Benefit Optimization of SDN Honeynet System Based on Mimic Defense

Desheng Zhang and Lei Chen(✉)

Jiangsu Province Key Laboratory of Intelligent Industry Control Technology, Xuzhou University of Technology, Xuzhou 221018, China
chenlei@xzit.edu.cn

Abstract. The role of Internet technology applications in the overall economic and social development is becoming more and more obvious and the risks and challenges it brings are also increasing, and cyberspace threats and risks are increasing. In recent years, software-defined networks have provided new solutions for the field of cyberspace security with the characteristics of simplicity, rapid deployment and maintenance, flexible expansion, and openness. Mimic defense is based on the dynamic heterogeneous redundant structure of the endogenous security mechanism in cyberspace, and provides a brand new defense idea in the face of various threats. Combining SDN and mimic defense technology to form a more powerful intelligent honeynet has become a new research direction in network security. Based on the predecessors, this paper constructs a SDN-based mimic defense honeynet. Through theoretical calculations, the benefits of both offense and defense are affected by various data, and find the optimal solution in the mimic defense honeynet, and verify each This kind of data reasoning finally achieves the optimal benefit of the defense system.

Keywords: Mimic defense · Software defined network · Honeynet · Intrusion detection system

1 Introduction

In recent years, the large-scale development of new technology applications such as cloud computing [1, 2], artificial intelligence [3, 4], big data [5, 6], and the Internet of Things [7] in developing countries has been applied to many previous Some people have never had a preliminary experience, such as applications in smart cities [8, 9], smart medical [10, 11], Internet of Vehicles [12] and so on. These technologies require a more powerful basic network, especially many rely on the mobile Internet [13, 14]. With the rapid development of modern networks, cyberspace security is also facing new problems and challenges [15]. Many network attack methods have begun to merge, interchange and quickly development of. However, traditional network security defense technologies, such as firewall [16], intrusion detection [17, 18], etc., face many limitations in the face of evolving network attack technologies, among which existing defenses have been discovered by some Vulnerabilities, viruses, etc., require a certain accumulation of

H. Song and D. Jiang (Eds.): SIMUtools 2020, LNICST 370, pp. 266–277, 2021.
https://doi.org/10.1007/978-3-030-72795-6_21

technology. Most of the attacks used by the attackers are hidden and unknown threats and breakthroughs.

Honeynet [19] is an active defense [20] technology, which can deceive the attacker to turn into what he wants to attack. At the same time, after capturing the attack behavior, it can analyze the attacker's attack strategy and attack. Methods, targets, etc. These data can be repaired and expanded to enhance the defense capabilities of their own systems. Furthermore, digital forensics [21] can be used to outline the characteristics of the attacker's portrait, etc., which can be used as the basis for reverse investigations. However, traditional honeynet deployment is very complicated, costly, dynamic adjustment is complicated, and flow control is difficult. Faced with the modern network environment, neither can it be adjusted in time according to changes in network traffic, nor can it obtain effective information from the attacker.

SDN [22] is a technology developed in the face of increasingly large, complex, and diverse network environments. SDN realizes the separation of data control and data transmission, in order to achieve extremely excellent traffic analysis [23, 24] control Ability, a more flexible dynamic adjustment [25] capability, is just suitable for the deployment of honeynets, and it can also make certain predictions [26], and defend the network structure of honeynets according to the predicted results [27, 28]. Mimic defense [29, 30] is proposed by Academician Wu Jiangxing to solve the problem of inequality in defense and defense. Through a large number of overlapping dynamic scheduling, the attacker can become unknown, change, and the effect of both time and space. Mimic defense Can better conceal or camouflage the defensive scene and defensive behavior of the target object, so that the target object can obtain a more reliable advantage in the continuous, extremely concealed, high-intensity man-machine attack and defense game [31], especially In the face of the current biggest security threat-unknown breakthrough backdoors, virus Trojan horses and other infinite threats, it has significant effects and overcomes many problems of traditional security methods. The honeynet of mimic defense is realized through SDN, and end-to-end network control [32, 33] is realized, which realizes a honeynet with convenient deployment, flexible dynamic scheduling and powerful functions. A large part of the effect of the honeynet is that the IDS server can accurately identify attacks, and can accurately handle the geographical balance to deal with normal user access and abnormal operations. IDS servers can use different identification strategies when working. Here we analyze different Security strategy has a defensive impact on honeynets and how to choose the best strategy.

