# Combining SDN and ICN for Network Survivability Improvement

Zheng-Yang Ai*, Fei Song, and Xi Wang
Beijing Jiaotong University, P. R. China
{fsong, 17111017, 17120126}@bjtu.edu.cn

**Abstract**

With the rapid development of Information Communication Technology (ICT), the traditional networks are facing tremendous challenges. In recent years, the network security has been constantly affected by various factors (e.g., the damages of natural disaster, network intrusion, and limited properties of network). It is urgent to make some appropriate adjustments for current network architecture. Software Defined Networking (SDN) and Information-Centric Networking (ICN) bring innovation, speediness in recovery and reconfiguration for network computing. SDN decouples the forwarding plane from controlling plane, thus moving the control logic from a node to the central controller for the real-time supervision. ICN separates the resources from the location, to make the host-oriented model transform into content-centric model, which promotes the utilization of network resources and relieves the explosive growth of network flow. In this paper, we present a novel safety network model by applying SDN and ICN to the network recovery and reconfiguration. The proposed model prevents the network congestion and monitors the network status in real time. The system can be quickly restored after being damaged, which improves the network survivability. We considered three scenarios (natural disaster, malicious damage, and system self-defect) to discuss the proposed model. We simulated the situation where system was damaged and calculated the recovery time. The simulation results show that recovery time of system is shorter in the proposed model than in traditional network. Finally, we explore the broader perspectives for the network security.

**Keywords**: SDN, ICN, Network Survivability, Security

## 1 Introduction

According to the 2017 cisco annual cyber security report (MCR) [4], the network security threats are rapidly evolving and the number of attacks is increasing. There are "Denial of Service" (DOS) attacks in current network, such attacks would remove the backup and security measures that companies use to recover their systems and data. With the emergence of the Internet of things, plenty of online operations have been implemented in key industries, and the potential size and impact of such threats are increasing. In addition, according to the 2017 Internet Trend report [13]: the number of Internet users worldwide has exceeded 3.4 billion, which increases by around 10%, and the global penetration rate of Internet is 46%. The global IP traffic in 2017 has increased more than 1.4 ZB, and the global average fixed broadband speed will grow 3.5 times than 2012, which is from 11.3 Mbps to 39 Mbps according to the Cisco Visual Networking Index (VNI) latest report. All of the above mentions illustrate the challenges of the existing network (i.e., network congestion, network delay, low transmission efficiency and ineffective network management), which eventually leads to the collapse of the system. Therefore, the network security is suffering a serious situation.

*Journal of Internet Services and Information Security (JISIS)*, volume: 8, number: 1 (February 2018), pp. 18-30
*Corresponding author: School of Electronics and Information Engineering, Beijing Jiaotong University, P. R. China, Tel: (+86)-17070137776, Email:17111017@bjtu.edu.cn

In order to deal with these issues, SDN and ICN have attracted more and more attention from academic institutions and enterprises in recent years. This model can improve the network transmission efficiency and security. In some cases, the information transmission is not based on IP protocol, which solves all the problems of IP effectively (i.e., tampering with the address, address eavesdropping, fake identity, etc.) and makes routers cache the relative data. The users can get the required content nearby, when there is a network attack or network collapse.

With the continuous development of SDN and ICN. On the one hand, several studies have addressed potential security and other network issues of SDN and ICN respectively [10, 2, 9, 8]. On the other hand, some authors analyzed the network issues (i.e., routing, caching, naming, router and controller, etc.) of the combination of SDN and ICN. Masahiro Jibiki et al. [7] proposed a new framework (OF-ICN) by combining the smart and forward parts of ICN with SDN. The data naming, routing and mapping identifiers, caching strategies, and access control are present. At the same time, the article analyzed the compatibility. Jaehyeok Son et al. [15] applied SDN to ICN, and proposed a new FT package format to replace FIB, PIT format. In this paper, a new forwarding mechanism was proposed, which solves network latency and large data packets. Myungchul Kwak et al. [3] proposed a new routing protocol (c-flow), which makes SDN apply to the ICN. This approach effectively improves the transfer efficiency and promotes the cache management capability. Mayutan Arumaithurai et al. [1] proposed a FCSC structure, which is a forwarding mechanism based on the naming service by introducing ICN to SDN and NFV architectures, and decoupling resources and location information. This model effectively solves the problem of extensibility, flexibility and reliability in the system. Anwar Kalghoum et al. [12] proposed the NDNS architecture, which applied the ICN to SDN architecture. This model reduces network load, improves network behavior, solves the problem of ICN extensibility and bandwidth consumption, and lowers the network delay, etc. Niels l. m. van Adrichem et al. [16] applied NDN to SDN and proposed an open software implementation method named NDNFlow, which is a new forwarding mechanism of concrete application. It can prevent interdependence in the protocol versions, and simplify routing deployment and maintenance. Specifically, the main contributions of this work are:

- We propose a novel network model which applies the SDN and ICN into the network security.
- Three security scenarios are considered respectively (i.e., natural disaster, malicious damage, and system self-defect), we study the recovery time of system to demonstrate the feasibility of model.
- The simulations and demonstrations show that the system can recover quickly through the proposed model, after being damaged.

