DOI 10.15302/J-SSCAE-2020.06.016

Node Status Monitoring of Information-Centric Internet of Things

Cui Liqun, Wu Jun

Institute of Cyber Science and Technology, Shanghai Jiao Tong University, Shanghai 200240, China

Abstract: To manage the constantly changing network status information of the information-centric Internet of Things (IC-IoT), this study proposes a node status monitoring program. It first proposes a new management information base structure for recording various network node status information and adopts the naming format of information-centric networking (ICN), centering on the content of the network node status. In this architecture, we combined the trace routing method and adaptive data placement strategy based on the importance of the data block, to obtain the required network status information and improve retrieval efficiency. At the same time, this scheme proposed the design of a security protection mechanism to achieve the purpose of ensuring data confidentiality and access control for management users. Finally, through the establishment of a network simulation test environment, the time delay caused by the above-mentioned trace routing mechanism, adaptive data placement strategy, and access control security protection was evaluated. The simulation results showed that this scheme could effectively improve the efficiency of data acquisition. The access control model provides data confidentiality and other security functions for the solution, at only a small computational cost.
Keywords: information-centric networking; Internet of Things; node status monitoring; access control

1 Introduction

Information-centric networking (ICN) is a new idea for future Internet of Things (IoT) network architecture design. There are few IoT solutions based on ICN that verify the applicability of ICN to IoT. Although there is much research on ICN architecture, current evaluation and verification methods have remained at the level of simulation and the theoretical discussion of ICN itself, such as cache optimization. Lee H et al. [1] proposed an ICN-OMF framework for the control and management of a scalable content-centric networking (CCN) test platform, including the control and management of multiple CCN nodes scattered in different geographical locations. Moreover, there have been few studies of the monitoring and management of ICN nodes, and most have focused on the implementation of a single IoT application. This paper focuses on the construction a complete framework for controlling and monitoring each device node of the information-centric IoT (IC-IoT) system.

2 Relevant background technology

2.1 ICN

ICN takes information as the core of the network, rather than the IP stack structure. It also uses information for unique identification. When a user requests certain information, the object of the request is the information itself,

Received date: September 15, 2020; **Revised date:** October 25, 2020
Corresponding author: Wu Jun, professor of Institute of Cyber Science and Technology of Shanghai Jiao Tong University. Major research field is Internet of Things and its security, cloud computing/fog computing and its security, next-generation Internet and its security, big data, and artificial intelligence security. E-mail: junwuhn@sjtu.edu.cn
Funding program: CAE Advisory Project "Strategic Research on Cyberspace Security Assurance"（2017-XY-45）
Chinese version: Strategic Study of CAE 2020, 22 (6): 121–127
Cited item: Cui Liqun et al. Node Status Monitoring of Information-Centric Internet of Things. *Strategic Study of CAE*, https://doi.org/10.15302/J-SSCAE-2020.06.016

and the information is the credential used during the processing of the request, which is equivalent to the IP address in the IP network. The information provider looks up the corresponding data according to the information name and returns it to the requesting user. ICN is regarded as a revolutionary form of architecture that places data in the primary position in the network by directly naming it. It is neither an IP mode nor an IP overlay mode but a brand-new network mode of the future [2]. There have been many achievements in ICN research in China and abroad, and due to the lack of design consensus, a considerable number of ICN structures have been proposed to date. The most used and recognized ICN structures are DONA, PSIRP, NetInf, and CCN.

Named data is the basic idea of ICN, but it does not represent a complete architecture design. ICN architecture also achieves efficient data distribution through an intra network caching mechanism; therefore, data not only exists in producers but may also be cached in other network routers, so that consumers can retrieve it from a more convenient location when there is a request for it again. This change from a “location-based” to a “content-based” network improves the efficiency of content dissemination and brings scalability, security, mobility, multi access points, and other characteristics [3].

Like ICN, in IoT, consumers are interested in data content, rather than their location, which means that IoT is actually content-centric. Therefore, the ICN design concept is also applicable to IoT, and there is no need to maintain point-to-point communication. The concept of IC-IoT has been put forward by some researchers. In recent years, there have been many studies of IoT mechanisms based on ICN. In future, IoT will develop in an information-centric direction [4,5].