2 Problem Introduction

First, construct the basic honeypot network structure as shown in Fig. 1. Use multi-interaction honeypots to connect to each other through the network to simulate the simulation working network, which can be simulated as a We b server, file server, etc., when the attacker enters, it will be mistaken I thought I had successfully entered the target's work network. Before the target enters, it must pass through the firewall and IDS server. After IDS analysis, it is determined whether the target traffic goes to the real server or the honeypot server. For the attacker's traffic, network managers can analyze the attack process, attack vulnerabilities, tools used, and so on. In order to achieve the effect of making the system more secure.

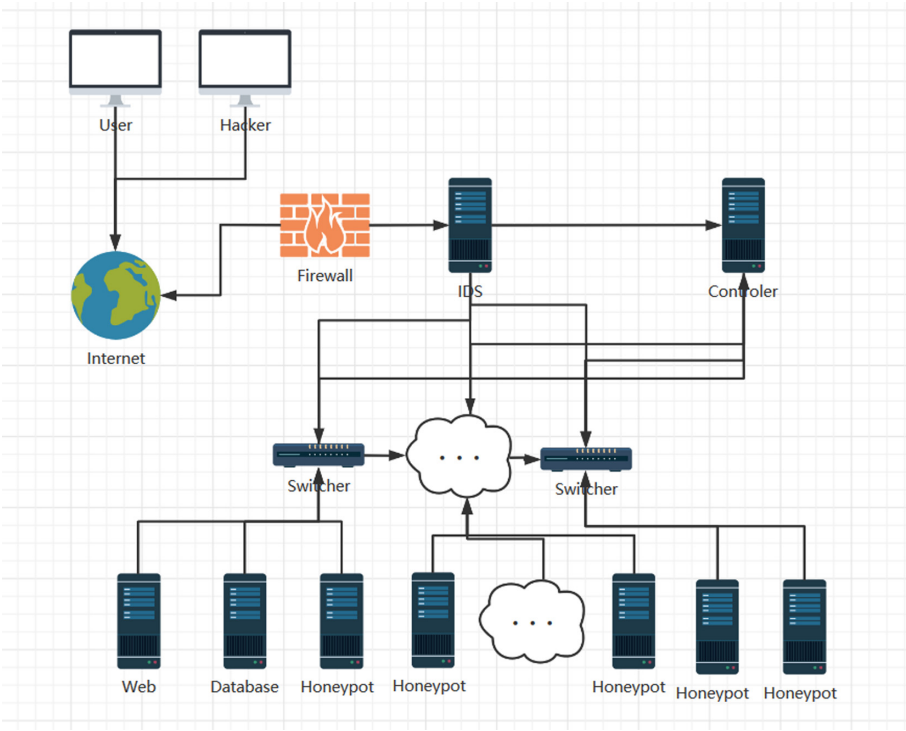

Fig. 1. System structure.

All switches in the honeynet are connected with the SDN controller, and exchange link status and flow table information with the controller through the Openflow protocol [34]. SDN controller can be programmed with its highly scalable, careful process flow for different attacks, regardless of the attacker what kind of attacks, the system will provide a highly realistic simulated network.

2.1 Theoretical Analysis of Mimic Honeynet

From previous studies on SDN mimic defense [35], it can be understood that the mimic defense honeynet can achieve the defense effect when q satisfies the following formula.

$$\begin{cases} p < 1 \\ \frac{\mu\alpha+\beta-\gamma}{\mu\alpha+\beta+\lambda} < q < \frac{1}{2} \end{cases} \tag{1}$$

Where the attack on behalf of the attacker's probability p, q represents the probability that the system uses honeypots, α indicates income, which $0 < \mu < 1$ indicates the degree of influence by the service itself, $\beta > 0$, indicates in addition to their other properties have been serving extent of damage degrees. Then the real honeypot services and services while providing service access side common with users normally access but do not attack the attacker can achieve this ideal combination of strategy Bayesian Nash equilibrium,

only this time the game equilibrium condition with honeypot presence probability q is related but not related to the attacker's attack probability p, so it can be concluded that the mimic SDN virtual honeynet defense can achieve the purpose of active defense.

