ISSN 2663-4546

Journal of Computer and Higher Education

6
2020

主办方：中国文化教育出版社

协办方：苏州教英信息科技有限公司

编辑出版：《Journal of Computer and Higher Education》Editor Office

主编：Yangyang Jiao

通讯地址： 香港九龙旺角弥敦道 555 号九龙行 16 楼 1605 室

邮箱：site@jiaoying.org

ISSN 2663-4546

JOURNAL OF COMPUTER AND HIGHER EDUCATION

June 2020

Contents

DoS Attack Study on Operating Systems within a Same LAN

Chang Liu, Beichen Liu, Jingxuan Kang, Wei Li, Jiahong Zhai, Kaiyan Jin, Kaipeng Zhao, Tianjie Xie, Zhenyi Wang, Xiaopeng Li

***Abstract*—This study was designed to focus on the performance of different operating systems after Denial of Service attack. Preparation shows the operating systems which consists of Windows, Linux running on VMware Virtual Machine, iOS and Android. The detail of attacking was introduced in attack process. The result and data of the test were listed in a table form and evaluated in the result and data analysis part. The conclusion was provided in the final part.**

***Index Terms*— DoS Attack, Kali Linux, hping3, operating systems, Windows, Linux, iOS, Android**

I. Introduction

THIS study is to discuss if different operating systems will have different performance when they are attacked, identify a system that is least affected by DoS attack, and will be easy to prevent and relieve from DoS attack. Windows, Linux, iOS and Android, which are four of the most popular operating systems, are chosen to be the tested targets.

II. Experiment and Analysis

A. Experiment

The machines respectively carried CentOS, Windows, iOS and Android were chosen to be targets and were respectively pinged 100, 200 and 300 times with a constant size 100 of each packet.

The central computer sent packets of 100, 200 and 300 sizes to each target for constant 100 times separately.

B. Result

The result is shown in the Tables below.

Table 1. The results of all devices.

	Android	iOS	Windows	CentOS
100 times ping	94% / 565.3ms	61.7% / 2928ms	40.3% / 3125ms	24.7% / 2654ms
200 times ping	93.7% / 597.3ms	59.7% / 3149ms	40.7% / 3180ms	25.7% / 2651.3 ms
300 times ping	93.7% / 660.3ms	63% / 3495ms	42.7% / 3051ms	25.7% / 2399ms
Average	93.8% / 607.6ms	61.5% / 3190ms	41.2% / 3119ms	25.4% / 2568ms

Table 2. The results of all devices.

	Android	iOS	Windows	CentOS
100 size	94% / 565.3ms	61.7% / 2928ms	40.3% / 3125ms	24.7% / 2654ms
200 size	92.3% / 639ms	88% / 3020ms	73.7% / 3177ms	74% / 3178ms
300 size	92.3% / 1557ms	90.7% / 2312ms	93.7% / 2643ms	89.7% / 2638ms
Average	92.9% / 920.4ms	80.1% / 2753.3ms	69.2% / 2981.7ms	62.8% / 2823.3ms

III. Conclusion and Future Work

In conclusion, this study found that when DoS attack occurred, Linux was the most stable system in the four type of systems. Furthermore, the study also found that the impact of DoS attack would not weaken over time if it had not stop, and would increase if the size of packets increased.

References

[1] S. Ranger. (2018, Mar. 1). GitHub hit with the largest DDoS attack ever seen [Online]. Available: https://www.zdnet.com/article/github-was-hit-with-the-largest-ddos-attack-ever-seen/

[2] N. Naik, P. Jenkins, R. Cooke, D. Ball, A. Foster and Y. Jin, "Augmented windows fuzzy firewall for preventing denial of service attack," in 2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), Naples, Italy, Jul. 9-12, 2017, pp. 1-6.

[3] NCCIC. (2018, Jun. 28). Understanding Denial-of-Service Attacks [Online]. Available: https://www.us-cert.gov/ncas/tips/ST04-015

[4] Y. Cui, Q. Liu, K. Zheng and X. Huang, "Evaluation of Several Denial of Service Attack Methods for IoT System, " in 2018 9th International Conference on Information Technology in Medicine and Education (ITME), Hangzhou, China, Oct. 19-21, 2018, pp. 794-798.