2.2 IoT node monitoring

With the continuous expansion of the Internet, the importance of appropriate Internet management (including network analysis and diagnosis) has also increased. It is necessary to monitor and manage all kinds of network equipment, and realize the centralized management of status information. IoT has many applications in smart homes and cities, transportation systems, industrial control systems, health care monitoring systems, and so on. Many studies have used wireless sensor networks (WSNs) to correlate the information associated with physical domains and IoT-driven computing systems by accessing the status of different entities in all locations and environments and collecting data for long-term IoT monitoring. For effective operation of the network, IoT must also monitor, control, and record the network performance and the use of device resources. The device manager is responsible for collecting network device information, including device characteristics, data throughput, communication overload, and errors. In future, IoT architecture will develop in a content-based direction, and network node monitoring systems using IoT technology will also change. In the application scenario of IC-IoT, network node monitoring has a large research space.

3 Node status monitoring architecture of IC-IoT

3.1 Overall architecture of an information management database based on naming

Inspired by the principles of ICN and based on a simple network management protocol (SNMP), this paper proposes the design of a content-based management information base (MIB) structure for the monitoring and management of IC-IoT nodes. Based on the basic idea of “unified maintenance of all network node devices,” and following ICN content-centric principles, the MIB structure saves relevant information of all running devices and responds to query requests by the management workstation. The corresponding overall structure is shown in Fig. 1.

Different from the tree structure of the MIB in a traditional SNMP, data objects are named and divided into a series of data blocks according to their types. An enterprise or organization can be defined as a data block, and a protocol or even a function module can be defined as a data block. The names and content of these data blocks are put together to form a central data block. In each data block, data objects are stored by content name, considering the status of network nodes, including their access rights, status, default value, historical access times, and other attributes. When the agent needs a data object, it first searches for the sub block where the data is located in the central data block and then obtains the required data in the sub block. Through this method, the principle of fast positioning of target data is briefly introduced, to better support data updating, such as block dynamic loading and unloading. To monitor the status of a network node, it is necessary to consider the working status and access status

DOI 10.15302/J-SSCAE-2020.06.016

of the node. The access status of a node in a traditional network system is divided into node identity and node access location. The former refers to the type of device, reflecting the role of the node in the network and its location in the network topology, and the latter is the logical location determined by subnet partition or the real physical location determined by the physical connection between nodes. Because ICN does not consider node locations, node states related to naming only need to describe the node working state (such as system information, interface information, and operation parameters) and node identity.