Because the user's revenue EVn meets the following formula:

$$\begin{aligned} EVn &= P(Sr|S1) \times \alpha + P(Sh|S1) \times (-\alpha) \\ &= (1-q) \times \alpha + q \times (-\alpha) \\ &= (1-2q)\alpha \end{aligned} \tag{2}$$

So from the user's point of view, q should be as small as possible.

But the system revenue EVa meets the following formula:

$$\begin{aligned} EVa &= P(Sr|S1) \times (\mu\alpha + \beta - \gamma) + P(Sh|S1) \times (-\lambda - \gamma) \\ &= (1-q) \times (\mu\alpha + \beta - \gamma) + q \times (-\lambda - \gamma) \\ &= \mu\alpha + \beta - \gamma - q(\mu\alpha + \beta + \lambda) \end{aligned} \tag{3}$$

From the system point of view, q should be as small as possible while λ should be as large as possible.

The greatest impact on the probability of q should be the false alarm rate of the IDS server system. IDS has two cases for false alarms of data:

$$\begin{aligned} IDSe &= \{En, Ea\} \\ &= \{\textit{Normal users falsely report as attackers}, \\ &\quad \textit{attacker was falsely reported as a normal user}\} \end{aligned} \tag{4}$$

The corresponding probabilities are respectively $\{Pen, Pea\}$. The relationship between the false alarm rate and q should be $q = (1-w) * Pen + w(1-Pea)$.Where w represents the proportion of malicious visits by attackers in all visits.

At this time, the attacker's income EVa becomes:

$$\begin{aligned} EVa &= P(Sr|S1) \times (\mu\alpha + \beta - \gamma) + P(Sh|S1) \times (-\lambda - \gamma) \\ &= Pea \times (\mu\alpha + \beta - \gamma) + (1 - Pea) \times (-\lambda - \gamma) \\ &= Peax(\mu\alpha + \beta + \lambda) - \lambda - \gamma \end{aligned} \tag{5}$$

The income EVn of ordinary users becomes:

$$\begin{aligned} EVn &= P(Sr|S1) \times \alpha + P(Sh|S1) \times (-\alpha) \\ &= (1 - Pen) \times \alpha + Pen \times (-\alpha) \\ &= (1 - 2Pen) \times \alpha \end{aligned} \tag{6}$$

The income ESr of the real server becomes:

$$\begin{aligned} ESr &= P(Vn|V1) \times \alpha + P(Va|V1) \times (-\mu\alpha - \beta) \\ &= (1-w) \times (1 - Pen) \times \alpha + w \times Pea \times (-\mu\alpha - \beta) \end{aligned} \tag{7}$$

The income of the honeypot becomes ESh as:

$$\begin{aligned} ESh =& P(Vn|V1) \times (-\alpha) + P(Va|V1) \times (\lambda) \\ =& (1-w) \times Pen \times (-\alpha) + w \times (1-Pea) \times (\lambda) \end{aligned} \tag{8}$$

For the entire server, the actual revenue ES becomes:

$$\begin{aligned} ES(S1, S2) =& ESr(S1) + ESh(S1) \\ =& (1-w) \times (1-Pen) \times \alpha + w \times Pea \\ & \times (-\mu\alpha - \beta) + (1-w) \times Pen \times (-\alpha) \\ & + w \times (1-Pea) \times (\lambda) \end{aligned} \tag{9}$$

Compared with the IDS server's false alarm probability, the user's single-access revenue α, once the server is set up, its business process and service objects are determined, α there will be basically no major changes, and the degree of impact on the service itself μ and other performance outside of its own service The extent of damage β depends largely on the attacker. Under the premise of a certain honeypot revenue, the judgment strategy of the IDS server greatly affects the entire system. Among them, the judgment performance of the IDS server, when the machine performance and detection technology cannot be improved, whether it is the Pen or Pea tends to zero, it will affect the other. The relationship between the two should be $Pen * Pea = k$, where k is a fixed constant, which represents the performance of the IDS server, that is, Pen and Pea are positively correlated. We can find the optimal strategy of the system in the following experiments.

3 Simulation Results and Analysis

In order to better practice before the projected offensive and defensive earnings results, we build a defense based on mimicry of SDN to the Honeynet testing, need to use Mininet [36] create multiple switches and host used to form SDN network, one of the hosts as a real server, you can use Python -m SimpleHTTPServer 80 & to open the command Mininet in http service. Then use VM ware to create a few new servers to install SDN controllers, firewalls, and IDS servers.

