

Rapidly Deployed Cyber Attack Bait Based on Software Defined Network Corresponding to Artificial Intelligence Strategy

Ming-Shen Jian^{1,*}, Bo-Yi Lee², Xing-En Liu¹, Rui-Lun Cai¹, Zhong-Wei Cai¹, Pei-Cen Liao¹, Ta-Yuan Chou²,
Wun-Yuan Huang²

¹CCIS Lab., Dept. of CSIE, National Formosa University, Yunlin County, Taiwan 632

²National Center for High-Performance Computing, Taiwan

jianms@nfu.edu.tw*, 1203007@narlabs.org.tw

Abstract— To protect the services and data of the main servers, Rapidly Deployed Cyber Attack Bait is proposed for the unpredictable cybersecurity attack in this research. Based on Software Defined Network, the data packet and operation of cybersecurity attack could be redirected to the on demand deployed bait container. By suitable artificial intelligence strategy, the idle bait containers corresponding to the type of cybersecurity attack can be on demand deployed automatically and rapidly. Verification shows the feasibility of the virtualized bait container could be about 1.16 times to 2 times enough for the future coming attacker and also record the all operations of the cybersecurity attack individually.

Keywords— cybersecurity, bait, Software Defined Network, Artificial Intelligence, container

I. INTRODUCTION

Cyber-attack of the network service and digital data was existed for a long time. In addition to the network transmission security issues such as Phishing attack, man-in-the-middle attack, DNS record forgery, etc., SQL injection attack, ransomware, Password attack, Brute force attack, insider threat, Malware, XSS attack, etc., which would change the file or content of the local devices. Through the network, various types of cyber attacks would damage the information systems. Data stealing, file encrypted due to ransomware, Data tampering or monitoring remotely, etc., always make the security more and more important.

Although the Security and protection mechanisms were proposed, to trace and track the behaviour and patterns of the hackers is required for finding the new possible security risks [1]. In addition to the real time monitoring, the bait for the security issues such as behaviour and patterns of the hackers is also proposed [2,3,16-19]. Then, based on the collected

data about the behaviour and patterns, the response or improvement of the security based on artificial intelligence could be developed [4].

Recently, artificial intelligence (AI) is popular and generally used in industry or information system. Generally speaking, a small AI models or service can be built and deployed with enough computing resource for specific functions or purposes. To parallel and distribute the computing missions of AI service into multiple computing nodes could be a possible method [5,6]. Furthermore, considering the possible types of cybersecurity issue, develop the independent AI service or module for the corresponding cybersecurity topic would enhance the accuracy of crisis response.

Since rapidly deploy the cybersecurity baits with AI module would need the computing resource, dynamical deployment of the bait corresponding to the identified cybersecurity crisis or attack could save the limited computing resource. In other words, the bait could be the “Security Crisis as a Service” for deployment corresponding to the cybersecurity crisis or attack [7]. Hence, when a network incoming connection is identified as the cybersecurity crisis or attack, the corresponding bait with specific pre-trained AI modules could be deployed for to the current connection.

To rapidly deploy the bait, virtual machine (VM) or Docker container on cloud platform can be the solution for computing resource and bait service management. There exists the virtual network for the deployed containers and VMs that also works similar to the physical network. To deliver the

attack or high risk data packet to the bait instead of the original terminal, Software Define Network (SDN) should be considered [8-11]. Based on OpenFlow protocol, rapidly delivering the data packets to the corresponding destination nodes can be achieved.

The contributions of this research can be shown as follows:

1. Based on Cloud environment and Docker container, the cybersecurity and attack bait could be rapidly and repeatedly deployed. In addition, the current status of each bait can be saved and maintained for further research or the next trick for hackers.
2. Based on SDN, the judged connection and data packets can be delivered to the corresponding bait containers. In addition, the SDN can re-direct the connection to the on demand deployed AI strategy for attack recording and analysis.
3. Based on the proposed system structure, the services or applications can be deployed on multiple similar containers. Each module or partition of the whole service can be distributed into different containers. In other words, the services can be quickly recovered for the normal users by re-deploying the containers. The hacker and normal users can be separated into different containers. Security risk can be reduced.

