A Signaling Analysis Algorithm in 5G Terminal Simulator

Yu Duan[1(✉)], Wanwan Wang[2], and Zhizhong Zhang[1]

[1] School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
s170102001@stu.cqupt.edu.cn
[2] School of Data Science,
Chongqing Vocational College of Transportation, Chongqing 402247, China

Abstract. Focused on the issue that the low efficiency for 5G network signaling analysis and processing, a hash topology under a new architecture based on the traditional LTE-A signaling monitoring and analysis system was proposed, its main subsystems and specific functional modules were introduced in detail, provided support for 5G terminal emulator signaling analysis. Firstly, the Key of the signaling message was sorted according to the value by using a large top heap; Secondly, the Key was mapped to a hash table, and the position of the Key value in the linked list was determined according to the probability, and the probability was obtained. The larger Key value was placed in the hash table with less conflicts. Finally, the hash table record was accessed, and the same signaling process information of the same user was associated and synthesized. The experimental results show that the improved algorithm under the proposed new architecture reduces the time spent on signaling analysis by 55.66% compared with the traditional algorithm, so it is suitable for practical engineering applications.

Keywords: 5G network · Terminal simulator · Signaling analysis · Hash conflict · Heap sort

1 Introduction

With the rapid development of mobile communication networks, the global 5G enters the critical period of commercial deployment. On June 6, 2019, China's Ministry of Industry and Information Technology officially issued 5G commercial licenses to China Telecom, China Mobile, China Unicom and China Radio and Television, and accelerated the deployment of 5G trial commercials, which means that the era of 5G is coming.

According to the "5G Vision and Demand White Paper" released by the IMT-2020 (5G) Promotion Group in May 2014, the theoretical transmission speed of 5G networks can reach 10 Gb per second, which will be hundreds of times higher than 4G network transmission speed [1]. The existing Long Term Evolution-Advanced (LTE-A) air interface monitoring analyzer is difficult to handle such massive mobile data, and it is difficult to adapt to the 5G network structure [2], there is an urgent need for a more

H. Gao et al. (Eds.): ChinaCom 2019, LNICST 312, pp. 729–740, 2020.
https://doi.org/10.1007/978-3-030-41114-5_55

high-performance test [3]. The United States and the European Union are actively developing analog terminals for 5G testing [4]. Anritsu Corporation of Japan and South Korea Samsung Corporation development 5G terminal analog devices that support 5G NR full protocol stack connectivity testing. At present, most of the communication instrumentation produced in China is still a low-to-medium product [5]. Therefore, the development of new 5G terminal analog instruments with independent intellectual property rights can enhance the research and development capabilities of domestic high-end communication equipment, and promote the rapid development of China's 5G industry chain.

In the 5G terminal simulator, the signaling analysis technology is the core technology of the analog terminal signaling analysis system. Through the analysis of the signaling process, the specific location of the problem is obtained, and the data characteristics are used to solve the problem in the communication. In recent years, more and more researchers research for it. In [6, 7], a Multi-Protocol Correlation Analysis (MPCA) system based on the Uu interface of the LTE-Advanced network is proposed. The user data signaling process is associated with the user service data flow, and the same is not considered. The user's same signaling process is associated with the message; in [8, 9], it is proposed that the composite service call/transaction detail record (XDR) is multi-protocol association after the decoding synthesis process, but it is only applicable to the traditional Analysis of the LTE-A air interface monitor.

Therefore, this paper will combine the traditional LTE-A air interface monitor analysis signaling analysis technology in the process of 5G terminal simulator signaling analysis, and an improved signaling analysis algorithm based on the combination of chain address method and hash top stack processing hash to deal with hash conflicts is proposed and the new signaling analysis system architecture based on the algorithm is designed. The research focuses on decoding synthesis and multi-protocol association in the signaling analysis process to achieve accurate signaling monitoring in the signaling analysis system.

2 The Overall Structure of the System

The traditional LTE-A network is a centralized UMTS evolved umts terrestrial radio access (E-UTRAN) flattened and evolved packet core (EPC) centralized network. Point-to-point (P2P) communication [10]. The user equipment (UE) carries more control functions. The control plane equipment has a single function and the function modules are tightly coupled. This will result in low network-side data collection efficiency during signaling monitoring and analysis, and XDR cannot be decoded and synthesized. Efficient storage.