3.1 Basic Data Simulation

The intrusion detection system is divided into two modes according to the behavior of intrusion detection:

$$T = \{Ty, Tw\} = \{\text{Abnormal detection}, \ \text{Misuse detection}\} \tag{20}$$

The order is based on the income α of the user′s single visit $\alpha = 1$. The proportion of attackers in all access locations w is 0.1%, that is, normal commercial servers face more ordinary users, and the degree of impact on the service itself $\mu = 0.1$ means that the attacker does not care about the service provided, and the degree of damage to performance $\beta = 100$ is The damage to the system is more serious. Honeypot revenue $\lambda = 10000$ is the ability to analyze attackers' attack methods, fix loopholes, digital forensics, etc. The revenue of honeypots needs to be far greater than the revenue of the attacker and the loss of real services.

3.2 Anomaly Detection Mode

In the anomaly detection mode, we must first establish a model of system access to normal behavior. Any visitor's behavior that does not conform to this model will be judged as an intrusion. Therefore, Pea can be very small and regarded as zero. The matching method is too strict except in Decreasing the abnormal rate of attackers being falsely reported as normal users, Pea, will inevitably increase the detection rate of normal users being falsely reported as attackers, Pen. Different Pen effects when pea is equal to 0 The real server revenue ESr is shown in Fig. 2. The honeypot server revenue ESh is shown in Fig. 3. The total income is shown in Fig. 4.

