meet needs of users' services.

In multi-path based link-status routing mechanism, the selection of path-set relies on two key parameters including path reliability and path length. Only when path meets the above two conditions, packet transmission for end-to-end communication can be accomplished by this path, as shown in formula (1).

$$\hbar(H_{s,t}^i) = \begin{cases} 1, ((\ell(P_{s,t}(i)) \geq \ell(M)) \& (d_{s,t}(u) + h_{s,t}(u) \leq h_{s,t}(N))) \\ 0 \end{cases} \quad (1)$$

In formula (1), s refers to source node, and t refers to destination node in network topology. $P_{s,t}(i)$ refers to the i^{th} optional path between source node s to destination node t. $\ell(P_{s,t}(i))$ indicates the reliability of path $P_{s,t}(i)$. $\ell(M)$ refers to an acceptable minimum of path reliability, which is determined by operators. Node is likely to choose paths to transmit

packets, only when optional path reliability is no less than $\ell(M)$. u refers to any node in one path, $d_{s,t}(u)$ means the shortest distance between current node and destination node, and $h_{s,t}(u)$ refers to the number of nodes that have already been passed through. $h_{s,t}(N)$ refers to an acceptable maximum of path length. $h(H_{s,t}^i(u))$ indicates whether or not node u choose this optional path: only when $h(H_{s,t}^i(u))$ equal to one, path can be regarded as one of optional path-set, which is used to transmit packets; otherwise, path isn't satisfied with these conditions of packet transmission.

Administrators can meet needs of different levels of security by setting $\ell(M)$. For example, when $\ell(M)$ is equal to zero, administrator doesn't make any request for network security. When only links with high reliability can transmit packets for end-to-end communication, network will have high reliability. However, $\ell(M)$ also affects the number of optional paths for end-to-end communication. Thus, it is necessary to select a reasonable value of $\ell(M)$ in multi-path based link-status routing mechanism.

Meanwhile, in order to ensure that network has a good transmission performance, optional path length is not too long. The longer the path length is, the higher the transmission delay is. Administrator can ensure the transmission performance by setting $h_{s,t}(N)$. However, $h_{s,t}(N)$ also affects the number of optional paths for end-to-end communication. Therefore, it is necessary to select a reasonable value of $h_{s,t}(N)$ in multi-path based link-status routing mechanism.

A. Path Reliability

In multi-path based link-status routing mechanism, paths selected by nodes are dependent on path reliability. Only when path reliability meets **condition (1)**, nodes can transmit packets via these optional paths. The path credibility is determined by the minimum of link reliability in one path, as shown in formula (2).

$$\ell(P_{s,t}(i)) = \min(\ell(L_{s,s+1}(i)), \ell(L_{s+1,s+2}(i)), \dots, \ell(L_{u,u+1}(i)), \dots, \ell(L_{t-1,t}(i)))$$

$$(L_{i,i+1}(i) \subset P_{s,t}(i), i \in [s, t]) \quad (2)$$

$L_{u,u+1}(i)$ refers to link between node u and node $u+1$, and $\ell(L_{u,u+1}(i))$ refers to link credibility of link $L_{u,u+1}(i)$. From the description of formula (2), in order to improve network credibility, administrators should try to enhance the security of link with the lowest reliability; otherwise, it cannot achieve

desired goal. So, it can provide certain guiding significance for maintaining links in the network topology.

B. Calculation of $h_{s,t}(N)$

In order to ensure that transmission delay meets needs of network service, end-to-end communication should choose the shorter path to transmit packets as far as possible. However, in order to avoid intercepting users' information, users use multiple paths between two ends. The scale of optional path-set for end-to-end communication has an influence on the amount of users' information intercepted by attackers. The higher the scale of optional path-set is, the more difficult the intercept of user's information is. The average of optional path-set for end-to-end communication is calculated, as shown in Formula(3).

$$NUM_{avg}(P_{s,t}) = \frac{\sum_{i=0}^M P_{s,t}(i)}{M} \quad (3)$$

$NUM(P_{s,t})$ refers to the average scale of optional path-set for end-to-end communication. M represents the total number of pairs of two different nodes in network topology. And $\sum_{i=0}^M P_{s,t}(i)$ is used to calculate the total number of optional paths in network topology. When the average scale of path-set is less than the minimum of optional path-set, namely $NUM_{min}(P)$, it is indicated that parts of end-to-end communication cannot meet security requirements.