However, there are few authors to emphasize the security on the combination of SDN and ICN. In this paper, we analyze the effects of ICN and SDN on network security in detail. The specific recovery process of combination network is proposed. We focus on three scenarios to study the system recovery. The benefits of the combining network on security include the following parts: fast fault restoration, no affect for users to access to resources, no related issues of IP network, etc.

## 2 Overview of SDN and ICN

In this section, we briefly introduce the basic theory of ICN and SDN. After that, the specific structure of SDN and ICN is introduced in detail respectively. Finally, we shortly discuss the combination structure of SDN and ICN.

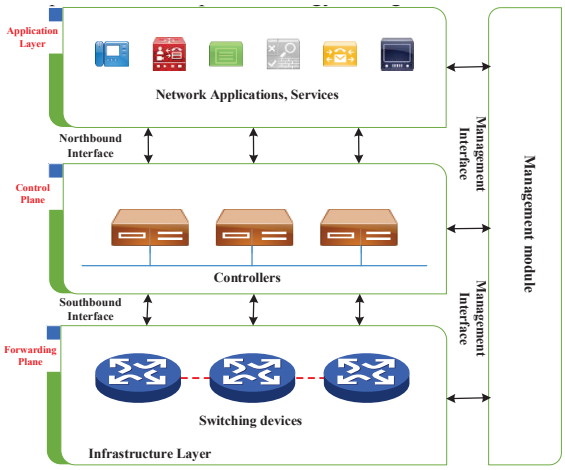



Figure 1: Structure of SDN

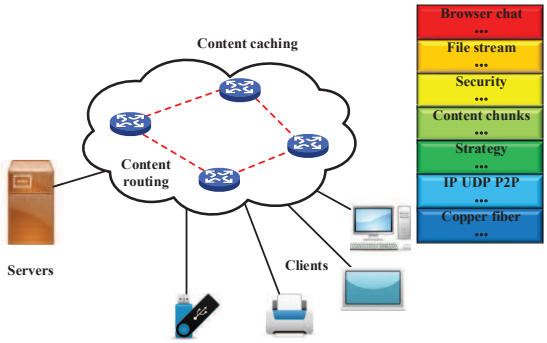



Figure 2: Structure of ICN

## 2.1 Preliminary of SDN

SDN is a research project that originated from Stanford university laboratory in the United States, it is a new type of network paradigm, which separates the controlling plane from the data plane. Actually, the relative controlling entity (SDN controller) is added into the traditional architecture (i.e., the software part controls the hardware infrastructure). The generation of SDN is closely related to OpenFlow, the OpenFlow provides the response strategy through the southbound interface.

Generally, the system is divided into four planes (i.e., forwarding plane, controlling plane, management plane, application plane) and three interfaces (i.e., southbound interface, northbound interface, management interface), as shown in Figure 1. This model contains the following features: Centralized data processing, High efficiency, Effective deployment of transmission bandwidth and other network resources, High network resource utilization, Efficient manageability. The underlying routers can be divided into several clusters, thus SDN controller can effectively manage multiple clusters together, the separation of controlling platform and data platform is helpful for the intelligent network. When the network architecture changes, the system can be supervised by the customized software at any time. The SDN controller is able to control the whole network, monitor the network flow in real time and allocate the path dynamically, which improves the security and reliability [6], [14].

## 2.2 Preliminary of ICN

ICN is also a new type of network architecture, which involves some aspects (i.e., information naming, name resolution, route forwarding, information distribution, routing cache). Since the traditional host-to-host communication no longer satisfies the network with a large number of content forwarding, ICN architecture overcomes above shortcomings and replaces the traditional model. The purpose of the naming-based service is to make each network node own the caching function. The ICN network relies on two types of information: interest packet and data packet, the interest packet acts as a request data information and the data packet stands for a response to transmit the required content, i.e., searching for the required data according to the interest packet. Actually, the content can be cached in the switch close to the host. On the contrary, the users can get the required data from the nearest router without complicated searching process.

The host only needs to send the interest packet to the network, until the packet is forwarded to the host including the content, the data will pass the original road to return. Moreover, each node in ICN contains

three structures: Content Storage (CS), Pending Information Table (PIT), and Forwarding Information Block (FIB), as shown in Figure 2. In addition, ICN solves the security problems caused by the host, such as, unreliability and high information risk. Therefore, ICN architecture is safer than traditional network due to the content-oriented model.

### 2.3 Combination Considerations

The architectures of SDN and ICN have greatly improved the traditional network architecture, as described in the precious sections. However, they have some challenges and problems respectively.