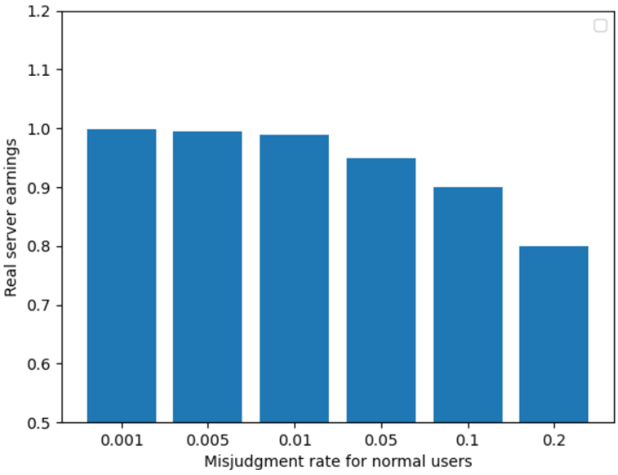

Fig. 2. The real server revenue

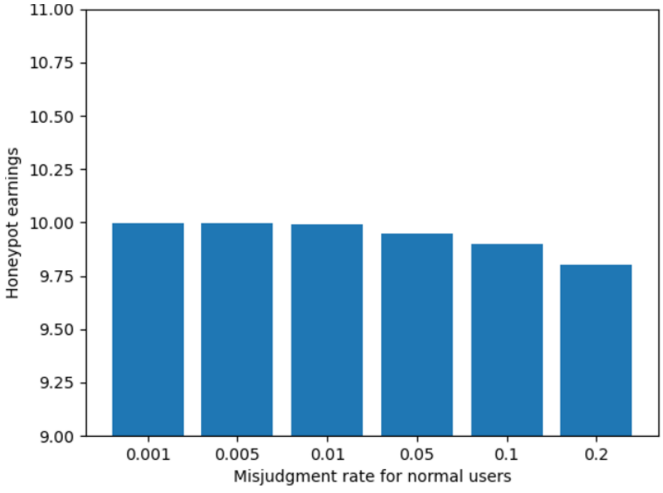

Fig. 3. The honeypot server revenue

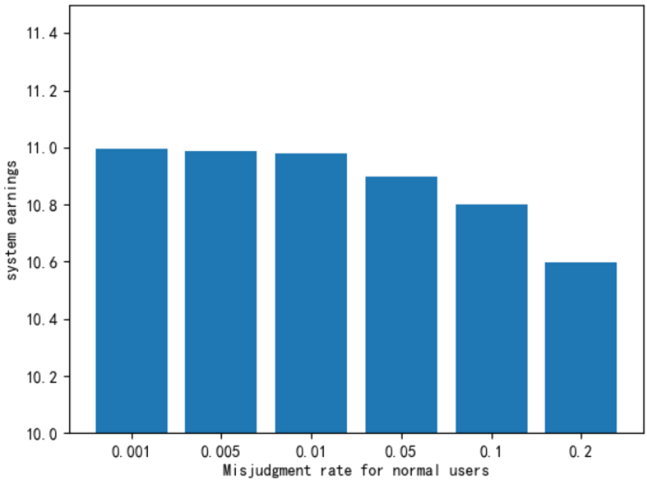

Fig. 4. The total income

3.3 Misuse Detection Mode

In the misuse detection mode, all possible unfavorable and unacceptable behaviors should first be summarized to establish a model. Any visitor's behavior that conforms to this model will be judged as an intrusion. Similarly, the decrease of Pen will also bring about the increase of Pea, so Pen = 0, at this time, the impact of Pea on the system. The real server revenue ESr is shown in Fig. 5. The income ESh of the honeypot server is shown in Fig. 6. The total income is shown in Fig. 7.