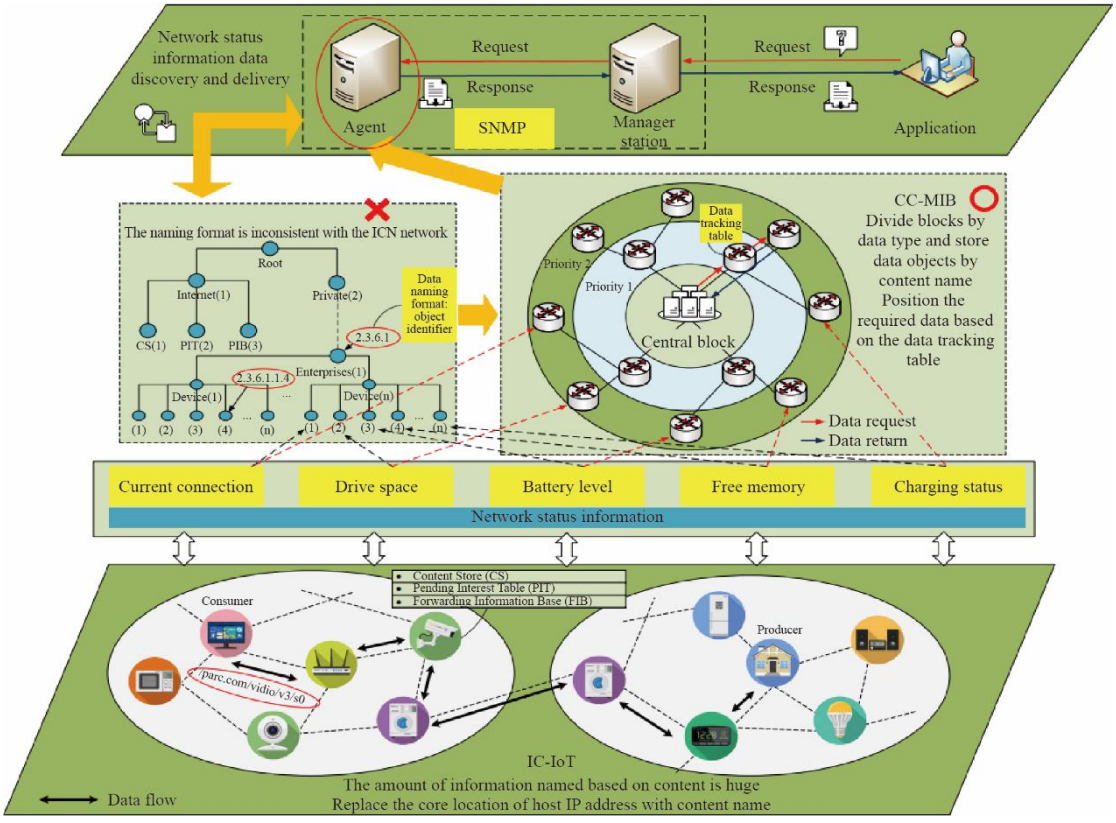

Fig. 1. Content-centric named MIB in IC-IoT.

3.2 Acquisition of node status data based on naming

Each ICN router has three functional modules for routing and forwarding content: content store (CS), pending interest table (PIT), and forwarding information base (FIB). With this forwarding strategy, information allocation in ICN is more efficient and accurate, which is consistent with the design goal of an effective IC-IoT management mechanism. Three tables are also defined: data block importance table, data block structure table, and data tracking table. The data block importance table records the importance of each data block, and the data block structure table records the topology information between data blocks, which are stored in the central data block. The data tracking table is stored in each sub data block, including the name of the content and the name of the next data block containing the content.

As shown in Fig. 2, when the agent receives a data request from the management station, it first checks whether the request name contains the data block name where the data object is located. If it exists, the data is directly obtained from the central data block and returned to the management station; otherwise, starting from the central data block, data is searched in all sub data blocks of the first priority. If the content name in the data tracking table of a sub block is found to match the required data content name, the request is forwarded to the next sub block according to the information in the data tracking table. In this way, the priority decreases until the data block where the required data exists is found.