For the SDN architecture, there are many problems to urgently deal with (i.e., how to set up the distance between the control plane and data plane, how many instances to meet the fault recovery ability, whether the control plane can be actually deployed far from the data plane absolutely, and how to expand the centralized control of system). In addition, some challenges also needs to be solved (high software complexity, pressure of calculation, no standardized interface and compatibility).

ICN also has some problems and challenges like SDN (i.e., lacking of forwarding control scheme, scalability problems, data mobility problems, routing deployment issues, cache saturation of the routing table and cache replacement problems).

Therefore, the ICN and SDN have large room for further development. As for the above shortcomings, the effective combination of ICN and SDN perfectly solves the defects and complements each other. At present, the combination of SDN and ICN has been extensively investigated, the main idea is to combine the core concepts of SDN with ICN. This architecture can be used to make users get resources within the shortest time, and the packets can be forwarded according to the optimal path calculated by the controller. The combination of both models completely compensates for their respective defects.

## 3 The integration structure for security

In this part, we introduce the integration model of SDN and ICN on security and related process. The components of model are analyzed in detail. In addition, the characteristics of model and specific scenarios are discussed.

### 3.1 Generic working process

The structure of the combination is roughly divided into three layers, the lowest layer is the infrastructure layer, which consists of some routers. The second layer is the control platform composed of SDN controller. The top layer is the application layer, which includes some texts and voice services. The specific working process of the integration is as follows, as shown in Figure 3:

1. The user 1 in network sends a request packet to the network.
2. The ICN router 1 receives the request, then find out whether it contains the required content. If it contains that, it will directly return the content to ICN router 1.
3. If not, when the ICN router 1 receives the request, the request will be sent to the SDN controller.
4. The SDN controller based on the global situation, sends the forwarding rule back to the ICN router 1 after calculation. Then the ICN router updates its forwarding list and forwards the request packet to the next router.
5. When the request packet is forwarded to the router containing the desired information, the router $n$ returns the contents to the ICN router 1 in the opposite direction of the original path.

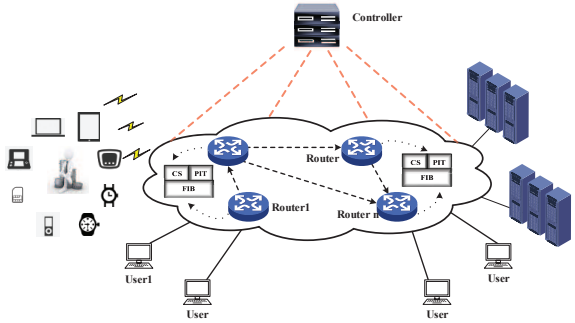



Figure 3: The working process of the combination structure

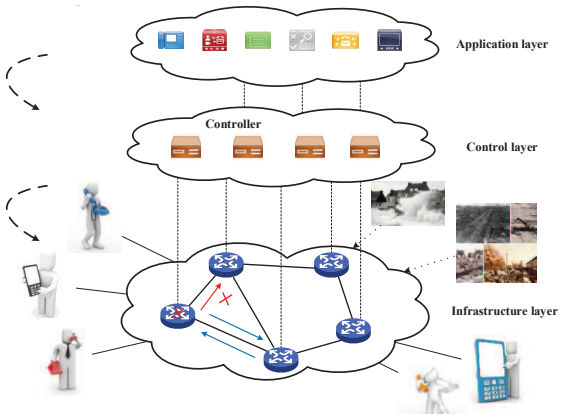



Figure 4: Network damage by disaster

6. The routers will store the information for later use during the return process.

7. The user 1 receives the required content.

Due to the high security, reliability, extensibility, low latency, high transmission efficiency and high resource utilization of SDN-ICN. It is a great potential network in the future. Whether in packet forwarding or real-time monitoring, the model plays a crucial role in the future network architecture. Moreover, it reduces network congestion and transmission time during the client gets resources nearby.

### 3.2 Security issues related to natural disasters

When natural disaster happens, the part of network is damaged, which results in the users cannot get the required data from the nearest router. Therefore, the network needs a policy to rapidly restore the network system for users. In addition, the maintenance crews need to know the location of the trouble quickly.

For the combination of SDN and ICN, this model can solve the above issues. Because of the global monitoring function of SDN controller and dynamical cache of ICN, on the one hand, the controller can get the link information periodically. On the other hand, the user can get the data requested previously from the secondary router. Thus, the system will not be severely affected, the detailed process is shown in the Figure 4.

### 3.3 Security issues related to malicious damage

The current network system has been subjected to malicious invasion and destruction (i.e., invasion, tampering, and falsification) due to the use of IP address. In addition, the traditional network system has no monitoring module to supervise the overall network. Finally, The user system was damaged and even paralyzed.

