Research on Access Control of Smart Home in NDN (Short Paper)

Rina Wu, Bo Cui(✉), and Ru Li

Inner Mongolia Key Laboratory of Wireless Networking and Mobile Computing,
College of Computer Science, Inner Mongolia University,
Hohhot 010021, China
wrn@mail.imu.edu.cn, {cscb,csliru}@imu.edu.cn

Abstract. Named Data Networking (NDN) is one of the future Internet architectures and can support smart home very well. There is a large amount of private data with lower security level in smart home. Access control is an effective security solution. However, the existing NDN's access control mechanisms that can be applied to smart homes don't reasonably use the cache in NDN and take into account users' authorization cancellation phase. Therefore, we designed an access control mechanism for smart homes in NDN. We mainly consider the process of the user requests permission, user requests data and user permission cancellation. By using the Cipher Block Chaining (CBC) symmetric encryption algorithm, identity-based encryption, and proxy re-encryption, the cache in NDN is effectively utilized, and the counting Bloom Filter is used to filter ineffective Interest packets and complete the user's privilege cancellation phase. Experimental results show that the access control mechanism designed in this paper can effectively reduce the total time which starts from user requests the permission to decrypt data and reduce the time overhead of the NDN routers in the process of user privileges cancellation after using the counting Bloom Filter.

Keywords: Named Data Networking · Access control · Smart home · Encryption

1 Introduction

Smart home is a recent research hot spot of the Internet of Things and has a great influence on people's daily life. It is composed of a large number of low-power resource constrained devices, and in the communication process it involves large amounts of small data exchange and so on. So these features lead to obvious differences between smart home and TCP/IP in design concept and construction system [1]. For example, the communication of TCP/IP is connection-oriented, making it difficult to maintain the communication in the smart home. Named Data Networking (NDN) can solve the above problems [2]. For example, NDN can use namespace to solve home devices which require a lot of IP address.

NDN can solve many problems of smart home in TCP/IP, but NDN still has many shortcomings in solving the problem of smart home security. Therefore, in NDN, the

H. Gao et al. (Eds.): CollaborateCom 2018, LNICST 268, pp. 560–570, 2019.
https://doi.org/10.1007/978-3-030-12981-1_39

security of smart home is crucial. Access control is an important solution to NDN-smart home security. It restricts users' access to the protected resources and ensures that private data is only used by legitimate users [3].

According to the characteristics of NDN, many kinds of access control mechanisms are designed to enhance the security of NDN communication. As the Zhang team at UCLA proposes that data can be protected in the communication process through encryption as long as the naming mechanism and the key representation are accurate [4]. Zhang et al. [5] explain the design of the naming mechanism in detail. The access control mechanism of the existing NDN can be divided into the following aspects: based on ordinary encryption, based on attribute encryption, based on ambiguous name, and access control mechanism combined in many ways [6]. Chen et al. [7] encrypt data using a symmetric encryption algorithm, encrypt data keys using asymmetric encryption algorithms, but without making reasonable use of the NDN cache feature. Hamdane et al. [8] proposed identity-based encryption access control, although it is guaranteed that private keys will no longer be allocated using public key certificates, Simplifying public key management and saving computing and communication costs, but cannot guarantee the security of key distribution. Attribute-based encryption is mainly based on users' attributes [9]. The mechanism includes a set of attributes composed of multiple attributes and integrates the access structure into the property set. This mechanism causes a large amount of encryption/decryption overhead and a lack of attribute recovery mechanism. Wood et al. [10] use proxy re-encryption method to design and implement the secure content transmission in order to ensure the security of the content itself without considering the data consumer's identity information and the stage of consumer permission application logout.

The main work of this paper is to make use of the NDN cache feature in the process of user requesting data to cancel the user privileges and reduce the total delay (from permission application to decryption) and improve the user logout mechanism.

The rest of this paper is organized as follows. Section 2 introduces system model design, namespace design and overall flow design of access control. Section 3 deals with experimental testing and performance analysis. Finally, Sect. 4 summarizes the full work and discusses future work.

2 NDN-Smart Home Access Control Design

2.1 System Model

In smart home, the home manager is responsible for managing all the devices. In this system, home manager is defined as the home administrator who performs the functions that grant users privileges. Figure 1 shows the NDN-smart home model. And this system includes five entities: home manager, user, intelligent gateway, home cloud and smart home devices. We assume that all five entities have very high security. The routers are NDN routers, and the security of the NDN routers is greatly improved. The research focus on the parts labeled ① and ② in Fig. 1, namely, the user application/revocation authority and user request data phase.