Through above analysis, $NUM(P_{s,t})$ is closely related with $h_{s,t}(N)$: as $h_{s,t}(N)$ continually increases, $NUM(P_{s,t})$ also increases gradually. So, we can ensure that $NUM_{avg}(P)$ is no less than $NUM_{min}(P)$ by adjusting $h_{s,t}(N)$, which can make network have high security. Thus, this paper presents an algorithm for calculating an acceptable maximum of path length, namely $h_{s,t}(N)$ to ensure that $NUM_{avg}(P)$ is no less than $NUM_{min}(P)$, as shown in Fig.2.

Algorithm 1: calculation of $h_{s,t}(N)$ input: M 、 N 、 $Len(P_{s,t}(i))$ 、 $h_{s,t}(N)$ 、 $NUM_{\min}(P)$ output: $h_{s,t}(N)$

Procedure:

initializing $h_{s,t}(N) = MAX(d_{i,j}(i))$;calculating $NUM_{avg}(P_{s,t}) = \frac{\sum_{i=0}^M Len(P_{s,t}(i))}{M}$;while ($NUM_{avg}(P) < NUM_{\min}(P)$) {while ($path\text{-}set \leq NUM_{\min}(P)$) {search paths with destination node t ;if ($h(H_{s,t}^t(u)) = 1$)

selecting this path;

}

calculating $NUM_{avg}(P_{s,t})$; $h_{s,t}(N) ++$;

}

return $h_{s,t}(N)$;**Figure 2.** Calculation algorithm of $h_{s,t}(N)$

$MAX(d_{i,j}(i))$ refers to the maximum of the shortest path between two nodes in network topology. From the description of **algorithm 1**, only when initialization of $h_{s,t}(N)$ is $MAX(d_{i,j}(i))$, nodes can communicate with any node in the network; otherwise, some nodes cannot transmit packets to parts of nodes. On this basis, this algorithm can calculate current value of $NUM_{avg}(P)$, and compares $NUM_{avg}(P)$ with $NUM_{\min}(P)$ to adjust whether or not $h_{s,t}(N)$ meets network services. This algorithm adjusts $h_{s,t}(N)$ by increment until $NUM_{avg}(P)$ is no less than $NUM_{\min}(P)$. Finally, our proposed algorithm can filter optional path-set for end-to-end communication, whose path length is no longer than $h_{s,t}(N)$.

C. Horizontal Cutting

In traditional routing protocols, in order to ensure normal operations of routing mechanism, horizontal cutting is usually used to avoid routing loops [17]. Similarly, multi-path based link-status routing mechanism uses horizontal cutting to ensure that the same packet is not forwarded between two adjacent nodes forever. Node will not forward

packets to next-hop via source interface, as shown in formula (4).

$$\tilde{h}(D_{s,t}^{u,v}(u)) = \begin{cases} 1, (D_{s,t}^{u,v}(u) > D_{s,t}^{u,v}(v)) \\ 0, (D_{s,t}^{u,v}(u) \leq D_{s,t}^{u,v}(v)) \end{cases} \quad (4)$$

In formula (4), u and v are two adjacent nodes in one path. $D_{s,t}^{u,v}$ refers to one packet passing through node u and node v successively when one packet is transmitted from source node s and destination node t . $D_{s,t}^{u,v}(u)$ refers to the shortest path from node u and destination node t . Only when the condition of $D_{s,t}^{u,v}(u) > D_{s,t}^{u,v}(v)$ is met, node u will send packets to node v ; otherwise, node u will not forward packets to node v . Thus, node will not forward packets to next-hop via source interface.