In the combination model, the controller of SDN has the global view of network and gets the updating status message from routers periodically. Once there is an exception in network, or the controller cannot get information from routers for a long time. The controller will announce the exception and the router will make corresponding measures after receiving the instruction, e.g., the router or path which is associated with the exception will be shut down. Alternatively, the router will change the transmission path. As shown in Figure 5.

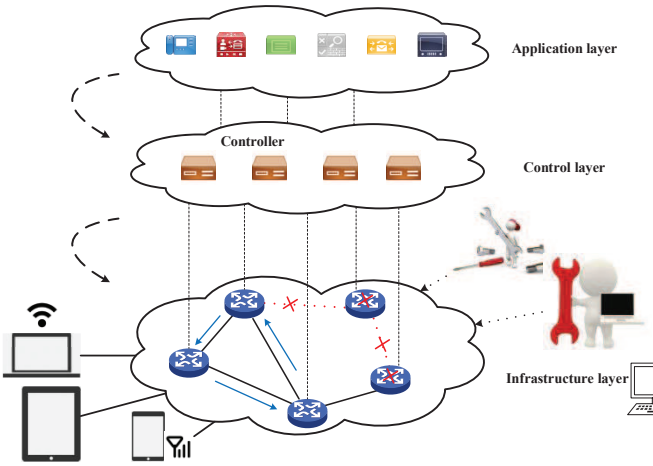



Figure 5: Network damage by malicious damage

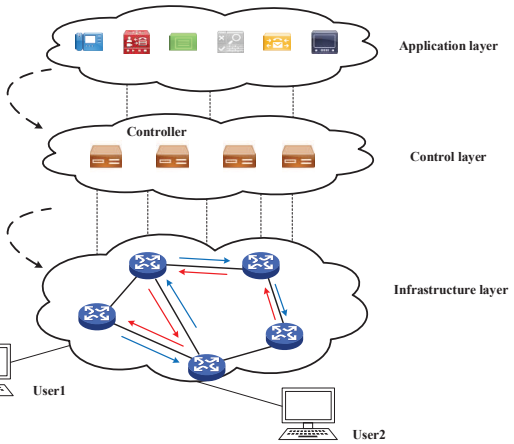



Figure 6: Network damage by system performance

### 3.4 Security issues related to system malfunction

The network data is increasing year by year, video and voice services will play an important role in the future network. Current network structure and management mechanism cannot meet the future traffic demand.

For the traditional network, there is no effective controlling policy and routing rules for preventing the system paralysis. In addition, it is true that network congestion, network latency, and massive data transmission will occur in the network, resulting in network paralysis. Thus effective routing scheme and architecture can prevent network congestion, even network crashes.

However, the combination of SDN and ICN can effectively solve above issues. The controller of SDN sends the instructions to the router after calculating the optimal path. Furthermore, the users can get the required data from the nearest router. Therefore, there is no various network data in the network. In other word, the combination of SDN and ICN promotes the robustness of network and then enhances the network security, as shown in Figure 6.

## 4 Performance validation

In this section, we evaluate the performance of the combination of SDN and ICN on security, the advantages and characteristics of the system are discussed. The results demonstrate the performances of proposed model (i.e., rapid recovery of the system, little effect for users to abstain the resources, and little related security issues of IP address).

### 4.1 System Simulation

In this part, we estimate the performance on security. We establish three security scenarios, and the recovery time of system is calculated by Dijkstra algorithm, after network was damaged. We stress the survivability of the network through the combination structure. By utilizing the optimal communication path, we analyze the whole process in detail. Finally, we demonstrate the theory and give out the comparison results.

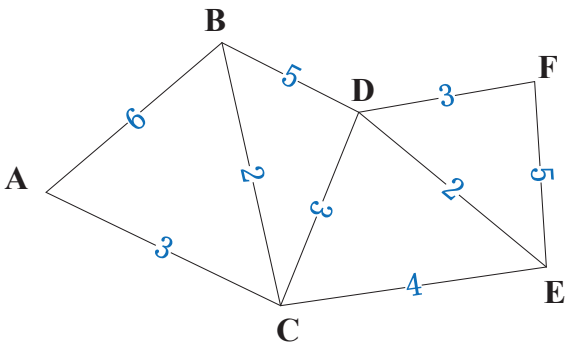



Figure 7: Dijkstra algorithm diagram

### 4.1.1 Algorithm description

- V: The set of total points.
- S: The set of vertices that have been calculated (initial time only contains source point $V_0$).
- T=V-S: A set of vertices that are not yet determined.
- $V_k$: A vertex in V.
- D[$i$]: The current length from the starting point $V_0$ (i.e., the source point) to each other vertex $V_i$.
- D[$j$] =Min D[$i$] — $V_i$=V-S: The shortest distance from $V_0$ to j.

Basis: it can prove the value of the direct path of $V_k$ from $V_0$ to T, from $V_0$ to $V_k$, or the sum of the path weights from $V_0$ through S to $V_k$.

The specific steps are shown in Figure 7.