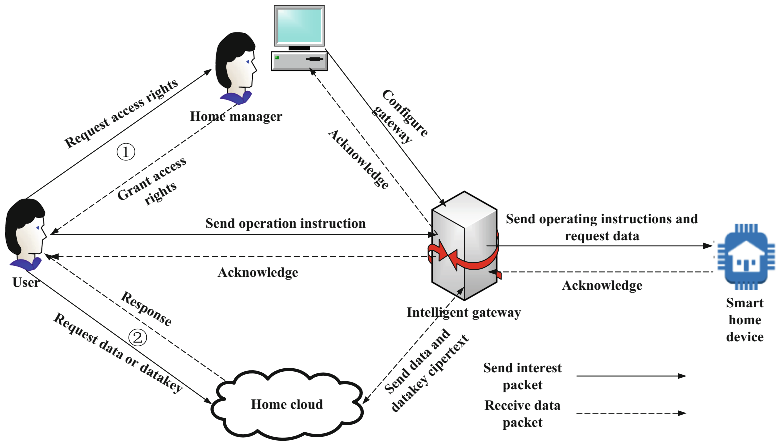


Fig. 1. The system model of NDN-smart home

2.2 NDN-Smart Home Namespace

Figure 2 shows the design of namespace by using a name tree to represent the composition of the namespace. In this paper, /ndn/homeID is used as the common prefix in smart home. /ndn indicates that all communication processes in smart home are performed in NDN. /homeID represents the home manager. The namespace is divided into user sub-namespace: /user, task sub-namespace: /task, and key sub-namespace: /key for three different service models. /location and/sensor are the correspondence of the physical location of the device. /userID represents the identity of the requesting user.

2.3 Overall Flow of Access Control Mechanism

The access control mechanism designed in this paper needs to be implemented in combination with symmetric encryption, identity-based encryption, proxy re-encryption and counting Bloom Filter.

The access control mechanism studied is the part of ① and ② of Fig. 1, corresponding to Fig. 3. The access control mechanism is divided into four stages: initialization stage shown as the part ① in Fig. 3, the user application permission stage shown as the part ② in Fig. 3, the user access data stage shown as the part ③ in Fig. 3 and the user logout stage, the logout process is similar as the user application process. The following is a detailed introduction to each phase:

Initialization Phase

In the stage of data encryption, we use CBC to encrypt the data generated by the device. Secondly, the private key generator in the identity-based encryption algorithm is used to generate the private key corresponding to the identity public key for the home manager and users.