D. The Distribution Ratio of Data-flow

The multi-path based link-status routing mechanism can achieve packet transmission via multiple paths, which can avoid intercepting users' communication traces and prevent the excessive leakage of users' information. Through the description of our proposed routing mechanism, the optional paths should satisfy conditions (1) and condition (2), so as to calculate optional path-set for end-to-end communication, which is used to address the first challenge in our proposed routing mechanism. On this basis, this part mainly studies how much data-flow for end-to-end communication is calculated on each path, which is used to solve the second challenge. Under the premise of ensuring the network has good transmission performance, packets are transmitted via paths with high reliability as far as possible.

On one hand, in order to guarantee end-to-end communication with low transmission delay, it should use short path to carry more users' information. Therefore, "exponential penalty" is used to make sure that packets are transmitted via paths with short length as far as possible, as shown in formula (5).

$$\frac{\dagger(P_{s,t}(i))}{\dagger(P_{s,t}(j))} \approx \frac{e^{-Len(P_{s,t}(i))}}{e^{-Len(P_{s,t}(j))}} ((i, j \in [s, t]) \& i \neq j) \quad (5)$$

$\dagger(P_{s,t}(j))$ refers to the distribution ratio of data-flow for path $P_{s,t}(j)$. From the description of formula (5), when path length is longer, the

distribution ratio of data flow via this path is less, which can reduce the average of transmission delay for end-to-end communication.

On the other hand, the distribution ratio of data-flow is closely related to path reliability. In order to make sure that network has good security, packets are transmitted via paths with high reliability as far as possible. Therefore, it can use "exponential reward" way to ensure that packets are transmitted via paths with high credibility. The higher the path reliability is, the more the distribution ratio of data-flow on this path is, as shown in formula (6).

$$\frac{\dagger(P_{s,t}(i))}{\dagger(P_{s,t}(j))} \approx \frac{e^{\ell(P_{s,t}(i))}}{e^{\ell(P_{s,t}(j))}} ((i, j \in [s, t]) \& i \neq j) \quad (6)$$

Through above description, the distribution ratio of data-flow on each path is mainly related to two key parameters: path credibility and path length. In combination with formula (5) and formula (6), the distribution ratio of data-flow on each path of optional path-set is calculated, as shown in formula (7).

$$\mathfrak{P}_{s,t}(i) \approx \frac{e^{\ell(P_{s,t}(i)) - \text{Len}(P_{s,t}(i))}}{\sum_{j=0}^N e^{\ell(P_{s,t}(j)) - \text{Len}(P_{s,t}(j))}} (j \in [0, \text{NUM}(P_{s,t})) \quad (7)$$

$\mathfrak{P}_{s,t}(i)$ refers to the distribution ratio of packets that path $P_{s,t}(i)$ carrying. From the description of formula (7), when path length is longer and path reliability is lower, the distribution ratio of data-flow on path is lower. In contrast, when path length is shorter and path reliability is higher, the distribution ratio of data-flow on path is higher. Our proposed routing mechanism uses formula (7) to calculate the distribution ratio of data-flow on each path for end-to-end communication, so packets can be transmitted via one path with high reliability and short length.

IV. DESCRIPTION OF ROUTING ALGORITHM

The multi-path based link-status routing mechanism achieves end-to-end communication by selecting multiple paths. It uses path length and link reliability to select paths to transmit packets, and to determine how much packets are transmitted by each path. In this way, it is more difficult for attackers to intercept users' information, to analyze users' characteristics, and to predict users' next-

behaviors. The core of routing mechanism has two points: first, how to calculate optional path-set quickly; second, how to calculate distribution ratio of data-flow via each path of optional path-set. The algorithm of multi-path based link-status routing mechanism is described, as shown in Fig.3.