Combined with the signaling analysis technology in the LTE-A air interface monitoring analyzer, the 5G network is introduced based on the service-based architecture (SBA), and next generation core (NGC) is separated by the control plane and the transfer plane. The user plane is simplified to achieve efficient forwarding. The new radio (NR) is separated by a centralized unit/distribution unit (CU/DU) to achieve centralized coordination and control of radio resources, and the network function to close and couple. According to the requirements of 3GPP and related industry test specifications, the signaling analysis system in the 5G terminal simulator is divided into three subsystems:

L1L2 subsystem, L3 decoding synthesis subsystem, and reverse inspection subsystem. Figure 1 is a signaling analysis system framework in a 5G terminal emulator.

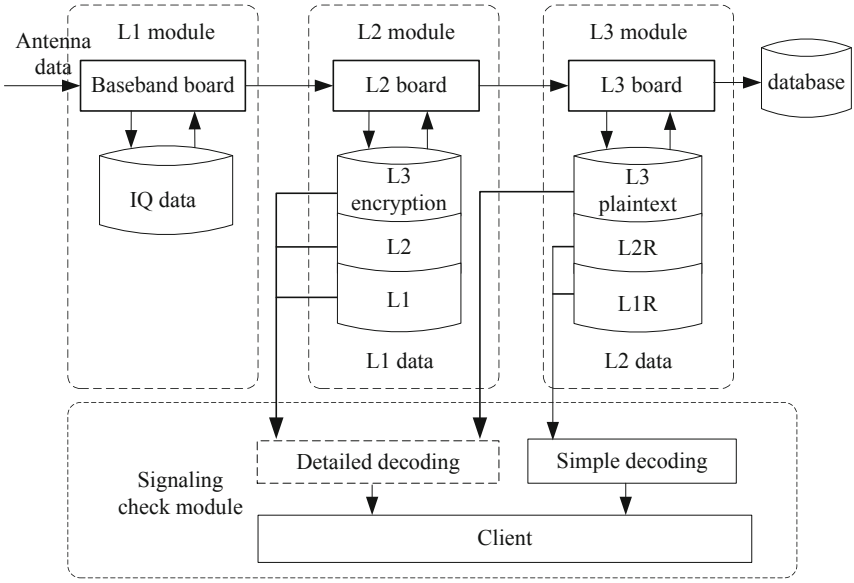

Fig. 1. Signaling analysis system framework in 5G terminal simulator.

The function of the L1L2 subsystem is mainly to complete the data acquisition and decoding, decryption and reorganization, and the L3 decoding and synthesis subsystem function is to complete the signaling plane and business plane decoding and synthesize the table, and the reverse check subsystem function is to complete the acquisition of the current page from the client. Message decoding result.

3 System Module Design

The 5G terminal simulator signaling analysis system draws on the design concept of micro service style (MSS) in the field of internet technology (IT), and introduces "service call" in signaling communication. According to the modular design idea, The network function is defined as a plurality of service modules that can be relatively independent and can be flexibly invoked. The signaling analysis mainly involves the baseband board collecting real-time data from the antenna and transmitting the L1 data to the layer two board; the layer two board stores the L1 data, and after completing the analysis of the MAC protocol, the RLC protocol, and the PDCP protocol, the output L2 is output. The data is transferred to the third board; the layer three board stores the L2 data to complete the protocol parsing; the decoding result is multi-protocol association, and the XDR is synthesized and stored in the database. The signaling analysis system can be divided into four modules: signaling acquisition module, decoding synthesis module, multi-protocol association module and synthetic output table and data back-checking module.

3.1 Signaling Acquisition Module

The function of the module is mainly to obtain the signaling data of the wireless port user by using the acquisition card, and realize the collection of the original signaling data. Using signaling messages collected from the signaling chain, and the collected signaling message is analyzed by the protocol, and divided it into signaling plane data and service plane data according to the message type, respectively corresponding to the control plane and the user plane of the air interface. The signaling plane data mainly includes the RRC and NAS protocols carried on the PDCP, and the system information block (SIB) and the master information block (MIB) such as the UE and the gNB for maintaining control message transmission. the service plane data includes user data such as PDCP and its IP protocol, as shown in Table 1.

Table 1. Signaling plane and business plane data.