The organizations of this research are shown as follows. Section 2 gives the related works. Section 3 introduces the proposed system. Section 4 provides the verification and laboratories. The conclusion is given in section 5.

II. RELATED WORKS

Software Define Network (SDN) includes three independent layers: Infrastructure Layer, Control Layer, and Application Layer. Infrastructure Layer consists of multiple switches. Each switch only needs to support the OpenFlow protocol. The Control Layer is the main software for the network connection management. Application Layer could be the firewall or load balancing services. Therefore, without changing the physical hardware, main software in Control Layer could control and

manage the whole network according to the on demand given programs [8-11].

Since there are various types of network security issues, attack scenarios that can be applied to the corresponding network vulnerabilities would be the most important research topics. Bait machines for the security issues were proposed and generally used [2,3,16-19]. Corresponding to the specific type or network vulnerability of the security issue, there will be some on demand given weakness of security deployed on the computer or network node. Therefore, when a malicious user tries to attack the node and finds the available security weakness, the information gathering related to attack preparation should be done first. The bait now could provide the on demand given weakness of security to malicious user. Hence, the malicious user would be cheated and attack the bait instead of the node that actually provides services. Recently, an open source intrusion prevention system, SNORT, is generally used for defining malicious network activity [12-15]. SNORT system can also use the rules to find packets which match malicious network activity and generates alerts for users. Hence, when the SNORT find the malicious user or data packets, the corresponding bait through the network could be used.

Honeypot [16-19], a bait for network malicious user, is usually disguised as seemingly valuable networks, data, and computer systems. It is intentionally buggy to attract hacker attacks. In addition, honeypot may also be equipped with monitoring software to monitor hackers' actions after intrusion.

Artificial intelligence (AI) recently was generally used in various applications and services [4,5,11,15]. Considering the possible types of attack from network, to monitor and predict the possible security risk and attack based on the AI module could be the solution [4,11,15]. After training, the services could be protected according to the protection of machine learning method and SDN [11]. Through Anomaly Detection based on machine learning, SNORT could find the possible security risk of the current connection [15].

However, to deploy the physical bait machine or honeypot corresponding to various types of cybersecurity risk and attack would cause the cost

and computing resource. In addition, without adopting suitable defence strategy of cybersecurity, the bait or honeypot would be found or revealed easily by the attacker or hacker. Hence, how to prepare enough bait system or service corresponding to the current coming identified cyber-attack would be an important issue.

III. PROPOSED SYSTEM

In this research, three partitions are proposed for the cyber-attack bait deployment based on SDN corresponding to artificial intelligence strategy: rapidly corresponding bait deployment, artificial intelligence cyber-attack speculation, and dynamic network configuration.

The system structure can be shown as Figure 1. The network packet from remote user with security risk would be delivered by RYU controller for further checking according to the database in SNORT. If the packet is identified as the cyber-attack or packet with high security risk, the RYU controller would command the SDN for the packet re-direction. According to the proposed Rapidly Corresponding Bait Deployment method, there will be the bait container corresponding to the identified type of cyber-attack or risk for the further monitoring and observation. In addition, according to the proposed Artificial Intelligence cyber-attack Speculation, there are always enough idle containers for the corresponding types of possible coming cyber-attack.

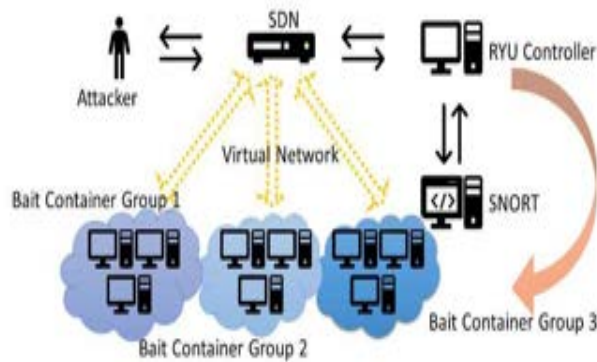


Figure 1. The structure of the proposed system

Rapidly Corresponding Bait Deployment

Since the time, types, and total amount of cyber-attack cannot be predicted, to prepare huge amount of various types baits for unpredictable cyber-attack

is not feasible. Hence, how to provide just enough baits corresponding to the type of current cyber-attack would be the issue.