Algorithm 2: Multi-path based routing mechanism

input: link-status notification packet

output: the distribution ratio of data-flow

procedure:

nodes notify its link-status to other nodes;
using **algorithm 1** to calculate $h_{s,t}(N)$;

$$\mathfrak{P}_{s,t}(i) \approx \frac{e^{\ell(P_{s,t}(i)) - \text{Len}(P_{s,t}(i))}}{\sum_{j=0}^N e^{\ell(P_{s,t}(j)) - \text{Len}(P_{s,t}(j))}} \mathfrak{P}_{s,t}(i) ;$$

return $\mathfrak{P}_{s,t}(i)$;

Figure 3. Algorithm of our proposed routing mechanism

From the description of **algorithm 2**, it is divided into three steps: first, node notifies its link-state to other nodes and can obtain the whole network status, such as connectivity relationship, and link reliability .etc; second, it uses **algorithm 1** to obtain an acceptable maximum of path length, namely $h_{s,t}(N)$, and to select optional path-set as well; third, it calculates the distribution ratio of data-flow on each path of optional path-set according to path reliability and path length. The data plane in one router can uses these above generated strategies to determine forwarding behavior of each packet.

Through the description of **algorithm 1** and **algorithm 2**, time complexity of our proposed mechanism is mainly determined by **algorithm 1**. Because it uses greedy algorithm [18] to traverse network topology to calculate paths from source node s to destination node t , the time complexity of **algorithm 1** is $o(n \log n)$. At the same time, after completing the selection of optional path-set, it should use the condition of $\text{NUM}_{\text{avg}}(P) < \text{NUM}_{\text{min}}(P)$ to decide whether or not $h_{s,t}(N)$ meets demands. Therefore, the time complexity of our proposed routing mechanism is $o(n^2 \log n)$ at the worst time.

V. EXPERIMENT AND ANALYSIS

In this section, we measure influences of two key parameters including link reliability and path length on the performance of multi-path based link-status

routing mechanism. On this basis, experimental results show that our proposed routing mechanism can ensure that packets are transmitted via paths with high reliability and short length.

A. Experimental Environment

In this experiment, we adopt the Abilene network topology, which is a typical network topology in real network and mainly consists of 11 nodes and 14 links [19]. In order to further verify influences of link reliability on the performance of routing mechanism, link reliability of each path is set randomly, whose value locates in a defined range from one to five, as shown in Fig.4. At the same time, $NUM_{\min}(P)$ is set to 2, and $\ell(P_{s,t}(i))$ is set to 1.

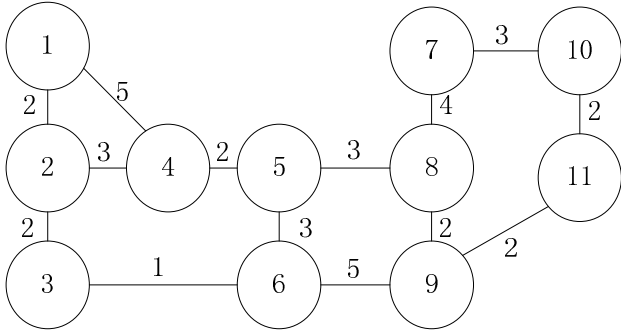


Figure 4. Abilene network topology

This experiment has three points: 1) exploring relationship between $NUM_{avg}(P)$ and $h_{s,t}(N)$, 2) influences of $\ell(P_{s,t}(i))$ on the performance of our proposed routing mechanism, and 3) verifying the validity of the distribution algorithm of data-flow.

B. The Influence of $h_{s,t}(N)$

$h_{s,t}(N)$ refers to the maximum of path length in the network topology, and the length of optional path between source node and destination node must be less than (or equal to) $h_{s,t}(N)$. So $h_{s,t}(N)$ has a direct effect on the performance of **algorithm 1**, because $h_{s,t}(N)$ can make influences on search range in processing of traversing network topology. However, if $h_{s,t}(N)$ is too small, the scale of optional path-set for end-to-end communication is also small, which may make parts of end-to-end communication not to be established. Therefore, the first experiment is used to evaluate the influences of $h_{s,t}(N)$ on $NUM_{avg}(P)$, as shown in Fig.5.