Signaling plane data	Business plane data
RRC protocol	PDCP protocol
NAS protocol	IP protocol
SIB	HTTP, FTP protocol
MIB	TCP, UDP protocol

3.2 Decoding Synthesis Module

The signaling collection module obtains the L2 data from the Layer two board, and identifies the data as the signaling plane and the service plane according to the message type, respectively corresponding to the control plane and the user plane of the air interface, and respectively sent to the signaling plane lock-free queue and the tail of the service-side lock-free queue, the corresponding decoding synthesis module acquires data from the head of the queue and performs decoding synthesis. According to different types of protocols, different decoders are called, and the corresponding decoding function is called for decoding.

The decoding of the signaling plane mainly includes decoding of the NAS and RRC protocols, using the abstract syntax notation one (ASN.1) standard definition format, storing the protocol in a specific format in the description text, and then using the corresponding compiler to generate C++ code from the file and loop it to the top level data. The business plane decoding is mainly the decoding of user data including protocols such as IP, TCP, HTTP, UDP, DNS, and FTP. The specific decoding process is shown in Fig. 2(a). Protocol synthesis is to obtain information about each layer protocol according to the protocol type, according to different synthetic information to obtain user and signaling information, and combine them to form a complete signaling process.

The synthesis module needs to be initialized to obtain decoded data, and the decoded result is L3 data, which includes a field corresponding to the message of the MsgId and

the CDR ID, traffic statistics information of the protocol, and storage protocol stack data. In addition, The respective protocol synthesizer needs to be defined for each layer of protocol. The key information of the message is used to search for a corresponding signaling flow message in the hash table and determine whether it exists. Update statistics if they exist, and create new XDR if they do not exist. At the same time, the timeout check is performed. If there is no time out, add that value of the corresponding key. When the end message is received, the synthetic table module is called to send the synthesized XDR and the statistics table to the multi-protocol association module for association. The specific synthesis process is shown in Fig. 2(b).

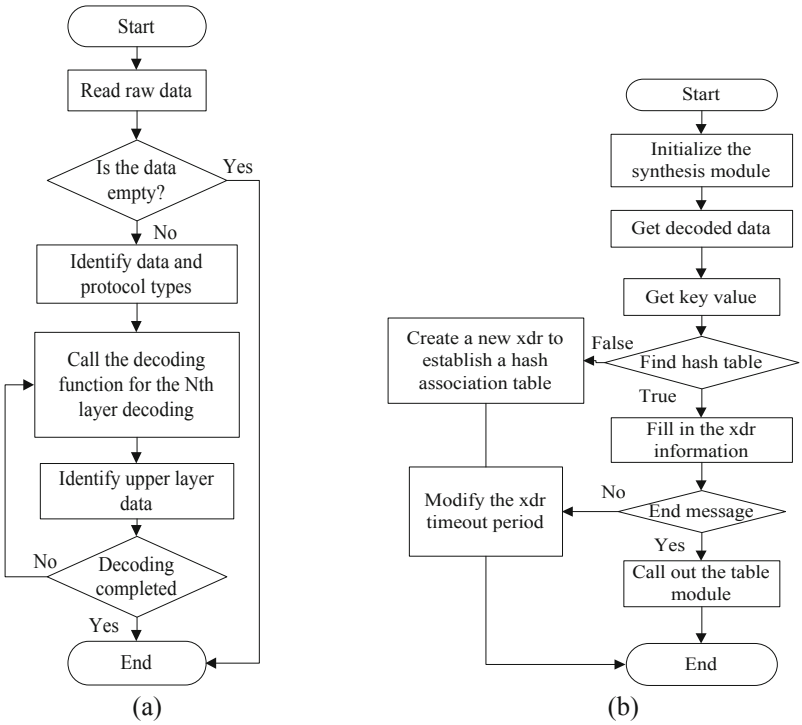

Fig. 2. Decoding synthesis process. (a) Decoding process. (b) Synthesis process

3.3 Multi-protocol Association Module

Multi-protocol association refers to the automatic association of network user information for real-time association backfilling. The complete signaling process is then synthesized by querying the temporary key correlation information Key value, and then synthesizing the complete signaling flow by means of the real Key value obtained by the detection system, and filled into XDR [4].

The system uses cell radio network temporary identifier (C-RNTI) as a user identifier, and combines messages associated with the same signaling process of the same

user to form a complete signaling process. Synthesize the protocol transaction detail record according to the protocol type, and extract the protocol type, associated primary key and value, UE identification (userID), international mobile subscriber identification number (IMSIN), user IP address (UserIP), start time (Runtime), end time (Endtime) and other information used for correlation analysis. Finally, the signaling plane and the business plane data of the same user are matched and associated, and the multi-protocol association label is added to further synthesize the integrated XDR. The multi-protocol association process is shown in Fig. 3.