[5] Z. Liu, L. Li, Y. Ju, Y. Liu, Y. Sun, K. Zheng and X. Huang, "The Efficiency Comparison Between DDoS and DoS Attack, " in 2018 9th International Conference on Information Technology in Medicine and Education (ITME), Hangzhou, China, Oct. 19-21, 2018, pp. 1050-1054.

[6] Q. Chen, H. Chen, Y. Cai, Y. Zhang and X. Huang, "Denial of Service Attack on IoT System, " in 2018 9th International Conference on Information Technology in Medicine and

Chang Liu, Beichen Liu, Jingxuan Kang, Wei Li, Jiahong Zhai, Kaiyan Jin, Kaipeng Zhao, Tianjie Xie, Zhenyi Wang, and Xiaopeng Li are with the Department of Computer Science and Software Engineering, Xi'an Jiaotong-Liverpool University, Suzhou, China.

Education (ITME), Hangzhou, China, Oct. 19-21, 2018, pp. 755-758.
[7] (2019). DDoS Attack Definitions – DdoSPedia [Online]. Available: https://security.radware.com/ddos-knowledge-center/ddospedia/hping/

Analysis of the Application Status of Blockchain in Power Grid

Yuding Zhang

***Abstract*—In recent years, it has become a hot issue to explore the application of blockchain technology in the area of energy Internet, and consequently, a large number of related projects have started their preliminary operations. This paper will summarize some of the existing applications and new technologies in the market or the laboratory.**

***Index Terms*—Blockchain, power grid, self-executing**

I. Introduction

BLOCKCHAIN is a decentralized, open and transparent database to store transaction information. Nowadays, electricity energy is no longer monopolized by a single company, and the energy has become more distributed, which well fits in with the distributed nature of blockchain. Therefore, this technology can be integrated well in the area of energy Internet. In this paper, some applications of blockchain technologies in the power grid will be summarized.

II. Development Status

American Energy Company "LO3 Energy" and "Consensus Systems" co-developed the "TransActiveGrid" project, which has become the first case of applying blockchain technology to power systems in the world. Using point-to-point transactions, this system makes use of ETH coins and smart meters to generate, connect and share data [1].

Besides, a project team named "scanergy" from Europe built a solar microgrid prototype system in the laboratory. By means of this system, residents can sell excess electricity generated by their own solar panels to the local smart grid companies and buy energy with NRG coins [1].

Electron, a UK company, has built a distributed power metering system, where consumers can switch from one supplier to another within just 15 seconds [2].

Furthermore, some academic researchers have proposed some new technologies, findings and solutions.

Donglan Liu team proposed a cross-domain authentication scheme. The program employs a hash algorithm to validate certificates, reduce the number of public key algorithm signatures and validations, thus making the solution more efficient and scalable [3].

Jian Ping team proposed a decentralized distribution network model, built a distributed multi-party power trading platform by means of Ethereum smart contract technology and successfully realized simulation [4].

Yuding Zhang is with Electrical Engineering, Xi'an Jiaotong Liverpool University, Suzhou, China (e-mail: Yuding.Zhang17@student.xjtlu.edu.cn).

Based on the analysis above, the application status of blockchain technology in the grid can be summarized in Table.1 as shown below.

Table.1 Application status of blockchain in power grid

Catalogue	Content
Companies and organizations	LO3 Energy, Consensus Systems, Scanergy, Electron
New technology	Point-to-point electricity trading, Cross-domain authentication scheme, VCG, Decentralized multilateral trade on Ethereum
Typical applications	TransActiveGrid, Solar microgrid prototype system, Smart power metering system, Decentralized distribution network model

III. Conclusion

In this paper, some typical applications of blockchain in power grid have been listed. The development of blockchain has brought many opportunities to the reform of the power grid. It has broken the energy monopoly and all these practices help make the electricity trading more concise, secure, open, transparent, fair and trustworthy.

References

[1] D.Yang et al., "区块链在能源互联网中应用现状分析和前进展望," 中国电机工程学报, Vol.37, no.13, pp. 3664-3671, Jul. 2017.

[2] H. Duan, "区块链技术正在积极促进能源产业变革," 科技中国, Vol. 7, pp. 91-93, Jul, 2018.

[3] D.Liu et al., "Research on a Cross-Domain Authentication Scheme Based on Consortium Blockchain in V2G Networks of Smart Grid," in 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, Oct. 20-22, 2018.