Suppose that the cyber-attack bait can be included and packaged in the Docker container. The Docker engine could deploy the chosen image as the independent container for services providing. One image could be rapidly deployed as the multiple containers which provide service individually and independently.

In this research, each type of the cyber-attack bait is formatted as the single Docker image. The container corresponding to the currently coming cyber-attack can be deployed when required. Considering the unpredictable cyber-attack, the statistical data of the past cyber-attack could be used as the possibility or probability of the new coming cyber-attack. Hence, assume that α_T is the threshold value, α_i is the percentage value of i^{th} type cyber-attack among all the past cyber-attack. for on demand deployment of the bait container. In other words, according to the statistical data, there will be several types of bait container individually on demand deployed when

$$\alpha_i \geq \alpha_T \text{ where } \sum \alpha_i = 1$$

Therefore, when the new cyber-attack coming, there would be at least one container with high probability matching the type of cyber-attack. The delay for network cyber-attack data packet transmission or container deployment can be reduced.

Every time a bait container is used or occupied, the proposed Rapidly Corresponding Bait Deployment method could immediately deploy a new same cyber-attack bait container immediately. If the trend of the specific cyber-attack type increases, it means that the corresponding bait container requires extensive deployment. Suppose that the trend of the specific cyber-attack can be presented as β_i where i indicate the i^{th} type of cyber-attack.

$$\beta_i = \frac{CA_i(t)}{CA_i(t-1)} \text{ and } CA_i(t-1) \neq 0$$

where $CA_i(t)$ indicates the total number of the i^{th} type cyber-attack at time t . Only when the i^{th} type cyber-attack continuously happens, the β can be counted. In the beginning, each type of cyber-attack

will be assigned at least 1 container. When cyber-attack happens, the existed first container will be assigned to the current coming cyber-attack. At the same time, the second container corresponding to the current coming cyber-attack will be deployed immediately. Then, if there exists more than two same type cyber-attack, the proposed Rapidly Corresponding Bait Deployment method would deploy total γ containers of i^{th} type cyber-attack for the next time period $t+1$ by the following equations:

$$\gamma(t+1) = CA_i(t) \times \beta_i$$

Hence, we can formulate the evaluation function for total γ container deployment as follows:

$$\gamma(t+1) = \begin{cases} 1 & \text{initial or no attack} \\ 2 & \text{1 attack exists} \\ CA_i(t) \times \beta_i & \geq 2 \text{ attack} \end{cases}$$

Therefore, when the total number of i^{th} type cyber-attack continuously increases, the proposed Rapidly Corresponding Bait Deployment method could deploy the possibly enough containers corresponding to i^{th} type cyber-attack for the next time period. The following figure shows two scenarios of the increasing cyber-attack.

IV. VERIFICATION AND RESULTS

To verify the rapidly corresponding bait deployment, in scenario 1, the total summation of the cyber-attack would increase 1 by every time period. In scenario 2, the total summation of the cyber-attack would randomly increase between value 1 to 3. The predicted new deployed total γ container for time period $t+1$ could be always 1 more than the attack in scenario 1. Even in scenario 2, predicted new deployed total γ container can still satisfy the total number of cyber-attack at time period $t+1$. It means that there are always about 1.16 times to 2 times enough bait containers for the future possible coming cyber-attack.

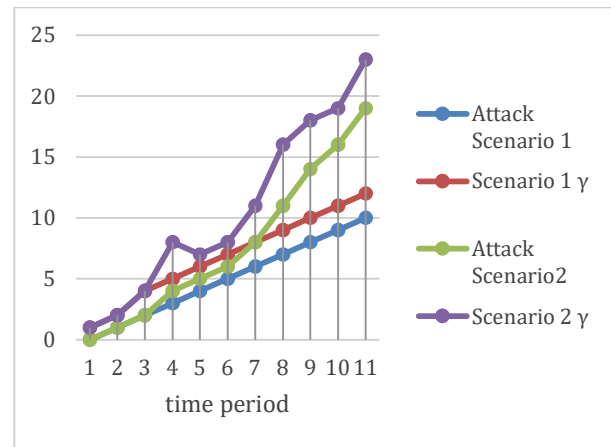


Figure 2. The example of the deployed γ container for time period $t+1$ versus different attack scenario

To verify the bait containers and network structure based on the SDN, the bait container, attacker, and SDN computing node are configured with different IP address

When the attacker tries to access the service server, the data packets would be checked by the SNORT. In this verification, we would require the Ryu controller to redirect all the data packet from the attacker to the bait container. Therefore, all the operation from the attacker would be indeed executed on the bait container. In addition, all the operation would be recorded in the log file. Figure 3 shows the redirection result on bait container. The bait container receives the data packet from the attack 192.168.127.1.