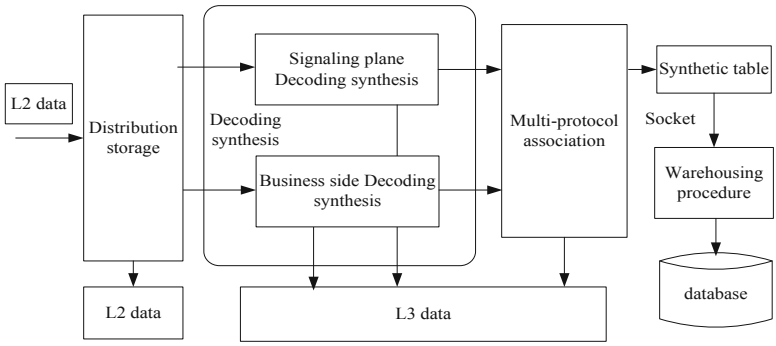

Fig. 3. Multi-protocol association.

3.4 Synthesizing the Table and Data Check Module

Synthesized the associated fields of the same user, and the synthesized XDR is sent to the storeroom program through the Socket interface, and the table is exported to the database. When the client wants to view the result, it first requests message statistics from the server, and the statistics are returned to the client. The client initiates a request to the service, and the service process obtains the summary information by searching for the L2 key data, and returns the summary information to the client. The user can check the composite signaling process after the multi-protocol association through the signaling reverse check.

4 Algorithm Design

4.1 Hash Signaling Analysis Algorithm

In the traditional hash signaling analysis algorithm (HSAA), the synthesis of the signaling and the multi-protocol association map the Key value of the signaling into the hash table [11]. Hash table is widely used because of its fast query speed in data query and convenient insertion and deletion operations [12]. When the signaling process information is associated with the XDR, the source IP, the source port number, the destination IP address, and the destination port number are selected as the Key value to construct a

hash function, and the hash algorithm is used to search for the corresponding letter in the hash table by using the Key value of the signaling message. Let the process complete the relevant signaling process association [13].

In the form of hash index, the index value adopts a specific Key value, and different signaling processes have corresponding Key values. In the integrated signaling XDR synthesis process, the user's Key value may correspond to different Value [14]. At this time, the Key value with the same hash address will cause a conflict [15]. Its hash address is $p = H(Key)$, When a conflict occurs, it is the address that generated the conflict $H(Key)$ Find an address sequence:

$$H_0, H_1, H_2, \ldots, H_s (1 \leq s \leq m-1) \tag{1}$$

Among:

$$H_0 = H(Key) \tag{2}$$

The general form of hash function is:

$$H_i = (H(Key) + di) \ \% \ m \ (i = 1, 2, \ldots s) \tag{3}$$

Where $H(Key)$ is a hash function, m is a table length and d_i is an incremental sequence.

The HSAA algorithm generally uses the open address method when dealing with hash collisions, but the open address method is prone to data accumulation problems. When the node size is large, it wastes a lot of space, consumes a large memory, and is not suitable for large-scale data storage, There may be multiple conflicts when inserting, and when the deleted element is one of multiple conflicting elements, the subsequent elements need to be processed, which is more complicated to implement.

In the HSAA algorithm, the value of the Key value of the signaling key message is sorted according to the direct insertion method, but the direct insertion method has more comparison times, greater time complexity, and lower efficiency.

4.2 Build a Hash Top Heap

In the signaling synthesis process, the HSAA algorithm is inefficient in dealing with hash collisions. in the improved signaling analysis algorithm, the hash table conflict is handled by the chain address method. Find the value in the hash table according to the hash Key value, and obtain the conflicting hash table entry pointing to the address of the linked list, and put all the Key values with the same hash address in the same synonym list, and store the head pointer of each linked list with an array. In the signaling analysis, a hash value key sequence of $\{K1, K2, K3, \ldots, Kn\}$ is assumed to be m, and a hash table that the chain address method handles conflicts is shown in Fig. 4.