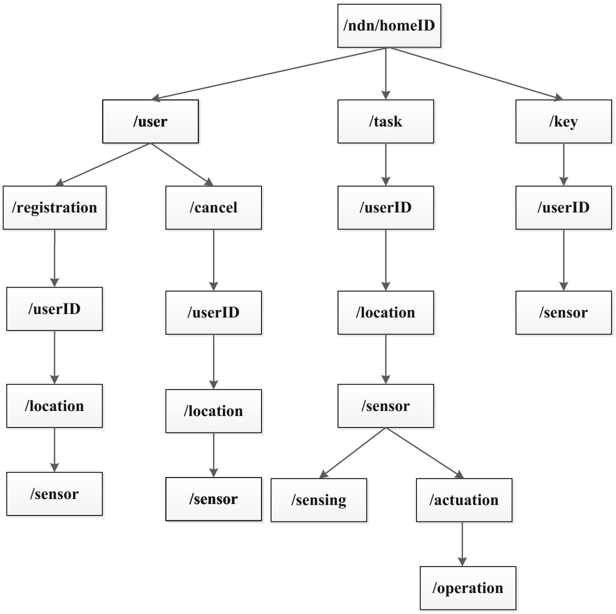


Fig. 2. NDN-smart home namespace

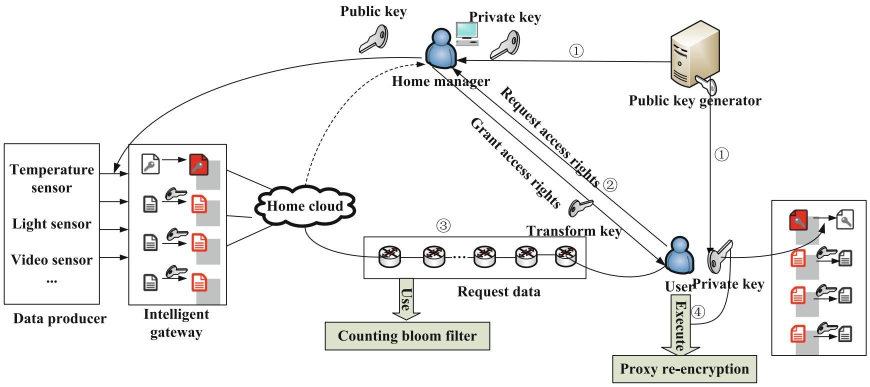


Fig. 3. Access control mechanism

User Applies Permission Phase

When users apply for access, $user_i$ must send an Interest packet signed by his private key to the home manager and indicate the time of application, if the user does not set the time, the time is set by the home manager to the default value. After successful authentication, the home manager will add $user_i$ information to the user registry. The user registry are listed in Table 1.

Figure 4 shows the message sequence chart of requesting permission for users. After successfully verifying the identity of users, the home manager will generate the

Table 1. User registry

User	Public key	Public key digest	Data type	Time (month)
Alice	Pk(Alice)	SHA256(Pk(Alice))	Light	6
Bob	Pk(Bob)	SHA256(Pk(Bob))	Temperature	12
John	Pk(John)	SHA256(Pk(John))	Light	6
Eva	Pk(Eva)	SHA256(Pk(Eva))	Electricity	24
…	…	…	…	…

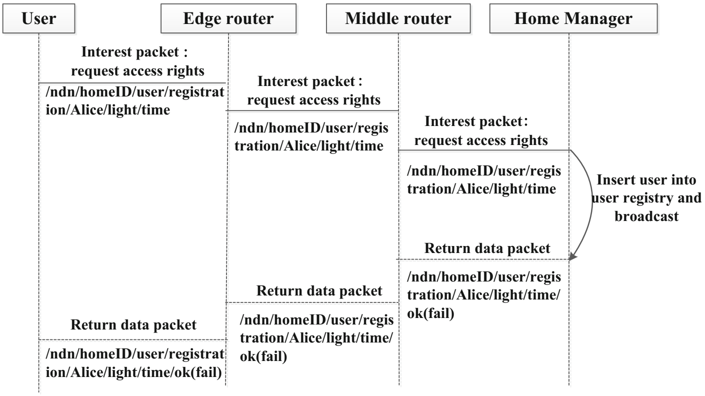

User
Edge router
Middle router
Home Manager
Interest packet : request access rights
/ndn/homeID/user/registration/Alice/light/time
Interest packet : request access rights
/ndn/homeID/user/registration/Alice/light/time
Interest packet: request access rights
/ndn/homeID/user/registration/Alice/light/time
Insert user into user registry and broadcast
Return data packet
/ndn/homeID/user/registration/Alice/light/time/ok(fail)
Return data packet
/ndn/homeID/user/registration/Alice/light/time/ok(fail)
Return data packet
/ndn/homeID/user/registration/Alice/light/time/ok(fail)

Fig. 4. MSC of user request permission process

transform key using the re-encryption key generation algorithm of proxy re-encryption. It is returned to users in the registration confirmation data packet, which is used as the certificate for users to register successfully.

User Requests Data of Data Key Phase

In the stage of user request data, there are four processes: user request data, user request data key, decrypt data key cipher text and decrypt data cipher text. The four processes will be explained in detail in this section.

Users can access the data in two ways:

One is the intermediate routers don't cache the data and data keys cipher text required by the authorized user. Figure 5 is the message sequence chart in which the user requests data from the data provider (i.e. home cloud) is shown.

The other is intermediate routers which have cached the data and data key cipher text needed by authorized users. Figure 6 is the message sequence chart, which makes reasonably use of the cache characteristic of NDN.