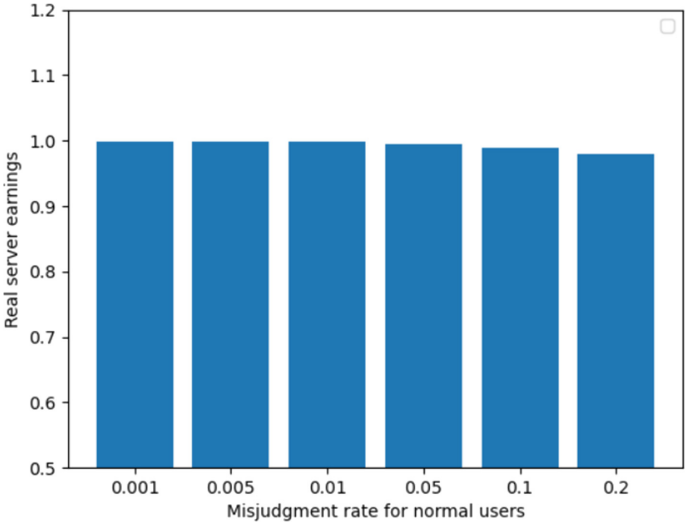

Fig. 5. The real server revenue

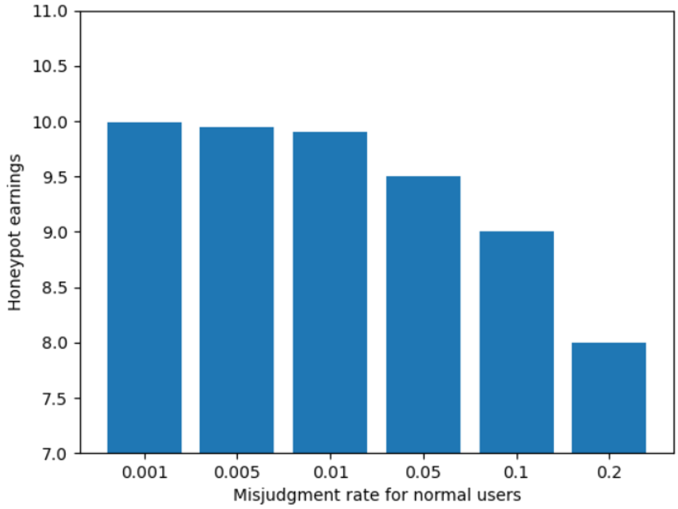

Fig. 6. The honeypot server revenue

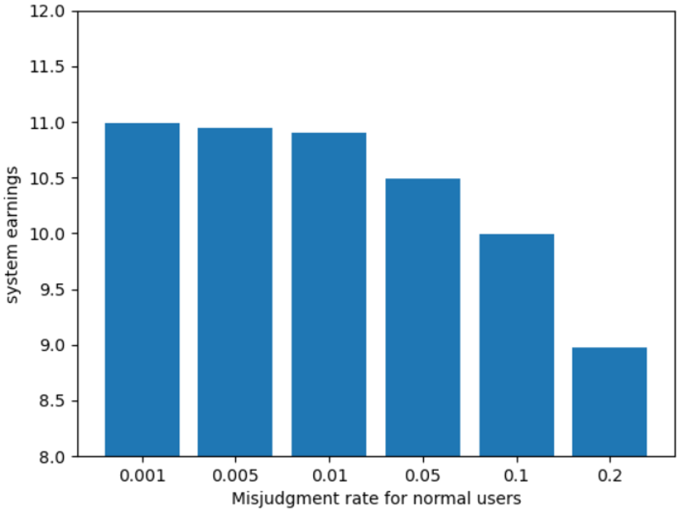

Fig. 7. The total income

3.4 System Best Profit

From the data results, the loss caused by the increase of Pea of the same magnitude will be higher than the loss caused by Pen. In the case that machine performance and detection technology cannot be improved, whether it is to turn Pen or Pea towards Zero will affect the other. In the case of $k = 0.001$, the mutual influence between the two is shown in Fig. 8.

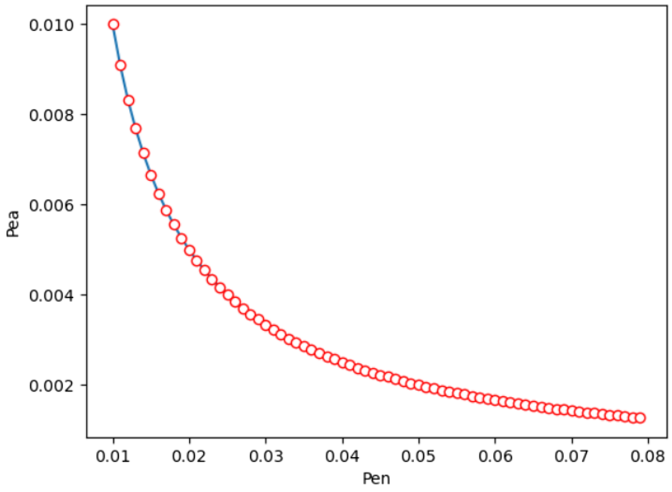

Fig. 8. The relationship between Pea and Pen

In this case, you can see the change in system revenue as shown in Fig. 9 below:

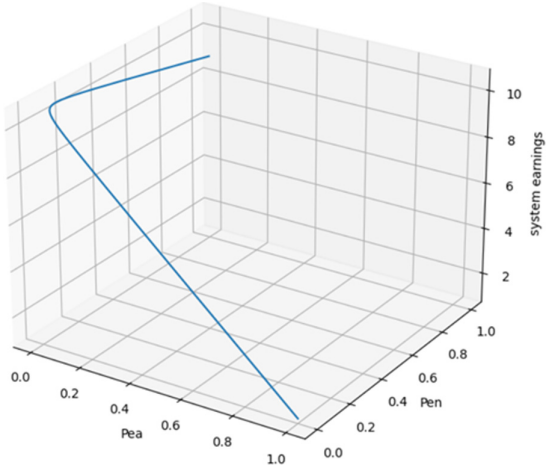

Fig. 9. Overall system benefits

We can be seen that the unilateral misjudgment rate reduction cannot be blindly pursued. Under the limit of the constant k, when $k = 0.001$, the overall profit of the system achieves the maximum boundary value $Pea = 0.014$ $Peh = 0.0714$ $E = 10.715$.

4 Conclusion

Through SDN-related technologies, the honeynet that realizes mimic defense has the characteristics of convenient deployment and convenient flow control compared with

traditional honeynets. It can easily control multiple network devices and add and delete multiple services. This article also uses related data reasoning Calculated, demonstrated the relevant influence of various service strategies of IDS server on the final defense effect, and demonstrated through simulation experiments, how to obtain the best defense effect, give full play to the role of real servers and honeypot servers, deceive attackers, and collect The attacker's information and attack methods are ultimately used to analyze the characteristics of the network, and in turn repair and strengthen the entire defense system based on relevant information, forming a virtuous circle, and ultimately achieving the effect of active defense.