In the process of signaling analysis to establish a hash table, based on the hash table address method, the Key value of the signaling message is sorted. This paper proposes a improved signaling analysis algorithm (ISAA). The same user signaling message has the Key value of the same Value, and the key top sorting method is used to sort the key words according to the probability of occurrence of Value, and the position in the linked

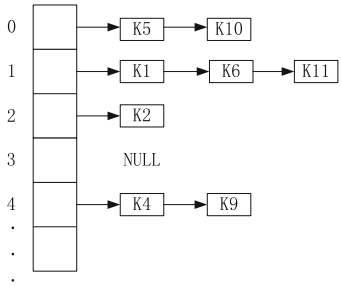

Fig. 4. Hash table when chain address method handles conflicts.

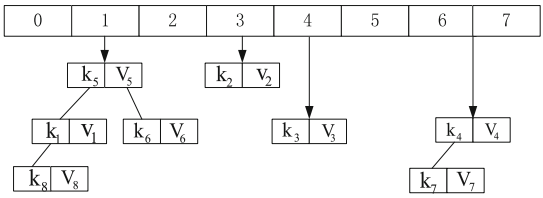

Fig. 5. Signaling message Key value hash big top heap.

list when the conflict is processed is determined according to the probability size, and increasing the look up efficiency in a hash-address conflict.

In the signaling analysis, assuming that the signaling message key sequence $\{(k_1, v_1), (k_2, v_2), (k_3, v_3), (k_4, v_4), (k_5, v_5), (k_6, v_6), (k_7, v_7), (k_8, v_8)\}$, the signaling message Key value hashes the top stack as shown in Fig. 5.

4.3 Analysis of Algorithms

In the signaling process synthesis of the signaling analysis, Judgment the corresponding signaling process message in the hash table is used to create the XDR by searching the key information of the message. The main operation is to compare the Key value of the key query. The average number of comparisons when the Key value is found successfully in the process is called Average Search Length (ASL). For the lookup table of n elements, the average search length is defined as:

$$ASL = \sum_{i=1}^{n} P_i C_i \tag{4}$$

Among them, P_i is the probability of the i-th data element in the lookup table, and C_i is the number of times that the i-th data element has been compared when it is found.

In the signaling message synthesis, based on the Value probability of finding the Key value of the signaling message, the Key value is mapped to a location in the hash table to access the record. the HSAA algorithm uses the direct insertion method to process hash collisions. The key message Key value is compared more frequently, and the time complexity is $O(n^2)$. The ISAA algorithm uses large top heap sorting when dealing with hash collisions. The number of comparisons in the search process is greatly reduced. In the worst case, the time complexity is $O(nlogn)$. Therefore, the search time is significantly reduced, and in the ISAA algorithm, the chain address method is used when processing hash collisions, the nodes in the linked list are dynamically applied, the processing conflict is simple, and there is no accumulation, and the average search length is short. It is more space-saving than the open address method, and it is convenient to insert a node in the head of the linked list and to delete a node, and only need to adjust the pointer without adjusting other conflicting elements. Therefore, for the ISAA algorithm,

the larger the amount of data, the less time consuming, which improves the efficiency and accuracy of data processing, and also improves the reuse of dynamic memory resources.

5 Test Results and Analysis

5.1 Test Results

Test environment: Windows 10 operating system, the processor is Inter(R) Core(TM) i5-4460 CPU @ 3.20 GHz, and the platform with 8.00 GB of memory is installed. This paper uses the Visual Studio 2017 compile running environment, the test program is written in C++. In the test process, based on the TS38.331 protocol in 5G, a dynamic identifier C-RNTI allocated by the base station to the UE in the signaling message is used as the key message Key value. Since the value range of C-RNTI is 003D to FFF3, the analog data source is randomly generated within its range, and 5000 test cases are obtained by assignment. Through improving the ISAA algorithm, for example, looking up the corresponding value of the key information of the signaling flow message in the hash table, and judges its existence. the statistical information is updated, and the same signaling process information of the same user is associated and synthesized. As shown in Fig. 6, During the test, the diagnostic tools of the Visual Studio 2017 compiler can be used to view the memory resources and time spent by the algorithm program in real time.