User Logs off Permission Phase

There are two different logout situations in this mechanism:

Figure 7 shows the active cancellation. The passive cancellation is the home manager which will delete the users in the registered user table according to the time in

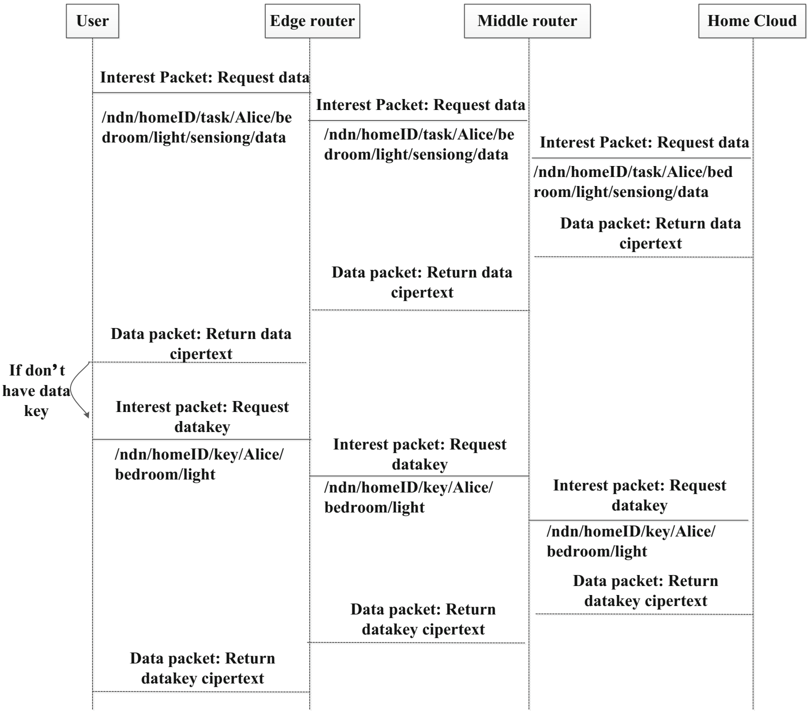

User
Edge router
Middle router
Home Cloud
Interest Packet: Request data
/ndn/homeID/task/Alice/be droom/light/sensiong/data
Interest Packet: Request data
/ndn/homeID/task/Alice/be droom/light/sensiong/data
Interest Packet: Request data
/ndn/homeID/task/Alice/bed room/light/sensiong/data
Data packet: Return data cipertext
Data packet: Return data cipertext
Data packet: Return data cipertext
If don't have data key
Interest packet: Request datakey
/ndn/homeID/key/Alice/ bedroom/light
Interest packet: Request datakey
/ndn/homeID/key/Alice/ bedroom/light
Interest packet: Request datakey
/ndn/homeID/key/Alice/ bedroom/light
Data packet: Return datakey cipertext
Data packet: Return datakey cipertext
Data packet: Return datakey cipertext

Fig. 5. MSC of user request permission process

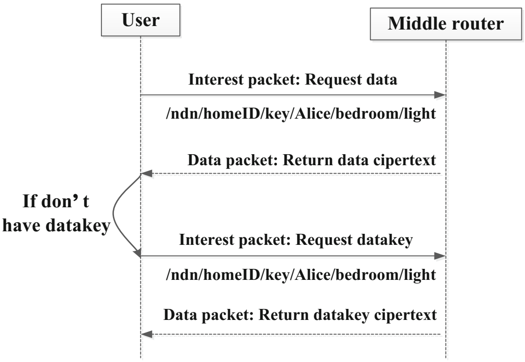

User
Middle router
Interest packet: Request data
/ndn/homeID/key/Alice/bedroom/light
Data packet: Return data cipertext
If don't have datakey
Interest packet: Request datakey
/ndn/homeID/key/Alice/bedroom/light
Data packet: Return datakey cipertext

Fig. 6. MSC of user request permission process

the registry within a certain period of time and broadcast the deleted users to the intermediate routers. And the middle routers will update the counting Bloom Filters in time.