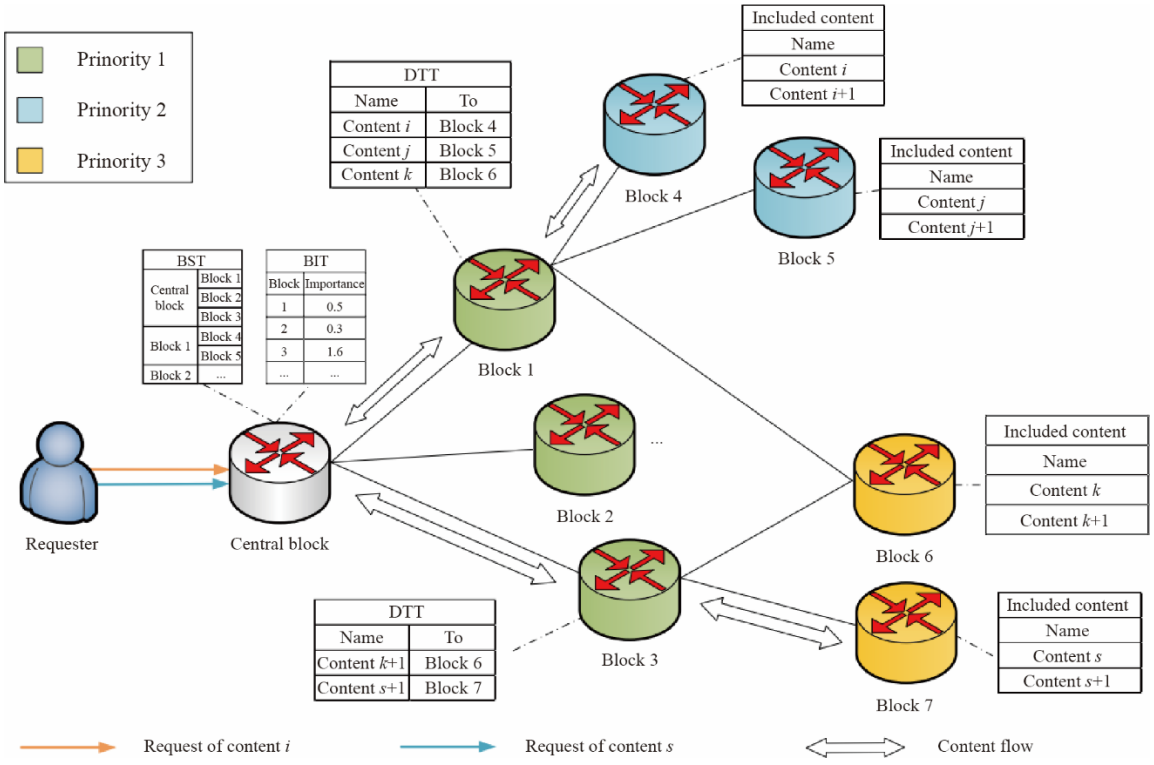

Fig. 2. Node status data acquisition process based on name.

Note: BIT is the data block importance table; BST is the data block structure table; DTT is the data tracking table.

For the placement of data blocks, this study used a priority-based edge placement strategy. First, the importance of the data block was defined as a parameter. Different from the traditional strategy which only considers popularity, this study changed the placement of the data blocks in real time according to their importance; the more important the data block, the higher its priority. Compared with the traditional MIB structure, the agent can retrieve the required data faster and improve the real-time performance of network node monitoring.

4 Status monitoring and security protection of IC-IoT

4.1 Security issues in node state monitoring

Compared with IP network technology, ICN is more suited to IoT applications because of its intra network caching and mobility support features. However, it also creates some security challenges. First, because content occupies the core position in the network, it is vulnerable to interest flooding and content poisoning attacks. Second, the most important security issues in ICN are content and cache privacy [6]. From the perspective of network monitoring and management, ICN has many security challenges, such as access control, authentication, data security, and privacy. This paper focuses on solving two security problems in the process of IC-IoT node status monitoring: content privacy protection and management station access control.

4.2 Name-based trust mechanism

Without considering the content itself, trust between consumers and producers is obtained from pre-agreed credentials. The principle is to obtain trust directly from the public identity or content name: if you choose a trusted identity, you will have a certain degree of trust in the content associated with the identity, and this association should be easy to verify.

When the name contains valid information about the real identity of the entity, the identity of the entity can be ensured, but a mechanism is needed to verify the validity of the information. Similarly, the public key should be bound to the real-world identity of its owner, as it will be used for producer authentication. To provide data

DOI 10.15302/J-SSCAE-2020.06.016

confidentiality, the data must be named based on an encryption model, and the authorized entity must know the decryption key. To verify the identity of the producer and ensure the validity of the data, all contents must be digitally signed with the private key of the original content provider. If the content name does not contain enough valid information about the identity of the producer, an attack will be launched in the following ways. By listening to the interest packet, the attacker will construct false content and bind it with the legal content name. The attacker will send a packet to the requester, including the same name, the wrong content, his own key information (in the signed information field), and the associated digital signature. After receiving the content, the requester considers the data as normal data according to the public key and the attacker's certificate. Because the packet looks legal and has a legal signature, the requester will not be aware of the attack.

4.3 Access control for node monitoring

Access control is an important means to ensure security in ICN. If access control is not applied, there will be no difference between legitimate and malicious users, the proxy will publish data in any namespace, and the requester can access any content. The importance of this security requires the use of an access control model. This paper suggests that while the agent handles key management and data content publishing, it should also set the maximum access time for the management user [7] and perform authentication and review according to the user signature attached to the interest package sent by the management station. When legitimate users try to exceed their limited access time, the agent will perceive this deceptive behavior.

In this design, the content provider (proxy station) divides its storage content into different groups with unique group identifiers (GIDs) according to the configured security policy and adds the GID to the content name. In addition, a privilege mask is used to represent the user's privilege, and a user can access the content of multiple groups. The privilege mask is a bit map, and each bit indicates whether the user can use the content in the corresponding group. For example, if the second bit of the user rights mask is "1," the user has access to the content in the group with GID 2.