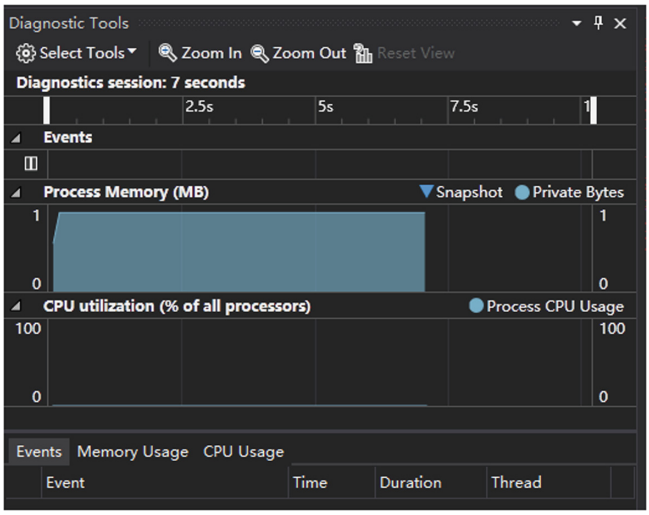

Fig. 6. Test process diagnosis.

5.2 Performance Analysis

By testing the above test cases, 5000 test cases were successfully tested. This paper compares the ISAA algorithm test results with the HSSA algorithm. As shown in Fig. 7,

compared with HSSA, the improved ISAA by using the chain address method to handle hash collisions have no memory accumulation, realizing the dynamic reuse of memory resources, and save more memory resources.

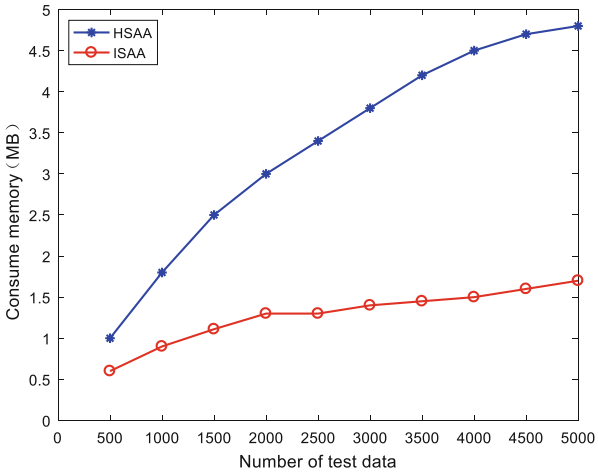

Fig. 7. Comparison of test signaling analysis consumes memory.

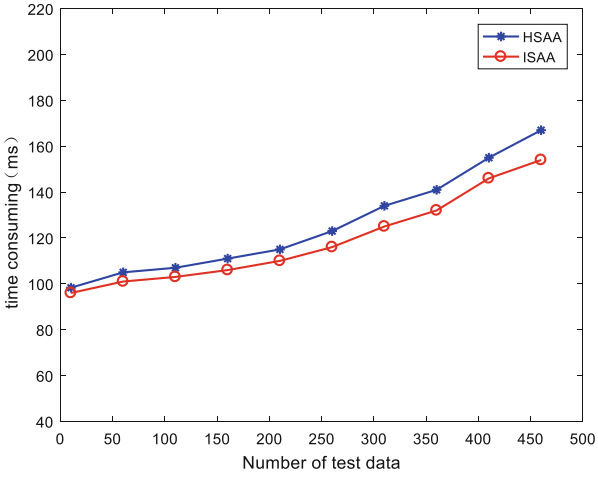

Fig. 8. Comparison of test signaling analysis consumes time of 500 data.

In the test process, as shown in Fig. 8, in the case of 50 to 500 test data, when the test data is 500, the traditional algorithm takes 167.4 ms, the improved algorithm takes 154.9 ms, and the time is reduced by 7.78%. Traditional algorithm and improvement the algorithm takes a small amount of time.

In the test results, as shown in Fig. 9, when the test data is 500, 2500, and 5000, the HSSA takes 167.4 ms, 393.1 ms, and 751.2 ms. ISAA takes 154.9 ms, 251.8 ms, and 333.5 ms, and reduced time by 55.66%. Compared to HSSA, the time required for the improved ISAA algorithm under the new architecture is significantly reduced.

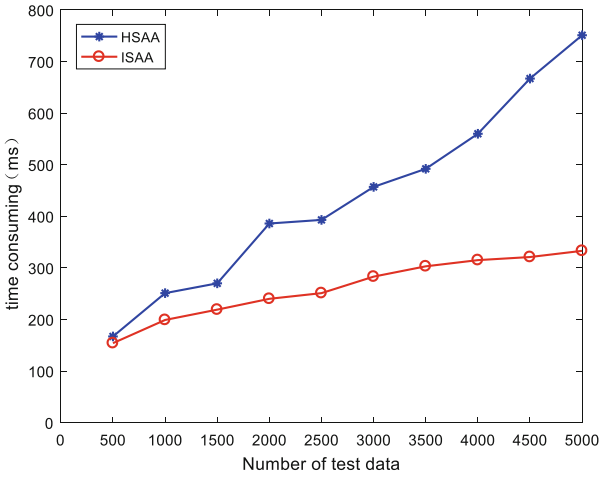

Fig. 9. Comparison of test signaling analysis consumes time of 5000 data.