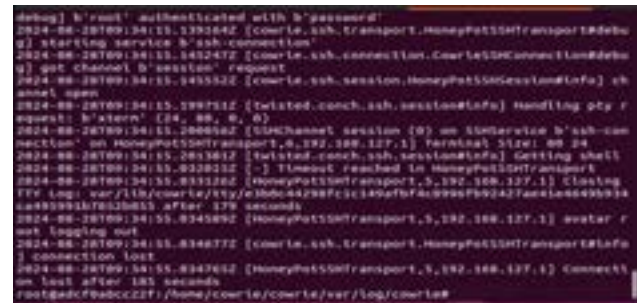


Figure 3. The data packet redirection result on bait container

Figure 4 (a) shows the operation done by the attacker. The attacker keeps the connection to the server on IP address 192.168.127.137. All the data packets of operations are redirected to the bait

which is on IP address 127.17.0.2. Hence, in Figure 4 (b), via reviewing the log file on bait container, we could see that all the operations from the 192.168.127.1 are recorded. In other words, the attacker could not aware that the operations are already redirected and now is baited. The server on IP address 192.168.127.137 could still provide the service without the attack risk.

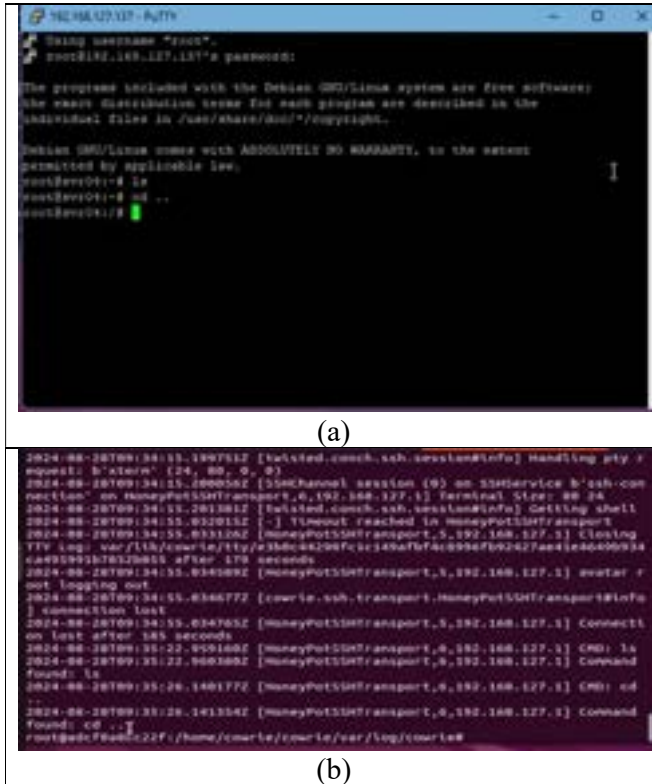


Figure 4. The (a) screen shot related on attacker side with server connection and operation, (b) log file information on bait

V. CONCLUSIONS

According to the proposed Rapidly Deployed Cyber Attack Bait, the attacker could be redirected to the bait instead of service server. Attackers could not aware of the data packet redirection. Based on the Software Defined Network Corresponding to Artificial Intelligence Strategy on cloud and Docker, it is possible for the security defence automatically executed.

ACKNOWLEDGEMENT

This research is also guided by the National Center for High-Performance Computing.