The management user first registers with the agent. When the management user whose access time is limited registers with the agent, the agent generates the privilege mask of the management user and sets the maximum access time according to the use's identity. Then, the user sends the interest packet with the additional signature to obtain the required data, and the agent verifies the request according to the obtained user information. After successful authentication, the interest packet is allowed to enter and return the corresponding content packet. To ensure the confidentiality of the data, the agent encrypts the content before returning the packet to the management station. The specific access control model is shown in Fig. 3. A hash chain is used to improve the efficiency of the authentication process and reduce the burden of the proxy station. The user will generally continue to request a series of data. The proxy can use the one-way attribute of the hash chain to authenticate the user by signing the first request of the file and use the hash chain to authenticate the subsequent request files that are the same as those of the hash chain.

5 Experimental test and evaluation

This study used ns-3 and ndnSIM2.5 to model and simulate the IC-IoT node condition monitoring architecture and analyze the results. The whole simulation was divided into two parts: the first evaluated the tracking routing data acquisition mechanism and importance-based data placement strategy, and the second evaluated the access control model and obtained the influence of the parameters on the delay in monitoring data acquisition. First, a simple data block topology was established, assuming that the amount of data in each data block was the same. Then, different importance levels were set for each data block.

5.1 Data placement strategy evaluation

In the simulation process, a topology structure with 37 available data blocks was adopted. Except for the central data block, the priority of other data blocks varied from 1 to 6. The expected result was that, in this information management library structure, the time required to obtain the data would be inversely proportional to the importance of the block. If there was no block name or tracking routing policy in the request, the time delay for obtaining the data would be significantly different.

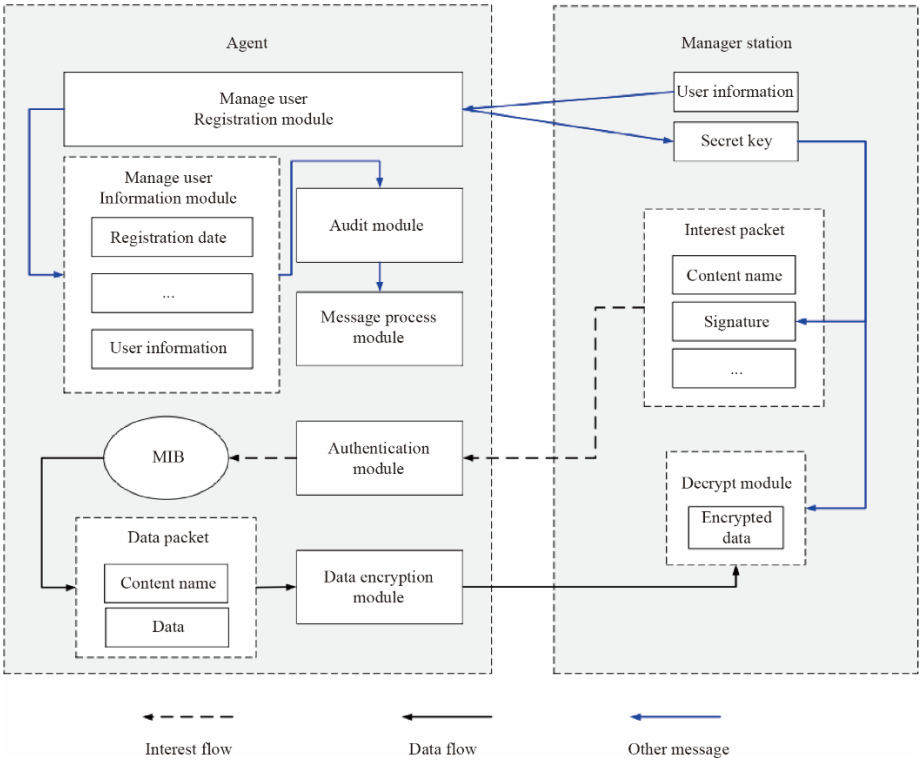

Fig. 3. Access control model for node monitoring.

As can be seen from Fig. 4, compared with the replacement strategy based only on the number of requests or the popularity of content, the average hop number of requested data was significantly reduced after using the replacement strategy based on the importance of data blocks. This was because in the latter strategy, frequently requested data were placed in a higher priority data block, making an adaptive replacement strategy of data blocks necessary.