### 4.1.2 Implementation procedures

In this section, we simulate the actual situation shown in Figure 8. When the network of sixth building and the path from first building to sixth building are damaged, the system based on the combination of SDN and ICN will recover at the fastest rate. The process of recovery is as follows:

Case 1:

- At first, when the network of sixth building and the path from first building to sixth building are damaged, the first building wants to communicate with other buildings, and then the controller of SDN will rapidly recalculate the latency of path to recover the network.
- The latency from building 1 to building 2 is 7ms, the latency from building1 to building 3 is 9ms, and the latency from building 1 to other places is Inf. Thus, the shortest latency from building 1 to building 2 is 7ms.
- Set building 2 as the middle node, building 1-building 2-building 3=17ms, which is longer than building 1-building 3=9ms. Then change it. Building 1-building 2-building 4=22ms, building 1-building 2-other building=Inf. Thus, the shortest latency from building 1 to building 3 is 9ms.

Table 1: Algorithm steps

| Steps | S set | T set |
|---|---|---|
| 1 | Select A, and then S =[ A ]<br>The shortest path A to A=0<br>Take A as the middle point and start at A | U=[B,C,D,E,F]<br>A to B=6,A to C=3,A to others=inf<br>Find: A to C is the shortest path |
| 2 | Select C, and then S=[ A,C]<br>The shortest path A to A=0,A to C=3<br>Take C as the middle point and start at the path (A to C=3) | U=[B,D,E,F]<br>A to C to B=5(shorter than the A to B=6)<br>The latest right from A to B: A to C to B=5<br>A to C to D=6, A to C to E=7<br>A to C to others=inf<br>Find: A to C to B is the shortest path |
| 3 | Select B, and then S=[A, C, B]<br>The shortest path A to A = 0,A to C=3<br>A to C to B=5<br>Take B as the middle point and start at the path (A to C to B=5) | U=[D,E,F]<br>A to C to B to D=10 (longer than the A to C to D=6)<br>The latest right from A to D: A to C to D=6<br>A to C to B to others=inf<br>Find: A to C to D is the shortest path |
| 4 | Select D, and then S=[A, C, B, D]<br>The shortest path A to A = 0,A to C=3<br>to C to B=5, A to C to D=6<br>Take D as the middle point and start at the path(A to C to D=6) | U=[E,F]<br>A to C to D to E=8 (longer than the A to C to E=7)<br>The latest right from A to E: A to C to E=7<br>A to C to D to F=9<br>Find A to C to E=7 is the shortest path |
| 5 | Select E, and then S=[A, C, B, D, E]<br>The shortest path AA=0,A to C=3<br>A to C to B=5,A to C to D=6, A to C to E=7<br>Take E as the middle point and start at the path (A to C to E=7) | U=[F]<br>A to C to E to =12(longer than the A to C to D to F=9)<br>The latest right from A to F: A to C to D to F=9<br>Find: A to C to D to F=9 is the shortest path |
| 6 | Select F, and then S=[A, C, B, D, E, F]<br>The shortest path A to A=0,A to C=3<br>A to C to B=5,A to C to D=6,A to C to E=7,A to C to D to F=9 | The U is empty and finished |

- Set building 3 as the middle node, building 1-building 3-building 4=20ms, which is shorter than building 1-building 2-building 4=22ms, building 1-building 3-other buildings=Inf. Thus, the shortest latency from building 1 to building 4 is 20ms.

- Set building 4 as the middle node, building 1-building 3-building 4-building 5=26ms, which is shorter than building 1-building 2-building 4-building 5=28ms. Thus, the shortest latency from building 1 to building 5 is 26ms.

- All the shortest latency from building 1 to other buildings is as follows:
  Building 1-building 2=7ms;
  Building 1-building 3=9ms;
  Building 1-building 4=20ms;
  Building 1-building 5=26ms;