REFERENCES

- [1] I. Ghafir, V. Prenosil, J. Svoboda and M. Hammoudeh, "A Survey on Network Security Monitoring Systems," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 2016, pp. 77-82, doi: 10.1109/W-FiCloud.2016.30.
- [2] S. Vasylyshyn, I. Oprisky and V. Susukailo, "Analysis of the use of software baits as a means of ensuring information security," 2020 IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT), Zbarazh, Ukraine, 2020, pp. 242-245, doi: 10.1109/CSIT49958.2020.9321925.
- [3] P. Bajaj and M. Edwards, "Automatic Scam-Baiting Using ChatGPT," 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Exeter, United Kingdom, 2023, pp. 1941-1946, doi: 10.1109/TrustCom60117.2023.00264.
- [4] Y. Sharma, V. Kumar and H. Chaudhary, "Attack Detection on Internet of Things Devices using Machine Learning Techniques," 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2023, pp. 281-287, doi: 10.1109/ICICCS56967.2023.10142701.
- [5] M. -S. Jian, J. -T. Gui, X. -M. Wu, "Uncentralized Artificial Intelligence Computing Agent with the Distributed Training and Computing Tasks Based on Open Source Cloud Proxy," CSCE 2023 - ICAI, Las Vegas, USA, p.93. (ISBN:1-60132-518-5)
- [6] M. -S. Jian, Y. -Z. Luo, P. -W. Wang and T. -Y. Lai, "Cloud and Edge Computing Based Movable 3D Dynamic Image Recognition and Analysis Layer System for Remote Biological Laboratory," 2023 25th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, Republic of, 2023, pp. 429-436, doi: 10.23919/ICACT56868.2023.10079325.
- [7] Ming-Shen Jian, Jun-Hong Shen, Kuan-Wei Lee, Yi-Chen Jhou, Chien-Tang Mai, "Cloud Based Software Computing as a Service in Hybrid Evolution Algorithm with Feedback Assistance" Journal of Electronic Science and Technology, Vol.14, Issue 4, pp.362-369, 2016.
- [8] A. H. Abdi et al., "Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI, and MTD Approaches to Security Solutions," in IEEE Access, vol. 12, pp. 69941-69980, 2024, doi: 10.1109/ACCESS.2024.3393548.
- [9] H. Liang, H. Liu, F. Dang, L. Yan and D. Li, "Information System Security Protection Based on SDN Technology in Cloud Computing Environment," 2021 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA), Dalian, China, 2021, pp. 432-435, doi: 10.1109/AEECA52519.2021.9574276.
- [10] Z. Fatehi and A. Montazerolghaem, "DDoS Detection in SDN using Deep Learning," 2024 8th International Conference on Smart Cities, Internet of Things and Applications (SCIoT), Mashhad, Iran, Islamic Republic of, 2024, pp. 201-206, doi: 10.1109/SCIoT62588.2024.10570129.
- [11] N. P. M. T, B. M. J, M. S, M. D. R and K. V. M, "Protecting Healthcare Systems Through an ML-Powered Cyberattack Detection Within Software-Defined Networking (SDN)," 2024 International Conference on Science Technology Engineering and Management (ICSTEM), Coimbatore, India, 2024, pp. 1-6, doi: 10.1109/ICSTEM61137.2024.10560593.
- [12] <https://www.snort.org/> (available 2024/07/03)
- [13] Y. Kaushik, A. Athmaraman, A. M. John and S. Sridhar Raj, "Signature-based Intrusion Prevention System for Software Defined Networks using SNORT," 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIoT), Vellore, India, 2024, pp. 1-6, doi: 10.1109/AIoT58432.2024.10574719.
- [14] M. Sheeraz, M. Hanif Durad, S. Tahir, H. Tahir, S. Saeed and A. M. Almuhaideb, "Advancing Snort IPS to Achieve Line Rate Traffic Processing for Effective Network Security Monitoring," in IEEE Access, vol. 12, pp. 61848-61859, 2024, doi: 10.1109/ACCESS.2024.3395123.