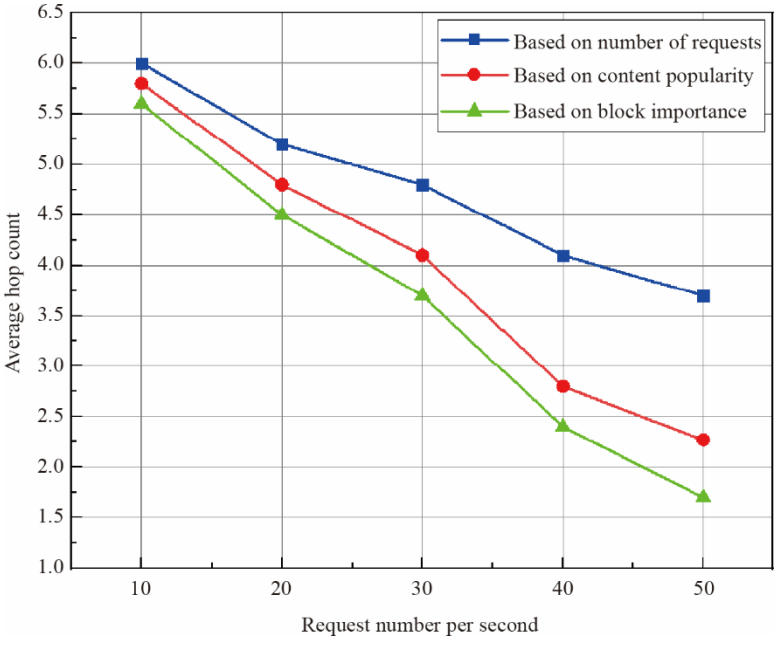

Fig. 4. Comparison of results of different replacement strategies.

DOI 10.15302/J-SSCAE-2020.06.016

5.2 Data acquisition model evaluation

According to the defined ICN data object naming rules, data acquisition model evaluation was applied to the IC-IoT node condition monitoring scenario. The content name defined in the new MIB structure based on content naming included the name of the data block (i.e., resource principal name). The management user sometimes does not know the specific and complete name of the content they are requesting; therefore, the data block name will not always be included in the requests. Three cases are considered for this purpose. Scenario 1: there is a request for an interest package containing a data block name. Scenario 2: the request does not contain the data block name, and there is no tracking routing strategy in the data collection process. Scenario 3: there is no data block name in the request, but there is a tracking routing strategy in the data collection process. This study tested the delay time for acquiring device status information data in these three scenarios. When the priority was high, the delay reduction effect of the tracking routing strategy was more obvious (Fig. 5).

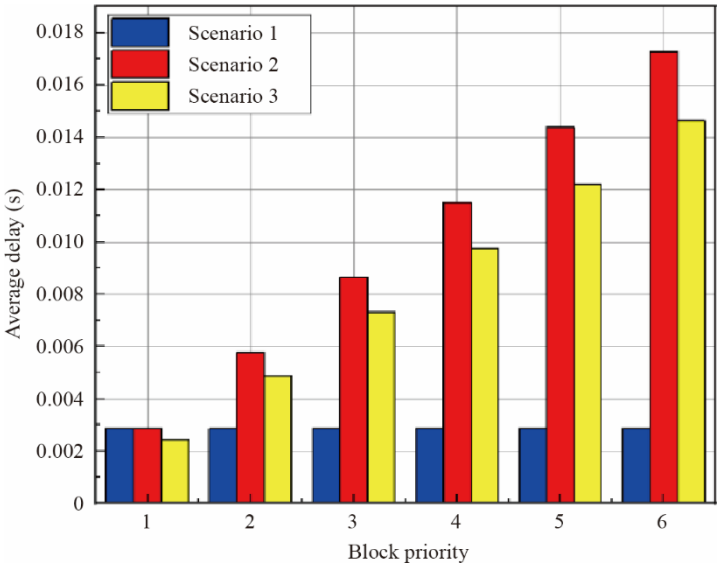

Fig. 5. Evaluation results of data acquisition model.