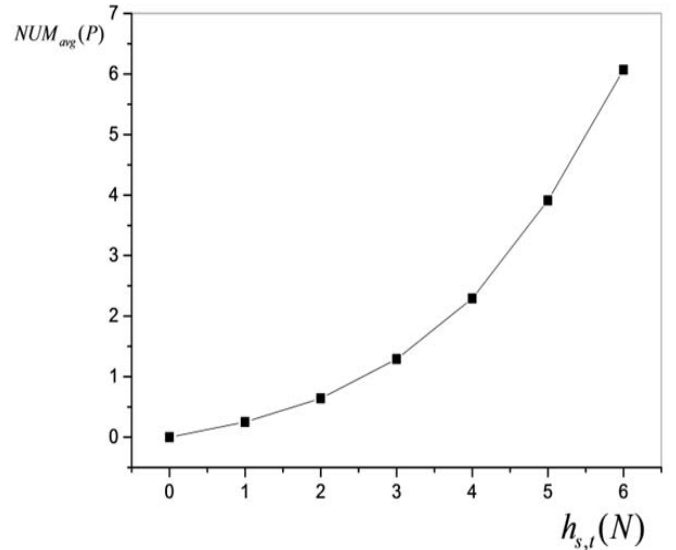


Figure 5. Relationship between $h_{s,t}(N)$ and $NUM_{avg}(P)$

Through the description of Fig.5, with the increase of $h_{s,t}(N)$, $NUM_{avg}(P)$ is continually increasing. For example, when $h_{s,t}(N)$ is set to 4, $NUM_{avg}(P)$ is about 2.3, which indicates that the average scale of optional path-set in the network topology is 2.3. Even if $NUM_{\min}(P)$ is set to 2, $NUM_{avg}(P)$ is bigger than $NUM_{\min}(P)$, which is still unable to meet needs of network transmission, because the shortest path between two nodes in Abilene network is 5 (e.g. the shortest path between node 1 and node 10 in Fig.4). According to the description of **algorithm 1**, the minimum of $h_{s,t}(N)$ should be 5. Only in this way it can ensure that any two ends can establish communication in the network. Therefore, $h_{s,t}(N)$ is set to 5, so $NUM_{avg}(P)$ is about 3.9, and the average scale of optional path-set is about 3.9, which is bigger than $NUM_{\min}(P)$.

C. The Influence of $\ell(P_{s,t}(i))$

$\ell(P_{s,t}(i))$ is determined by the lowest reliability of link in one path. Only when the reliability of all link in one path is no less than $\ell(P_{s,t}(i))$, path can be selected for optional path-set, which can be responsible for packet transmission. $\ell(P_{s,t}(i))$ also affects the scale of optional path-set for end-to-end communication. In order to further verify the influences of $\ell(P_{s,t}(i))$ on the performance of our proposed routing mechanism, we measure some

main characteristics, including the total amount of paths that should meet **condition (1)** and **condition (2)** in the network topology, $NUM_{avg}(P)$, pair of nodes that can communicate with each other and $MAX(d_{i,j}(i))$, as shown in TABLE II.

Through the analysis of results in TABLE II, we can see that path reliability has high influence on the performance of our proposed routing mechanism. We further analyze experimental result in four points. First, the higher $\ell(P_{s,t}(i))$ is, the smaller the scale of optional path-set is. For example, when $\ell(P_{s,t}(i))$ is set to three, the optional path-set just includes 18 paths; while $\ell(P_{s,t}(i))$ is set to two, the optional path-set just includes 149 paths. Second, with the increase of $\ell(P_{s,t}(i))$, $NUM_{avg}(P)$ continually decreases, which indicates that the scale of optional path-set for end-to-end communication is becoming smaller. For example, when $\ell(P_{s,t}(i))$ is no less than three, $NUM_{avg}(P)$ is lower than one, which indicates that network cannot transmit packets for any end. Third, the pair of nodes that can communicate with each other becomes smaller with the increase of $\ell(P_{s,t}(i))$, which indicates that parts of nodes cannot transmit packets to other nodes. For example, when $\ell(P_{s,t}(i))$ is set to five, only a pair of node 1 and node 4 can communicate with each other, as well as a pair of node 6 and node 9. At last, $MAX(d_{i,j}(i))$ also become higher with the increase of $\ell(P_{s,t}(i))$, which may result in the increase of $h_{s,t}(N)$. For example, when $\ell(P_{s,t}(i))$ is set to one, $h_{s,t}(N)$ is equal to five; when $\ell(P_{s,t}(i))$ is set to two, $h_{s,t}(N)$ becomes six. Moreover, when $\ell(P_{s,t}(i))$ exceeds a certain value, $MAX(d_{i,j}(i))$ doesn't exist, which indicates that network topology includes some "islands". These "islands" just communicate with nodes in the same "island", rather than nodes in the other "island".