The analysis rate of the signaling data of the HSSA algorithm is low, and when the amount of data is gradually increased, the analysis rate of the signaling data is slightly decreased; The signaling data analysis rate of the improved ISAA algorithm gradually increases with the amount of data, and can maintain a gradually increasing signaling analysis rate. This shows that the improved algorithm is very effective in signaling analysis.

6 Conclusion

Focused on the signaling analysis system in 5G terminal simulator, this paper designs a new signaling analysis system architecture. Compared with the traditional flat LTE-A network, it introduces the 5G network service system structure, According to the idea of modularization, the realization of centralized collaboration and control of wireless resources System, and network functions are tightly coupled moreover, in the signaling analysis process, when synthesizing XDR for signaling association, the user dynamic identification C-RNTI is selected as the Key value of the signaling message to construct a hash function, and advantages of combining the chain address method and the hash top heap sorting. An improved signaling analysis algorithm is proposed. The test results show that compared with the traditional signaling analysis system, the improved algorithm under the new architecture consumes significantly less time and memory, and the more the amount of data, the more obvious the effect. It shows that the system is effective and feasible, and it is of great significance for the optimization and testing of the 5G network to be commercialized.

References

1. IMT-2020 (5G) Program. White paper on 5G concept [S.l.:s.n.] (2015)
2. Hucheng, W., Hui, X., Zhimi, C.: Current research and development trend of 5G network technologies. Telecommun. Sci. **9**, 149–155 (2015)
3. Droste, H., Rost, P., Doll, M.: An adaptive 5G multiservice and multitenant radio access network architecture. Trans. Emerg. Telecommun. Technol. **27**(9), 1262–1270 (2016)
4. Padilla, P., Hirokawac, J., Foged, L.J., et al.: Future 5G millimeter-wave systems and terminals: propagation channel, communication techniques, devices, and measurements. IEEE Commun. Mag. **56**(7), 12–13 (2018)
5. Liu, T., Li, J., Feng, S., et al.: On the incentive mechanisms for commercial edge caching in 5G wireless networks. IEEE Wirel. Commun. **25**(3), 72–78 (2018)
6. Fan, Z.: The key technologies research of the signaling monitoring system correlation and correlation and refill. Telecommun. Netw. Technol. **10**, 56–59 (2011)
7. Wang, F., Jiao, M., Jia, Y.: Research and implementation of traffic monitoring technology on S1 interface in LTE network. J. Chongqing Univ. Posts Telecommun. Nat. Sci. **26**(3), 292–297 (2014)
8. Li, L., Zhang, Z., Xi, B.: Research and implementation of multi-protocol association scheme on Uu interface in LTE-Advanced network. Telecommun. Sci. **32**(6), 167–176 (2016)
9. Peng, L., Longhan, C., Zhizhong, Z.: Research and implementation of user behavior analysis system on Uu interface in LTE-Advanced network. Video Eng. **11**, 135–140 (2017)
10. Luo, F.L.: 5G new radio: standard and technology. ZTE Commun. 15(s1) (2017)
11. Zhang, Z., Liu, Y.J.: Effective solution to hash collision. J. Comput. Appl. **30**(11), 2965–2966 (2010)
12. Collom, G., Redman, C., Robey, R.W.: Fast mesh to mesh remaps using hash algorithms. SIAM J. Sci. Comput. **40**(4), 450–476 (2018)
13. Fangfang, Z., Xungen, L.: Improved searching method of hash table. J. Hangzhou Dianzi Univ. (Nat. Sci. Ed.) **5**, 46–49 (2013)
14. Chevalier, Y., Kourjieh, M.: A symbolic intruder model for hash-collision attacks. In: Okada, M., Satoh, I. (eds.) ASIAN 2006. LNCS, vol. 4435, pp. 13–27. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-77505-8_2
15. Ndoundam, R., Karnel, J.: Collision-resistant hash function based on composition of functions. Comput. Sci. **14**, 167–183 (2011)