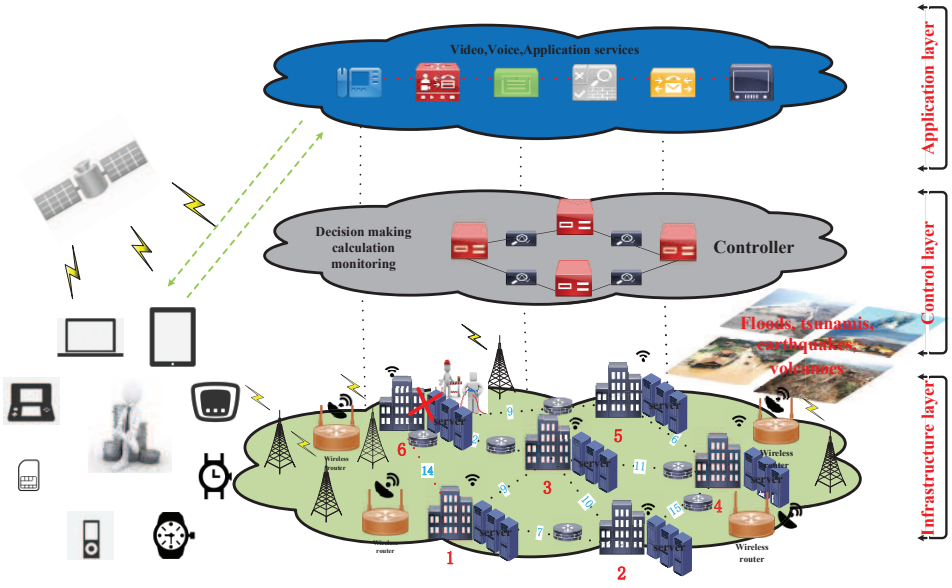



Figure 8: Network topology for case 1.

- Finished

Case 2:
There is a similar conclusion under another topology, as shown in the follows:

- At first, when the network of sixth building and the path from first building to sixth building are damaged, the first building wants to communicate with other buildings, and then the controller of SDN will rapidly recalculate the latency of path to recover the network.
- The latency from building 1 to building 2 is 2ms, the latency from building 1 to building 5 is 3ms, and the latency from building 1 to other places is Inf. Thus, the shortest latency from building 1 to building 2 is 2ms.
- Set building 2 as the middle node, building 1-building 2-building 5=11ms, which is longer than building 1-building 5=3ms. Then change it. Building 1-building 2-building 3=6ms, building 1-building 2-other building=Inf. Thus, the shortest latency from building 1 to building 5 is 3ms.
- Set building 5 as the middle node, building 1-building 5-building 3=8ms, which is longer than building 1-building 2-building 3=6ms, building 1-building 5-building 4=5ms. Thus, the shortest latency from building 1 to building 4 is 5ms.
- Set building 4 as the middle node, building 1-building 5-building 4-building 3=8ms, which is longer than building 1-building 2-building 3=6ms. Thus, the shortest latency from building 1 to building 3 is 6ms.
- All the shortest latency from building 1 to other buildings is as follows:
  Building 1-building 2=2ms;
  Building 1-building 3=6ms;
  Building 1-building 4=5ms;
  Building 1-building 5=3ms;

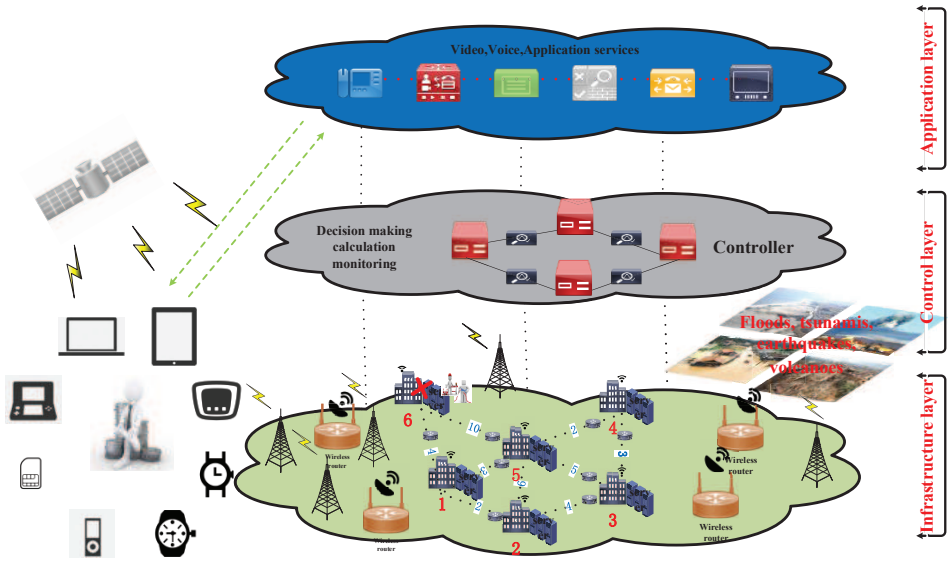



Figure 9: Network topology for case 2.

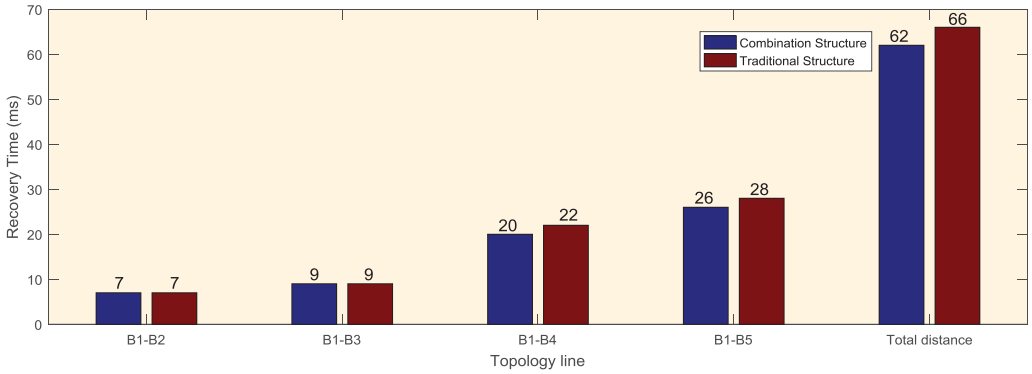



Figure 10: Comparison results in case 1

- Finished

After the controller recalculated the path, the users want to get the content which was required previously, the structure is convenient for users to get the content because of the caching function of ICN router. If the building node including the caching content is damaged, the users do not need to research the content from the other nodes. They can get the content through the secondary path, which reduces the transmission latency.