5.3 Access control mechanism evaluation

The access control model in ndnSIM 2.5 was simulated and compared with the performance of a basic named data networking (NDN). At the time, the size of the data blocks in the MIB was different. Five types of nodes were set in the simulation: 10 MB, 100 MB, 300 MB, 700 MB, and 1 GB. Each topology node represented a data block. The packet size of each request by the management node was set to 1 MB, and the request interval was set to 2 s. When a request from a management station node arrives at the data provider node, the request must be authenticated. During this process, the time cost of the access control model was evaluated by analyzing the delay in network packet acquisition. When the management station router requests the content with the correct prefix and always requests the data in the same data block continuously, Fig. 6 shows the data retrieval delay of different data block sizes, and the basic NDN caused a lower delay. When the access control mechanism was added to the network, if the size of the data block was not too large, its performance was still very good. With the increase in data block size, the difference between the network with the access control mechanism and the basic NDN became obvious, as more data blocks meant that authentication and decryption needed to be performed more often. Overall, the gap between the basic NDN and the network with the access control mechanism in the data acquisition delay was acceptable.

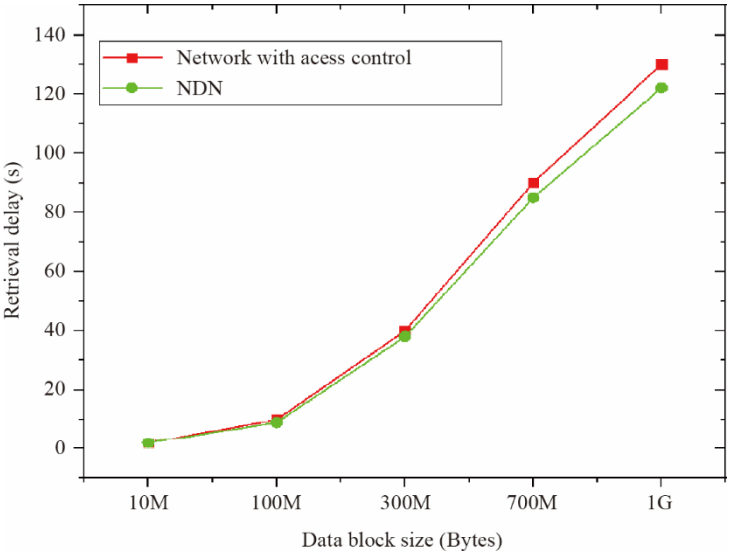

Fig. 6. Impact of access control mechanism on data acquisition.

6 Conclusion

This paper focuses on the design of node status monitoring architecture and security protection technology for IC-IoT. In terms of monitoring architecture, only a new MIB structure different from the traditional network management protocol is proposed to adapt to the future development of ICN, but the monitoring process was only carried out in the local management station. Follow-up research can extend intelligent management to the edge of the network and use hierarchical architecture to implement local management decisions, to thereby expand network coverage and implement more accurate monitoring of network nodes. It could also further enhance the security protection mechanism of the architecture, from access control and simple data encryption to a more advanced and service-independent security mechanism. Adding decentralized blockchain technology to security protection could also be considered to better protect data confidentiality and integrity in the process of data exchange and avoid damaging the necessary functions of future mobile devices and Internet supporting fifth generation mobile communication.

References

[1] Lee H, Kim D, Suh J, et al. ICN-OMF: A control, management framework for Information-Centric Network testbed [C]. Gwangiu: International Conference on Information Networking (ICOIN), IEEE, 2015.

[2] Sun Y B, Zhang Y, Zhang H L. Survey of research on informationcentric networking architecture [J]. Acta Electronica Sinica, 2016, 44(8): 2009–2017. Chinese.

[3] Yang R B, Ma Y. Research on forwarding strategies in named data networking [J]. The Journal of New Industrialization, 2015, 5(10): 63–71. Chinese.

[4] Amadeo M, Campolo C, Quevedo J, et al. Information-centric networking for the internet of things: Challenges and opportunities [J]. IEEE Journals and Magazines, 2016, 30(2): 92–100.

[5] Arshad S, Azam M, Rehmani M. Recent advances in Information-Centric Networking-Based Internet of Things (ICN-IoT) [J]. IEEE Internet of Things Journal, 2019, 6(2): 2128–2158.

[6] Huo Y H, Liu Y L. Survey on security issues in content-centric networking [J]. Telecommunication Engineering, 2016, 56(2): 112–120. Chinese.

[7] He P, Wan Y, Xia Q, et al. LASA: Lightweight, auditable and secure access control in ICN with limitation of access times [C]. Kansas City: IEEE International Conference on Communications, IEEE, 2018.