To sum up, when link credibility in the network is relatively low, $h_{s,t}(N)$ can affect network's interoperability. When network has a small scale of links with low credibility, our proposed routing mechanism can avoid transmitting packets via links with low reliability. Therefore, it is necessary to set

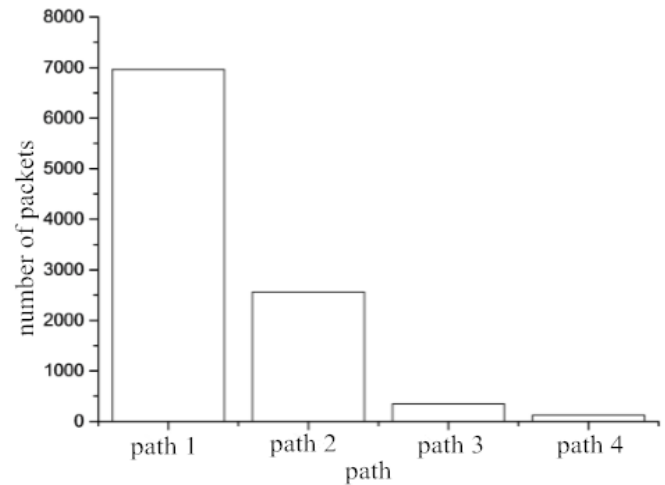
up a reasonable value for $\ell(P_{s,t}(i))$ in our proposed routing mechanism.

TABLE 2. MAIN CHARACTERISTICS

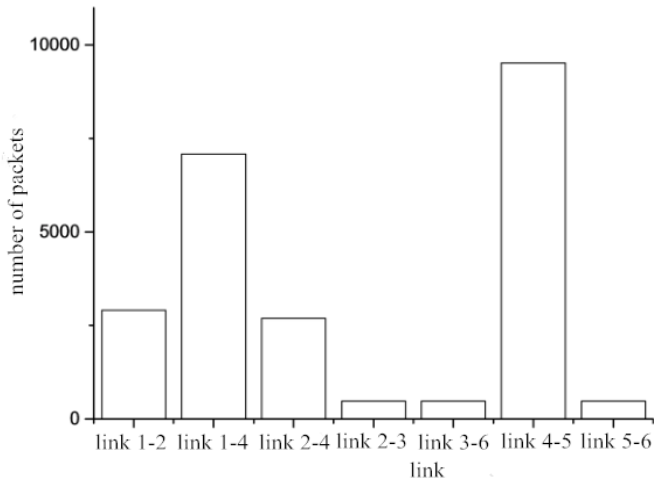
$\ell(P_{s,t}(i))$	0	1	2	3	4	5
Amount of paths	215	215	149	18	3	2
$NUM_{avg}(P)$	3.91	3.91	2.7	0.33	0.05	0.04
Pair of nodes	55	55	55	18	3	2
$MAX(d_{i,j}(i))$	5	5	6	null	null	null

D. The Distribution Ratio of Data-flow

The purpose of our proposed routing mechanism is to realize packet transmission via multiple paths. At the same time, in order to determine the distribution ratio of packets transmitted by each path, we proposed two key functions by using "exponential penalty" and "exponential reward". Supposed that node 1 communicates with node 5, and the number of interactive packets between these two nodes is 10000. Because $NUM_{min}(P)$ is 2 and $h_{s,t}(N)$ is 5, the amount of paths between node 1 and 5 is four: path 1 (1-4-5), path 2 (1-2-4-5), path 3 (1-2-3-6-5), and path 4 (1-4-2-3-6-5). In order to verify the validity of our proposed routing mechanism, we measure the amount of packets transmitted by four paths and the number of packets transmitted by each link, as shown in Fig.6.