In short, the combination of SDN and ICN is beneficial to the network recovery. The first one is that the SDN is used for the first routing on reconfiguration, the other is that the ICN is benefit for users to get the repeated required services. We just think about two damaged conditions in building1. Of course, we can also consider other building nodes, and the corresponding process is the same as previous mentions.

The following is the result of the second scenario we mentioned:

### 4.1.3 Data analysis

Through the above process, we can compare the performance of system based on the combination struc-

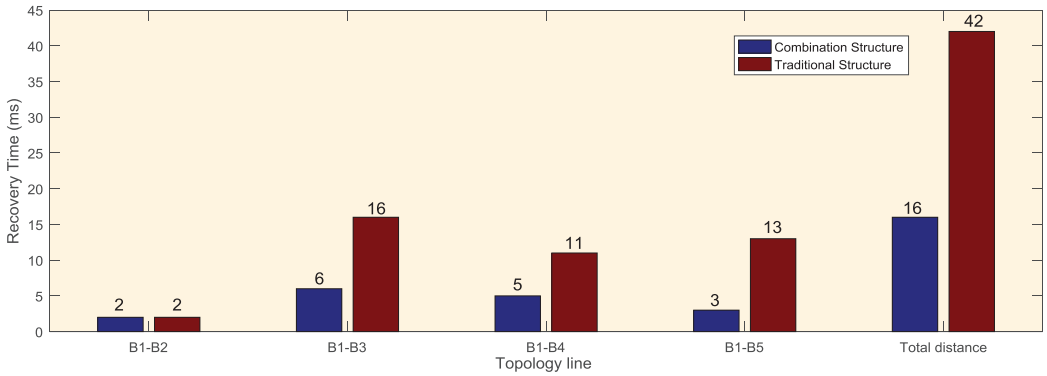



Figure 11: Comparison results in case 2

ture with traditional network structure. And, then we know that the damaged system can be recovered quickly by using the combination network, this structure reduces the transmission latency, improves the quality of experience for users, promote the survivability of system, and users will not feel the interruption of services.

The comparison results between the combination structure and traditional structure are shown in Figure10 and Figure11. After the attack and damage of network, the combination network will be used to provide service for users with the shortest distance.

## 5 Conclusion and Future Work

In this paper, we analyzed the network architecture of SDN and ICN technology from security aspect. Then, we introduced the current condition of the Internet and the problems that need to be solved urgently. The SDN and ICN structure were analyzed to highlight their functions respectively. We discussed the combination model of SDN and ICN based on the working process and its characteristics. Furthermore, we divided the security issues into three aspects (natural disaster, malicious damage, and system self-defect) and analyzed them. The performance of the combination model was introduced. The demonstration shows that the network can recover quickly based on the proposed model.

In short, the combination of SDN and ICN may have a huge impact on Internet technology security in the future. At present, SDN and ICN architecture are attracting more and more scientists and technical experts. We hope the analysis and discussions in this paper will bring benefits to future research. We will integrate other network technologies (Big data, Cloud computing, Data center, and wireless access network) [18, 17, 11, 5] to make the network more secure and reliable.

## Acknowledgments

We would like to thank all the reviewers and editors for their invaluable comments and efforts on this article. This work was supported by the Project of State Grid Corporation of China under Grant no. SGRIXTJSFW[2016]377.

## References

[1] M. Arumaithurai, J. Chen, E. Maiti, and X. Fu. Prototype of an icn based approach for flexible service chaining in sdn. In *Proc. of the 2015 IEEE Conference on Computer Communications Workshops (INFOCOM*

*WKSHPS'15), Hong Kong, China*, pages 5–6. IEEE, April 2015.

[2] M. R. Celenlioglu and H. A. Mantar. A scalable routing and admission control model in sdn-based networks. In *Proc. of the 2014 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS'14), Marina del Ray, California, USA*, pages 231–232. IEEE, October 2014.

[3] D. Chang, M. Kwak, N. Choi, and T. Kwon. C-flow: An efficient content delivery framework with openflow. In *Proc. of the 2016 International Conference on Information Networking (ICOIN'14), Phuket, Thailand*, pages 270–275. IEEE, February 2014.