References

1. Bahrami, M.: Cloud computing for emerging mobile cloud apps. In: 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, San Francisco, CA, pp. 4–5 (2015)
2. Jiang, D., Wang, Y., Lv, Z., Wang, W., Wang, H.: An energy-efficient networking approach in cloud services for IIoT networks. IEEE J. Sel. Areas Commun. **38**(5), 928–941 (2020)
3. Arsenijevic, U., Jovic, M.: Artificial intelligence marketing: chatbots. In: 2019 International Conference on Artificial Intelligence: Applications and Innovations (IC-AIAI), Belgrade, Serbia, p. 193 (2019). https://doi.org/10.1109/IC-AIAI48757.2019.00010
4. Huo, L., Jiang, D., Qi, S., Song, H., Miao, L.: An AI-based adaptive cognitive modeling and measurement method of network traffic for EIS. Mob. Netw. Appl. (2019). https://doi.org/10.1007/s11036-019-01419-z
5. Mian, M., Teredesai, A., Hazel, D., Pokuri, S., Uppala, K.: Work in progress - in-memory analysis for healthcare big data. In: 2014 IEEE International Congress on Big Data, Anchorage, AK, pp. 778–779 (2014). https://doi.org/10.1109/BigData.Congress.2014.119
6. Jiang, D., Wang, Y., Lv, Z., Qi, S., Singh, S.: Big data analysis based network behavior insight of cellular networks for industry 4.0 applications. IEEE Trans. Ind. Inform. **16**(2), 1310–1320 (2020)
7. Singh, S., Singh, N.: Internet of things (IoT): security challenges, business opportunities & reference architecture for E-commerce. In: 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, pp. 1577–1581 (2015). https://doi.org/10.1109/ICGCIoT.2015.7380718
8. Ceballos, G.R., Larios, V.M.: A model to promote citizen driven government in a smart city: use case at GDL smart city. In: 2016 IEEE International Smart Cities Conference (ISC2), Trento, pp. 1–6 (2016). https://doi.org/10.1109/ISC2.2016.7580873
9. Jiang, D., Zhang, P., Lv, Z., et al.: Energy-efficient multi-constraint routing algorithm with load balancing for smart city applications. IEEE Internet Things J. **3**(6), 1437–1447 (2016)
10. Lu, S., et al.: A study on service-oriented smart medical systems combined with key algorithms in the IoT environment. China Commun. **16**(9), 235–249 (2019). https://doi.org/10.23919/JCC.2019.09.018
11. Jiang, D., Li, W., Lv, H.: An energy-efficient cooperative multicast routing in multi-hop wireless networks for smart medical applications. Neurocomputing **2017**(220), 160–169 (2017)
12. Jiang, D., Huo, L., Lv, Z., Song, H., Qin, W.: A joint multi-criteria utility-based network selection approach for vehicle-to-infrastructure networking. IEEE Trans. Intell. Transp. Syst. **19**(10), 3305–3319 (2018)