[4] J. Ping et al., "Decentralized Transactive Mechanism in Distribution Network Based on Smart Contract," 中国电机工程学报, Vol.37, no.13, pp. 3682-3690, Jul. 2017.

The Performance Comparison of PBFT Consensus Mechanism and Kafka Consensus Mechanism

Kai Zheng, and Xin Huang

***Abstract*—In recent years, blockchain has been used in a lot of areas. A critical problem is the performance of the blockchain network; and one of the most important influential factors is the consensus mechanism, for example, Proof of Work (POW), Practical Byzantine Fault Tolerance (PBFT) and Kafka. In this paper, the continuous-time Markov chain(CTMC) models are built to study the performance of PBFT and Kafka, and the comparative analysis of them will also be given.**

***Index Terms*— Blockchain network, CTMC, Kafka, PBFT**

IV. Introduction

In recent years, blockchain has been used in many areas. In [1], blockchain has been used in financial transactions, agri-food supply chain traceability, and energy trading respectively.

However, the performance of blockchain is a bottleneck for its development. Finding out how to improve efficiency is very important. Blockchain has many mechanisms such as POW, PBFT, and Kafka [2] [3]. So far, most performance analyses are based on real blockchain networks [4]. If the performance of the consensus mechanisms can be simulated, the cost of building real networks will be saved. However, the research about performance simulation analysis is still lacking.

In this paper, CTMC models are used for simulating the process of PBFT and Kafka. The efficiency analysis of them will also be given. The contribution of the paper includes:

- The efficiency comparison of PBFT and Kafka is given.
- The models can be used for analyzing influencing factors of PBFT and Kafka in further research.

The paper is organized as follows: section II gives the simulation results of PBFT and Kafka. Section III gives the conclusion and further research.

I. The simulation results of PBFT and Kafka.

CTMC is a stochastic model that can be used to describe a sequence of possible events. The CTMC models refer to [5].

In this paper, 2 CTMC models are built to simulate the performance of PBFT and Kafka respectively. The broadcast rate of all the nodes is 1000 messages/s. The probability for PBFT and Kafka reaches a consensus is shown in Fig.1.

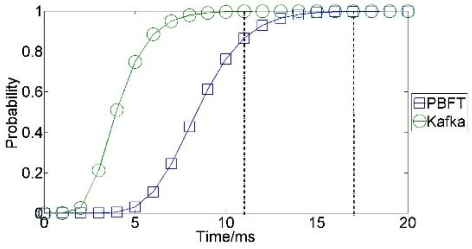

Fig.1. the performance of PBFT and Kafka

Finding1: At 11ms, the probability of Kafka reaches a consensus is almost 1. At 17ms, the probability of Kafka reaches a consensus is almost 1.

Finding2: the time for PBFT reaches a consensus is 1.55 times longer than that of Kafka.

II. conclusion

In this paper, we use CTMC models to simulate the process of PBFT and Kafka. The simulation result shows that Kafka is about 1.55 times faster than PBFT.

There are some other influencing factors that influence the efficiency of consensus mechanisms. These will be included in further research.

Acknowledged

This work was supported by the XJTLU research development fund projects under Grant RDF140243 and Grant RDF150246, in part by the National Natural Science Foundation of China under Grant No. 61701418, and in part by Innovation Projects of The Next Generation Internet Technology under Grant NGII20170301.

.

References

[1] Zhu H, Zhou Z Z. Analysis and outlook of applications of blockchain technology to equity crowdfunding in China[J]. Financial Innovation, 2016, 2(1):29.

[2] Buccafurri F , Lax G , Nicolazzo S , et al. Overcoming Limits of Blockchain for IoT Applications[C]// the 12th International Conference. ACM, 2017.

[3] Jian L,Wenting L, Karame G,et al. Scalable Byzantine Consensus via Hardware-assisted Secret Sharing[J]. IEEE Transactions on Computers, 2018:1-1.

[4] Sukhwani H , Martinez J M , Chang X , et al. Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric)[C]// 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS). IEEE Computer Society, 2017.

Kai Zheng is with the Department of Computer Science and Software Engineering, Xi'an Jiaotong Liverpool University, Suzhou, China (e-mail: Kai.Zheng@xjtlu.edu.cn).