[4] Cisco. Cisco annual cybersecurity report. Technical report, Cisco, 2017.

[5] A. Dambreville, J. Tomasik, J. Cohen, and F. Dufoulon. Load prediction for energy-aware scheduling for cloud computing platforms. In *Proc. of the 37th IEEE International Conference on Distributed Computing Systems (ICDCS'17), Atlanta, Georgia, USA*, pages 2604–2607. IEEE, June 2017.

[6] T. Dargahi, A. Caponi, M. Ambrosin, G. Bianchi, and M. Conti. A survey on the security of stateful sdn data planes. *IEEE Communications Surveys & Tutorials*, 19(3):1701–1725, 2017.

[7] S. Eum, M. Jibiki, M. Murata, H. Asaeda, and N. Nishinaga. A design of an icn architecture within the framework of sdn. In *Proc. of the 7th International Conference on Ubiquitous and Future Networks (ICUFN'15), Sapporo, Japan*, pages 141–146. IEEE, July 2015.

[8] C. Fang, F. R. Yu, T. Huang, J. Liu, and Y. Liu. A survey of green information-centric networking: Research issues and challenges. *IEEE Communications Surveys & Tutorials*, 17(3):1455–1472, 2015.

[9] A. Gupta, S. Shailendra, and A. Girish. Analysis of in-network caching for icn. In *Proc. of the 2016 IEEE Annual India Conference (INDICON'16), Bangalore, India*, pages 1–5. IEEE, December 2017.

[10] X. He, Z. Ren, C. Shi, and J. Fang. A novel load balancing strategy of software-defined cloud/fog networking in the internet of vehicles. *China Communications*, 13(S2):140–149, 2016.

[11] R. H. Hwang and H. P. Tseng. Load balancing and routing mechanism based on software defined network in data centers. In *Proc. of the 2016 International Computer Symposium (ICS'16), Chiayi, Taiwan*, pages 165–170. IEEE, February 2017.

[12] A. Kalghoum and S. M. Gammar. Towards new information centric networking strategy based on software defined networking. In *Proc. of the 2017 Wireless Communications and Networking Conference (WCNC'17), San Francisco, California, USA*, pages 1–6. IEEE, March 2017.

[13] KPCB. Internet trend report. Technical report, KPCB, 2017.

[14] J. S. B. Martins and M. B. Campos. A security architecture proposal for detection and response to threats in sdn networks. In *Proc. of the 2016 IEEE ANDESCON, Arequipa, Peru*, pages 1–4. IEEE, October 2017.

[15] J. Son, D. H. Kim, H. S. Kang, and C. S. Hong. Forwarding strategy on sdn-based content centric network for efficient content delivery. In *Proc. of the 2016 International Conference on Information Networking (ICOIN'16), Kota Kinabalu, Malaysia*, pages 220–225. IEEE, January 2016.

[16] N. L. M. van Adrichem and F. A. Kuipers. Ndnflow: Software-defined named data networking. In *Proc. of the 1st IEEE Conference on Network Softwarization (NetSoft'15), London, UK*, pages 1–5. IEEE, April 2015.

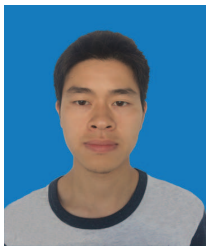
[17] K. Wang, Y. Wang, D. Zeng, and S. Guo. An sdn-based architecture for next-generation wireless networks. *IEEE Wireless Communications*, 24(1):25–31, February 2017.

[18] J. Zhao and M. Chen. Under the vision of the big data: The internal causes of economic transformation. In *Proc. of the 3rd International Conference on Big Data Security on Cloud (BigDataSecurity'17), IEEE International Conference on High Performance and Smart Computing (HPSC'17), and IEEE International Conference on Intelligent Data and Security (IDS'17), Beijing, China*, pages 122–126. IEEE, May 2017.

## Author Biography

**ZHENG-YANG AI** received the B.S. degrees in School of Computer and Information Technology from Northeast Petroleum University in 2016. Currently he is a Ph.D. student in the National Engineering Laboratory for Next Generation Internet Technology, School of Electronics and Information Engineering, Beijing Jiaotong University. His current research interests include network architecture and network security.

**FEI SONG** is with the National Engineering Laboratory for Next Generation Internet Technology, School of Electronics and Information Engineering, Beijing Jiaotong University. His current research interests include network architecture, network security, protocols optimization, wireless communications, and cloud computing. He also serves as a technical reviewer for several journals, including the IEEE Transactions on Services Computing, IEEE Transaction on Parallel Distribution System, IEEE Transaction on Emerging Topics in Computing.



**XI WANG** received the B.S. degrees in School of Information and Communication Engineering from Beijing Information Science and Technology University in 2017. Currently he is a master student in the National Engineering Laboratory for Next Generation Internet Technology, School of Electronics and Information Engineering, Beijing Jiaotong University.