a. Distribution on each path



b. Distribution on each link

Figure 6. Distribution of data-flow

Through description of figure 6.a, there is a significant difference in the amount of packets carried by each path. For example, both path 2 and path 1 carry 95% of packets, and path 1 is responsible for about 70% of packets, because the reliability of path 1 is greater than (or equal to) others', and the length of path 1 is two, which is shorter than others', as shown in TABLE 3. $\ell(P_{s,t}(i))$ in path 3 and path 4 is lower than $\ell(P_{s,t}(i))$ in path 2, and $Len(P_{s,t}(i))$ in path 3 and path 4 is larger than $Len(P_{s,t}(i))$ in path 2, so either path 3 or path 4 carries a very small amount of packets. Through the above analysis, it is proved that our routing mechanism is effective, which can ensure that the transmission delay is low and packets are transmitted via paths with high reliability as far as possible.

However, further analysis of figure 6.b shows that the number of packets in each link is significant difference. For example, link 4-5 is responsible for about 95% of packets, and link 2-3 only carries about 5% of packets. In some specific scenarios, certain links (such as link 4-5) may become the bottleneck of network performance.

TABLE 3. MAIN PARAMETERS

path	$\ell(P_{s,t}(i))$	$Len(P_{s,t}(i))$
path 1	2	2
path 2	2	3
path 3	1	4
path 4	1	5

VI. CONCLUSION AND FUTURE WORKS

The traditional routing mechanisms usually use a single path to transmit packets, which makes it easy for attackers to obtain a complete interactive communication between users and end systems. Attackers can analyze users' characteristics, thus causing users' information leakage. Aiming at these problems, this paper proposes a multi-path based link-status routing mechanism, which can realize packet transmission via multiple paths. Our proposed routing mechanism mainly solves two challenges: 1) the selection of optional path-set that carrying packets for end-to-end communication, 2) the distribution ratio of data-flow that is carried by each path. Finally, we analyze the influences of $h_{s,t}(N)$ and $\ell(P_{s,t}(i))$ on our proposed routing mechanism. And experimental results proves that the way of "exponential penalty" and "exponential reward" is useful for the second challenge.

Through the analysis of experimental results, the distribution ratio of data-flow based on path reliability and path length may be a better mechanism, which may be the bottleneck of network performance. The next step is to further improve and perfect multi-path based link-status routing mechanism by researching on traffic engineering [20-21].

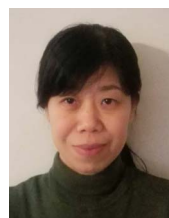
ACKNOWLEDGMENT

This work is supported by Program for National Basic Research Program of China (973 Program) 'Reconfigurable Network Emulation Testbed for Basic Network Communication', and research on XXX access authentication and authorization protocol standards.

REFERENCES

- [1] Feamster N, Gao L, Rexford J. How to lease the Internet in your spare time[J]. ACM SIGCOMM Computer Communication Review, 2007, 37(1): 61-64.
- [2] ZHANG Huan-Guo, University W, University W, et al. Research on Trusted Network Connection[J]. Chinese Journal of Computers, 2010.
- [3] Ou W, Wang X, Han W, et al. Research on Trusted Network Model Based on BLP Model[C]// Computer Sciences and Convergence Information Technology, 2009. ICCIT '09. Fourth International Conference on IEEE, 2009:1137-1142.
- [4] Zhang L R, Yan C P, Zhan B R. Trusted Network Access and Authentication Technology Based on EAP-TTLS[J]. Computer & Modernization, 2013, 218(10):110-113.
- [5] Biham E, Shamir A. Differential Cryptanalysis of the Data Encryption Standard[M]// Springer New York, 1993.
- [6] Moy J. Multicast Extensions to OSPF[J]. IETF RFC 1584, 1994.
- [7] X S, J L, T N, et al. RIP3, a novel apoptosis-inducing kinase.[J]. J Biol Chem, 1999, 274,.