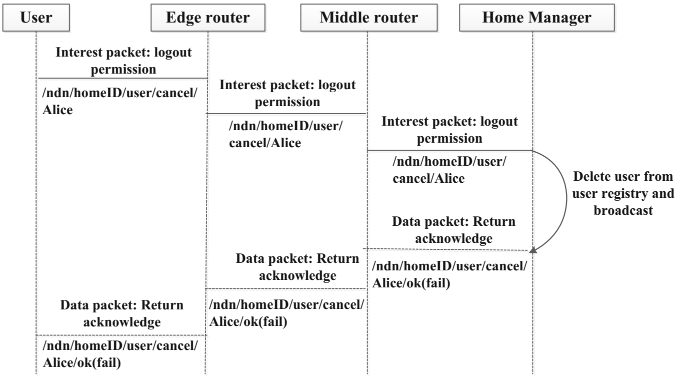

User
Edge router
Middle router
Home Manager
Interest packet: logout permission
/ndn/homeID/user/cancel/Alice
Interest packet: logout permission
/ndn/homeID/user/cancel/Alice
Interest packet: logout permission
/ndn/homeID/user/cancel/Alice
Delete user from user registry and broadcast
Data packet: Return acknowledge
/ndn/homeID/user/cancel/Alice/ok(fail)
Data packet: Return acknowledge
/ndn/homeID/user/cancel/Alice/ok(fail)
Data packet: Return acknowledge
/ndn/homeID/user/cancel/Alice/ok(fail)

Fig. 7. MSC of user requests to cancel authority

3 Experimental Results and Performance Evaluation

3.1 Reference [7]'s Access Control Mechanism

In reference [7] the user first needs to send the private key signed Interest packet to the producer to apply for access privilege, and record it in the user registry after the data producer has verified successfully. It is used for intermediate forwarding nodes to generate Bloom Filter to filter Interest packets sent by unauthorized users. Secondly, the producer encrypts the data generated by using symmetric key and encrypts the data key with the public key of each registered user. When the user obtains the data key, he decrypts the data key with his own private key, and then decrypts the data with the data key.

3.2 Index of Performance Testing

This experiment aims at the designed access control mechanism and simulates the whole process using ndnSIM2.4. Performance measurement is the time a user takes from the request for permission to successfully decrypt the data, expressed in terms of $\mathrm{T_{Total}}$, which is computed according to the following formula:

$$\mathrm{T_{Total} = T_{Authority} + T_{DataKey} + T_{Data}} \tag{1}$$

For the access control mechanism proposed in this paper, $\mathrm{T_{Authority}}$, $\mathrm{T_{DataKey}}$ and $\mathrm{T_{Data}}$ are computed according to the following formulas:

$$\mathrm{T_{Authority} = T_{TransformKey} + T_{Response}} \tag{2}$$

$$\mathrm{T_{DataKey} = T_{Response} + T_{Re\_Enc} + T_{Decrypt}} \tag{3}$$

$$\mathrm{T_{Data} = T_{Response} + T_{Decrypt}} \tag{4}$$

Access control mechanisms proposed in reference [7], $T_{\text{Authority}}$, T_{DataKey}, the formula is as follows:

$$T_{\text{Authority}} = T_{\text{Response}} \tag{5}$$

$$T_{\text{DataKey}} = T_{\text{Response}} + T_{\text{Pub\_Enc}} + T_{\text{Decrypt}} \tag{6}$$

The meaning for each time variable in the formula is shown in Table 2:

Table 2. The meaning of the time variable of the formula

Formula symbol	Representative meaning
$T_{\text{Authority}}$	Time of users successfully obtained permission
T_{DataKey}	Time of users successfully obtained data key
T_{Data}	Time of users successfully obtained data
T_{Response}	Time of users successfully obtained data packet
$T_{\text{TransformKey}}$	Time of the permission provider generated the transform key
$T_{\text{Re\_Enc}}$	Re-encryption time
T_{Decrypt}	Time of users successfully decrypted data
$T_{\text{Pub\_Enc}}$	Time of encrypting data key

Experimental Results and Performance Evaluation

Figure 8(a) shows the time with the length of plaintext in different methods. We can see that the time used in re-encryption is not proportional to the length of plaintext. With the increase of plaintext length, the curve tends to be more and more peaceful. In public key encryption algorithm, the time of public key encryption increases with the length of plaintext. When the length of encrypted plaintext is 90 KB, the time of re-encryption is less than the public key encryption algorithm.