13. Raghunandan, G.H., Chaithanya, G.H., Hajare, R.: Independent robust mesh for mobile adhoc networks. In: 2017 4th International Conference on Electronics and Communication Systems (ICECS), Coimbatore, pp. 125–128 (2017). https://doi.org/10.1109/ECS.2017.8067852
14. Jiang, D., Huo, L., Song, H.: Rethinking behaviors and activities of base stations in mobile cellular networks based on big data analysis. IEEE Trans. Netw. Sci. Eng. **7**(1), 80–90 (2020)
15. Zainudin, Z.S., Nuha Abdul Molok, N.: Advanced persistent threats awareness and readiness: a case study in Malaysian financial institutions. In: 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, pp. 1–3 (2018). https://doi.org/10.1109/CR.2018.8626835
16. SenthilKumar, P., Muthukumar, M.: A study on firewall system, scheduling and routing using pfsense scheme. In: 2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW), Erode, India, pp. 14–17 (2018). https://doi.org/10.1109/I2C2SW45816.2018.8997167
17. Penya, Y.K., Bringas, P.G.: Experiences on designing an integral intrusion detection system. In: 2008 19th International Workshop on Database and Expert Systems Applications, Turin, pp. 675–679 (2008). https://doi.org/10.1109/DEXA.2008.54
18. Borkar, A., Donode, A., Kumari, A.: A survey on Intrusion detection system (IDS) and internal intrusion detection and protection system (IIDPS). In: 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, pp. 949–953 (2017). https://doi.org/10.1109/ICICI.2017.8365277
19. Watson, D., Riden, J.: The honeynet project: data collection tools, infrastructure, archives and analysis. In: 2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing, Amsterdam, pp. 24–30 (2008). https://doi.org/10.1109/WISTDCS.2008.11
20. Zhang, H., Wang, J., Yu, D., Han, J., Li, T.: Active defense strategy selection based on static Bayesian game. In: Third International Conference on Cyberspace Technology (CCT 2015), Beijing, pp. 1–7 (2015). https://doi.org/10.1049/cp.2015.0806
21. Akremi, A., Sallay, H., Rouached, M., Sriti, M., Abid, M., Bouaziz, R.: Towards a built-in digital forensics-aware framework for web services. In: 2015 11th International Conference on Computational Intelligence and Security (CIS), Shenzhen, pp. 367–370 (2015). https://doi.org/10.1109/CIS.2015.95
22. Kim, D., Gil, J.-M., Wang, G., Kim, S.-H.: Integrated SDN and non-SDN network management approaches for future internet environment. In: Park, J.J.H., Ng, J.-Y., Jeong, H.Y., Waluyo, B. (eds.) Multimedia and Ubiquitous Engineering. LNEE, vol. 240, pp. 529–536. Springer, Dordrecht (2013). https://doi.org/10.1007/978-94-007-6738-6_64
23. Jiang, D., Huo, L., Li, Y.: Fine-granularity inference and estimations to network traffic for SDN. PLoS ONE **13**(5), 1–23 (2018)
24. Akyildiz, H.A., Hökelek, İ., Saygun, E., Çırpan, H.A.: Flow re-routing based traffic engineering for SDN networks. In: 2017 25th Signal Processing and Communications Applications Conference (SIU), Antalya, pp. 1–4 (2017). https://doi.org/10.1109/SIU.2017.7960321
25. Huo, L., Jiang, D., Lv, Z., Singh, S.: An intelligent optimization-based traffic information acquirement approach to software-defined networking. Comput. Intell. **36**(1), 151–171 (2019)
26. Wang, Y., Jiang, D., Huo, L., Zhao, Y.: A new traffic prediction algorithm to software defined networking. Mob. Netw. Appl. (2019). https://doi.org/10.1007/s11036-019-01423-3
27. Perepelkin, D., Tsyganov, I.: SDN cluster constructor: software toolkit for structures segmentation of software defined networks. In: 2019 XVI International Symposium Problems of Redundancy in Information and Control Systems (REDUNDANCY), Moscow, Russia, pp. 195–198 (2019). https://doi.org/10.1109/REDUNDANCY48165.2019.9003334
28. Wang, F., Jiang, D., Qi, S.: An adaptive routing algorithm for integrated information networks. China Commun. **7**(1), 196–207 (2019)
29. Jiangxing, W.: The original intent and prospect of mimic computing and mimic security defense. Telecommun. Sci. **30**(07), 2–7 (2014). (in Chinese)

30. Ma, B., Zhang, Z.: Security research of redundancy in mimic defense system. In: 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, pp. 2910–2914 (2017). https://doi.org/10.1109/CompComm.2017.8323064
31. Sun, Y., Liu, Z., Jiang, Z., Meng, X., Hu, W.: Conceptual model of situational awareness for advanced persistent threats. Inf. Secur. Res. **6**(06), 482–490 (2020). (in Chinese)
32. Jiang, D., Wang, W., Shi, L., Song, H.: A compressive sensing-based approach to end-to-end network traffic reconstruction. IEEE Trans. Netw. Sci. Eng. **7**(1), 507–519 (2020)
33. Qi, S., Jiang, D., Huo, L.: A prediction approach to end-to-end traffic in space information networks. Mob. Netw. Appl. (2019). https://doi.org/10.1007/s11036-019-01424-2
34. McKeown, N., Anderson, T., Balakrishnan, H., et al.: Openflow: enabling innovation in campus networks. ACM SIGCOMM Comput. Commun. Rev. **38**(2), 69–74 (2008)
35. Lian, Z., Yin, X., Xi, Q., Tan, R.: A SDN virtual honeynet based on mimic defense mechanism. Comput. Eng. Appl. **55**(01), 109–114 (2019)
36. Qureshi, S., Braun, R.: Mininet topology: mirror of the optical switch fabric. In: 2019 29th International Telecommunication Networks and Applications Conference (ITNAC), Auckland, New Zealand, pp. 1–6 (2019). https://doi.org/10.1109/ITNAC46935.2019.9078014