Xin Huang is with the Department of Computer Science and Software Engineering, Xi'an Jiaotong Liverpool University, Suzhou, China (e-mail: Xin.Huang@xjtlu.edu.cn).

[5] Liang L , Zheng K , Wei Z , et al. Model Checking of IoT System in Microgrid[C]// 2016 8th International Conference on Information Technology in Medicine and Education (ITME). IEEE, 2016.

Evaluation of Denial of Service Attack for IoT System

Yumeng Cui, and Qianli Liu

I. Introduction

LAST decades witnessed the rapid growth of information technology, novel theories are proposed to increase the capability of human, such as the Block Chain, Facial recognition and the Internet of Things.

The aim of IoT is to integrate the physical and digital worlds in one single ecosystem [1]. However, it has become a widely concern that these innovative theory may cause safety issues.

DoS attack is regarded one of the most popular attacking methods. The definition of DoS attack focuses on out-of-order, which attempt to make a device unavailable to its intended users. The paper intended to discuss the possible effect impact on attacking efficiency when the packets' amount and the number of attacker changed.

II. Experiment Design

The DoS attacking is described as the flood attack because the mean to broke the targeted machine by transmitting superfluous requests in order to overload the system [2]. In addition, the legitimate requests from the users are prevented.

The equipment includes a PC, a router, a sensor node and an attacker based on Kali Linux. In order to attack the sensor node, PC should send a large amount of packets to the sensor node. [3].In the experiment, hping3 will be applied as the attacking methods. Loss rate and success time were chosen as indicators. Higher loss rate and less success time imply a better attacking performance.

III. The Process Of Attack Experiment

Launch the hping3 command in the terminal of Kali Linux "hping3 –c 1000 –d 10 –S –w 64 –p 80 —flood —rand-source targetIP". "targetIP" stands for the victim IP address. "hping3" is the name of the application binary. "-c" means the number of packets to send and "-c 1000" means there are sending 1000 packets. "-d 10" stands for the size of each packet is 10 bytes that was sent to target machine.

TABLE I: Experiment Result For DoS Attack Using Hping3 With Different Amount Of Packets

Packets Amount (15bytes)	CPU utility	Memory utility	Success time	Packet loss rate
1000	51%	47%	58.23s	25%
2000	59%	48%	47.91s	36%

Finding. The further experiment implies that the amount that packets being sent also have an impact on the response time. Within certain range, the larger the amount of packets is sent, the less successful time it has.

TABLE II: Experiment Result For DoS Attack Using Hping3 With Different Size Of Packets

Size of packets (bytes)	CPU utility (%)	Memory utility (%)	Time for success of attack (s)	Packet loss rate (%)
5	32	43	119.12	16
10	41	44	72.61	22
15	51	47	58.23	25

Finding. Table II demonstrates the memory utility changes. As the size of packets increased, the time for success of attack will reduce and the packet loss rate increased as well. In conclusion, within certain range, the bigger packet size it sends, the more remarkable efficiency DoS attack will have.

IV. Conclusion

The Paper demonstrates the process how hping3 attack commenced by Kali Linux achieved its purpose to paralyze an IoT system. The result indicates that within certain range, the greater amount of packets will expedite the attacking process and thus improve the efficiency.

References

[1] Y. Al-Halabi et al., Study on access control approaches in the context of Internet of Things: A survey. 2017 International Conference on Engineering and Technology (ICET), pp. 1-7, 2017

[2] N. Tripathi et al., How Secure are Web Servers? An Empirical Study of Slow HTTP DoS Attacks and Detection. 2016 11th International Conference on Availability, Reliability and Security (ARES), pp. 454-463, 2016.

Yumeng Cui is with the Department of Computer Science and Software Engineering, Xi'an Jiaotong Liverpool University, Suzhou, China (e-mail: Yumeng.Cui16@xjtlu.edu.cn).

Qianli Liu is with the Department of Computer Science and Software Engineering, Xi'an Jiaotong Liverpool University, Suzhou, China (e-mail: Qianli.Liu16@xjtlu.edu.cn).

[3] K. Zheng et al., A Denial of Service Attack Method for an IoT System. 2016 8th International Conference on Information Technology in Medicine and Education (ITME), pp. 360-364, 2016.