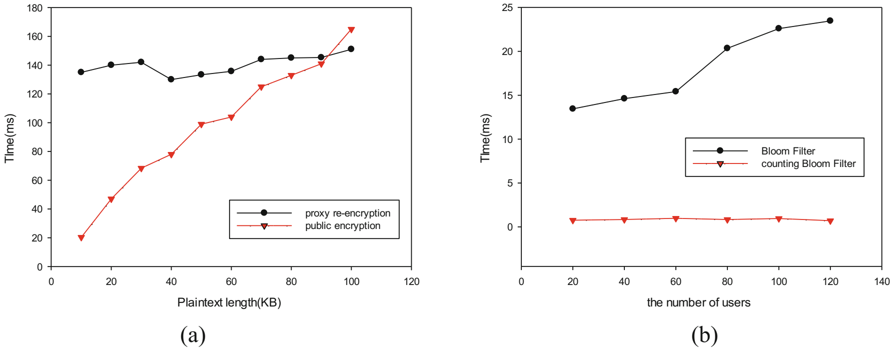
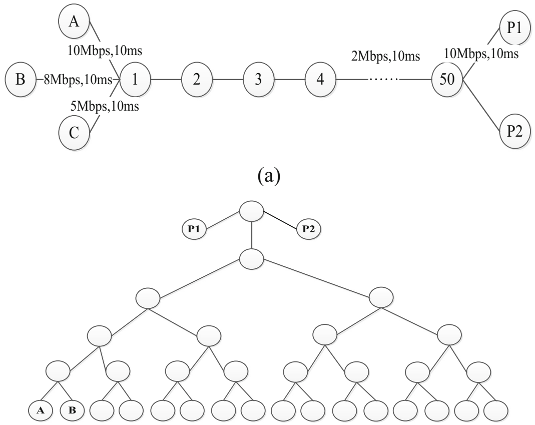


Fig. 8. Comparison between encryption and identity filtering mechanism

As Fig. 8(b) shows the time with different number of users in different methods. As you can see from Fig. 8(b), it takes much longer to regenerate the Bloom Filter than to counting Bloom Filter to perform only delete operations, and it takes more and more time to generate the Bloom Filter as the number of users' increases. The counting Bloom Filter is not affected by the number of users.

Experimental Scene and Simulation Experiment

Figure 9(a) shows the network topology used by the simulation. The topology uses a single link with multiple user sources, with 55 nodes, with three user nodes: Node A, Node B, Node C; a privileges provider: node P1; a data provider: node P2. Node A, node B, node C sends the authority Interest packet to the node P1 in turn. After the user receives the confirmation data packet, user A, user B and user C in turn send the Interest packets requesting the data key and data to P2.



(a)

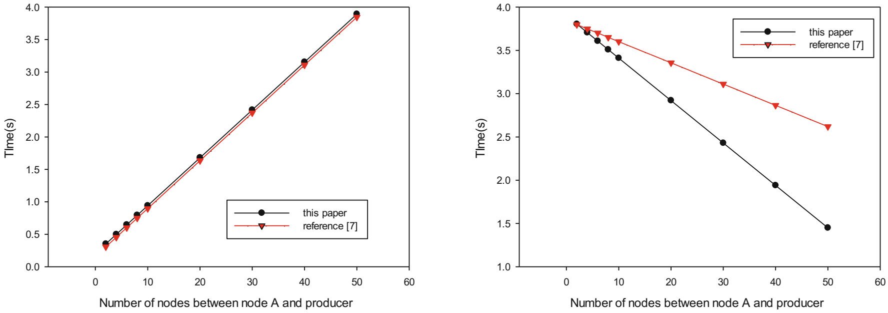
(b)

Fig. 9. Simulation topology structure

Figure 9(b) shows the tree topology used by the simulation. The topology with 34 nodes, with two user nodes: Node A, Node B, a privileges provider: node P1, a data provider: node P2. The T_{Total} of User B is calculated according to user A distance P1 and P2 position (that is, the number of nodes between user A and P1 and P2).

The length of transform key is 256 bit, the data segment size is 4 KB, the data key length is 128 bit, the forwarding route policy is the best route strategy, the cache policy is the least recently used, the packet size is 1024 KB.