- [8] Griffin T G, Wilfong G. An analysis of BGP convergence properties[J]. In SIGCOMM, 1999:277-288.
- [9] Peng Q, Coltd H C. Research on Traffic Analysis Platform Solution Based on Big Data Technology[J]. Designing Techniques of Posts & Telecommunications, 2014.
- [10] Jeong Y, Ma J, Yang L T, et al. Advanced communication systems for enhanced big data technology and applications[J]. International Journal of Communication Systems, 2014, 27(6):825-827.
- [11] Dzida M, Zagozdzon M, Pioro M, et al. Optimization of The Shortest-Path Routing with Equal-Cost Multi-Path Load Balancing[J]. Transparent Optical Networks, 2006 International Conference on, 2006:9 - 12.
- [12] Schuchard, M., Aohaisen, A., Kune, D., et al.: Losing Control of the Internet: Using the Data Plane to Attack the Control plane. In: Proc. of the 17th ACM Conf. on Computer and Communications Security, pp. 726–728. ACM, New York (2010)
- [13] Xu D, Chiang M, Rexford J. Link-State Routing with Hop-by-Hop Forwarding Can Achieve Optimal Traffic Engineering[C]. //INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE, 2008:1717 - 1730.
- [14] Feamster N, Rexford J, Zegura E. The road to SDN: an intellectual history of programmable networks[J]. Computer Communication Review, 2014, 44(12):87-98.
- [15] Banikazemi M, Olshefski D, Shaikh A, et al. Meridian: an SDN platform for cloud network services[J]. IEEE Communications Magazine, 2013, 51(2):120-127.
- [16] Gude N, Koponen T, Pettit J, et al. NOX: towards an operating system for networks.[J]. ACM SIGCOMM Computer Communication Review, 2008, 38(3):105-110.
- [17] Hou R, Sun J Q, Ding P F. Study on a routing loop detection method in MPLS network[J]. Study on Communications, 2005.
- [18] Wolsey L A. An analysis of the greedy algorithm for the submodular set covering problem[J]. Core Discussion Papers Rp, 1982, 2(4):385-393.
- [19] "Abilene backbone network," Internet2, Ann Arbor, MI [Online]. Available: <http://abilene.internet2.edu/>.
- [20] A. Sridharan, R. Guérin, and C. Diot, "Achieving near-optimal traffic engineering solutions for current OSPF/IS-IS networks," *IEEE/ACM Trans. Netw.*, vol. 13, no. 2, pp. 234–247, Apr. 2005.
- [21] S. Srivastava, G. Agrawal, M. Pioro, and D. Medhi, "Determining link weight system under various objectives for OSPF networks using a Lagrangian relaxation-based approach," *IEEE Trans on Network & Service Management*, vol. 2, no. 1, pp. 9–18, Nov. 2005



Jing Tao (F'71), associate professor with School of Computer Science, National University of Defense Technology (NUDT), Changsha China. She has joined the academic group of NUDT to visiting some international universities, including the ETH (Switzerland), the University of Melbourne (Australia), etc. Her current research interests include Network Application, Network Security and Distribute Simulation.



Xianming Gao (M'88), doctoral student with School of Computer Science, National University of Defense Technology (NUDT), Changsha China. His current research interests include Next-generation Network Architecture, Router Architecture, and Network Functions Virtualization, etc.



Baosheng Wang (M'71), associate professor with School of Computer Science, National University of Defense Technology (NUDT), Changsha China. His current research interests include Next-generation Network Architecture, Router Architecture, Routing Protocol and Communication Security, etc.



Xiaozhe Zhang (M'64), professor with School of Computer Science, National University of Defense Technology (NUDT), Changsha China. His current research interests include Router Architecture, Routing Protocol and Network Infrastructure, etc.



Shicong Ma (M'86), doctoral student with School of Computer Science, National University of Defense Technology (NUDT), Changsha China. His current research interests include Next-generation Network Architecture, Router Architecture, and Network Functions Virtualization, etc.