- [15] T. Preethi, P. R. Reddy, L. Likhitha, P. P. Kumar and A. Kamani, "A Novel Approach for Anomaly Detection using Snort Integrated with Machine Learning," 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2024, pp. 796-801, doi: 10.23919/INDIACom61295.2024.10498401.
- [16] S. A. Raghul, G. Gayathri, R. Bhatt and K. A. Varun Kumar, "Enhancing Cybersecurity Resilience: Integrating IDS with Advanced Honeytrap Environments for Proactive Threat Detection," 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2024, pp. 1363-1368, doi: 10.1109/ICAAIC60222.2024.10575865.
- [17] A. Albaseer, M. Hamood and M. Abdallah, "Adaptive Honeytrap Defense Deployment: A Stackelberg Game Approach with Decentralized DRL for AMI Protection," 2024 International Conference on Computing, Networking and Communications (ICNC), Big Island, HI, USA, 2024, pp. 1-5, doi: 10.1109/ICNC59896.2024.10556285.
- [18] T. Shivaprasad, A. S. Mouly and N. Guruprasad, "Enhancing Network Security through a Multi-layered Honeytrap Architecture with Integrated Network Monitoring Tools," 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2024, pp. 473-477, doi: 10.23919/INDIACom61295.2024.10498895.
- [19] Á. Balogh, M. Érsök, A. Bánáti and L. Erdödi, "Concept for real time attacker profiling with honeypots, by skill based attacker maturity model," 2024 IEEE 22nd World Symposium on Applied Machine Intelligence and Informatics (SAMI), Stará Lesná, Slovakia, 2024, pp. 000175-000180, doi: 10.1109/SAMI60510.2024.10432876.



Ming-Shen Jian was born in Kaohsiung City, Taiwan in 1978. He received the B.S. from the National Chiao Tung University, HsinChu, and Ph.D degrees in Computer Science and Engineering from the National Sun Yat-sen University, Kaohsiung, Taiwan in 2007. From 2018, he was an Associate Professor and director with the National Formosa University Cloud Computing and Intelligent System Laboratory.

Currently he is also an IEEE Senior Member. Since 2009, he has been an Assistant Professor with the Computer Science and Information Engineering Department, National Formosa University. He is the author of four books, more than 50 articles, and at least 15 invention patents. His research interests include IOT development and application, Big Data, Optimal Solution, Intelligent System, and Cloud Computing. He was a Secretary of the Taiwan Association of Cloud Computing. Dr. Jian was a recipient of the IEEE sponsored international conference Paper Award in 2016, 2017, and 2018



Bo-Yi Lee is a Ph.D. candidate in the Department of Information Management at National Sun Yat-sen University and has served as a senior engineer at the National Center for High-Performance Computing. He possesses extensive experience in various fields, including cyber security architecture design, malware analysis, and intrusion detection. His primary research interests focus on network threat detection through data-driven threat intelligence and machine learning

techniques.



Xing-En Liu currently is a bachelor degree student of Dept. Computer Science and Information Engineering at National Formosa University. His current research interests are in the area related to Cloud Computing and Docker container services, security, and intelligent system. He joins the Cloud Computing and Intelligent System Lab. (CCIS Lab.) from 2022.



Rui-Lun Cai currently is a bachelor degree student of Dept. Computer Science and Information Engineering at National Formosa University. His current research interests are in the area related to Cloud Computing and Docker container services, and security services. He joins the Cloud Computing and Intelligent System Lab. (CCIS Lab.) from 2022.



Zhong-Wei Cai currently is a bachelor degree student of Dept. Computer Science and Information Engineering at National Formosa University. His current research interests are in the area related to Cloud Computing and Docker container services, security, and intelligent system. He joins the Cloud Computing and Intelligent System Lab. (CCIS Lab.) from 2022.



Pei-Cen Liao currently is a bachelor degree student of Dept. Computer Science and Information Engineering at National Formosa University. His current research interests are in the area related to Cloud Computing and Docker container services, security, and intelligent system. He joins the Cloud Computing and Intelligent System Lab. (CCIS Lab.) from 2023.



Ta-Yuan Chou received the Ph.D. degree at the department of computer science and engineering, National Sun Yat-Sen University, Kaohsiung, Taiwan, R.O.C in 2008. He is an assistant researcher in National Center for High-Performance Computing. His doctoral research mainly focuses on evolutionary computation, multiobjective optimization, and scheduling problems. His current research interests include various open networking technologies, such as software defined network, and P4 programming.



Wun-Yuan Huang received his BS degree in Information and Computer Engineering from Chung Yuan Christian University, Taiwan, in 2006, and his MS degree in Computer Science and Information Engineering from National Dong Hwa University, Taiwan, in 2009. He is currently an associate researcher at the National Center for High-Performance Computing. His primary research focuses on SDN, threat deception, and the deployment of honeypots.