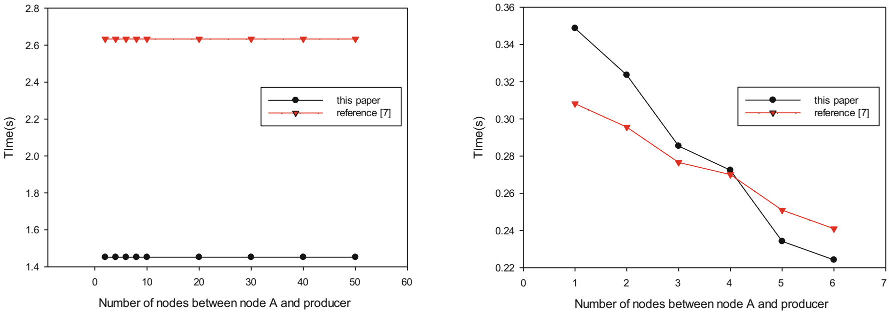
Figure 10(a) shows the T_{Total} of node A. It can be seen that because node A is the node that firstly sends the request Interest packet, the data needed by node A isn't cached in the intermediate nodes, so the Interest packet is returned by node P2. Therefore, we can see that when the cache of intermediate nodes is not used the T_{Total} is slightly higher than that in reference [7], about 14%. Figure 10(b) shows the T_{Total} of node B. As can be seen that because the content of user B request is the same as that of user A request, the intermediate forwarding nodes cache the copy of user A request data. Therefore, user B can retrieve the data in the cache of intermediate nodes, and when node A is two hops from node P2, the T_{Total} is lower than reference [7]. And the longer distance between node A and node P2, the better for user B.



(a) (b)

Fig. 10. T_{Total} for node A and B to get data in the dumbbell topology

Figure 11(a) shows the T_{Total} of node C. It can be seen that node C is affected by the location of node B. The time of node C to make full use of NDN cache is obviously lower than that of reference [7], about 45%.



(a) (b)

Fig. 11. T_{Total} for node C and T_{Total} for node B

Figure 11(b) shows in the tree network topology, the time when user B successfully acquired the data. When user A is four nodes away from node P2, The scheme presented in this paper is lower than that in reference [7] in terms of calculation.

4 Conclusion and Future Work

This paper is mainly to design and implement the access control mechanism of smart home in NDN and design the process from user application permission stage to user logout stage. It can effectively reduce the time from registering permission to successfully decrypting the data, and improve the identity filtering mechanism and user logout mechanism. The following work deploys the proposed access control mechanism in the smart home and tested the performance.

Acknowledgment. This paper is supported by the National Natural Science Foundation of China (Grant No. 61751104) and Natural Science Foundation of Inner Mongolia (Grant No. 2018MS06028) and Research Project of Higher Education School of Inner Mongolia Autonomous Region under Grant NJZY16020.

References

1. Shang, W., Yu, Y., Droms, R., et al.: Challenges in IoT networking via TCP/IP architecture. Technical report NDN-0038. NDN Project (2016)
2. Datta, S.K., Bonnet, C.: Integrating named data networking in Internet of Things architecture. In: IEEE International Conference on Consumer Electronics-Taiwan, pp. 1–2. IEEE (2016)
3. Sandhu, R.S., Samarati, P.: Access control: principle and practice. IEEE Commun. Mag. **32** (9), 40–48 (1994)
4. Zhang, L., Estrin, D., Burke, J., et al.: Named data networking (NDN) project. Technical report NDN-0001, 157–158 (2010)
5. Zhang, Z., Yu, Y., Afanasyev, A., et al.: NAC: name-based access control in named data networking. In: 4th ACM Conference on Information-Centric Networking on Proceedings, pp. 186–187. ACM (2017)
6. Chaabane, A., De Cristofaro, E., Kaafar, M.A., et al.: Privacy in content-oriented networking: threats and countermeasures. ACM SIGCOMM Comput. Commun. Rev. **43** (3), 25–33 (2013)
7. Chen, T., Lei, K., Xu, K.: An encryption and probability based access control model for named data networking. In: Performance Computing and Communications Conference, pp. 1–8. IEEE (2014)
8. Hamdane, B., Serhrouchni, A., El Fatmi, S.G.: Access control enforcement in named data networking. In: 8th International Conference for Internet Technology and Secured Transactions, pp. 576–581. IEEE (2013)
9. Qiao, Z., Liang, S., Davis, S., Jiang, H.: Survey of attribute based encryption. In: International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, pp. 1–6. IEEE (2014)
10. Wood, C.A., Uzun, E.: Flexible end-to-end content security in CCN. In: 11th Consumer Communications and Networking Conference, pp. 858–865. IEEE (2014)