A Congestion Control Mechanism based on Identity Authentication for Named Data Networking

Yi Zhu, Qiang Luo, Yu Tao, Ruilan Huang

Abstract—**Congestion Control is a critical issue of Named Data Networking (NDN). Facing limited link resources, how to guarantee the QoS of the authorized user is puzzling NDN researchers. By introducing the idea of Access Class Barring, this paper designs a congestion control mechanism based on identity authentication (IACCM). In IACCM, a signature is added to the interest packet for router to distinguish the identity of requester. When network suffers congestion, the router will restrict the unauthorized user to access the congestion link, and protect the authorized user against congestion. To avoid managing too many users' public keys in the router when the scale of requesters is massive, IACCM generates the signature using the re-encryption technology. Under this design, the router only needs save one public key of the network service provider. The simulation results show that IACCM can effectively defend congestion for the authorized users and it has good dynamic adaptability, but this improvement is based on the performance sacrifice of the unauthorized users.**

Index Terms—**Named data networking, Congestion control, Identity Authentication, Re-encryption, Quality of Service**

I. Introduction

NAMED Data Networking (NDN) is a typical representative of the next generation Internet architecture[1][2], which builds a new name-based addressing mode regardless of where the content comes from. Combing with the in-network caching mechanism, NDN gains obvious advantages in content distribution and mobility support[3]. Although NDN solves some difficulties of traditional IP architecture, it is still facing several challenges, including congestion control, named routing optimization and privacy risk, etc.

Congestion control is an important topic in NDN research field, the multi-sources feature of NDN makes it become complex. On one side, multi-sources transmission potentially sharpens the congestion phenomenon. On the other side, multiple possible content sources lead that the RTT(Round-Trip Time) cannot be accurately measured. Lacking the believable RTT value, most of the congestion control mechanisms used in IP architecture are no longer applied in NDN[4]. Aiming at this problem, existing major solutions are designed from two aspects, one is that of adjusting the sending windows of interest packet, another is that of optimizing the routing to balance the forward traffic[5]. Although these solutions can partially alleviate in-network congestion, how to effectively guarantee the QoS (Quality of Service) of requester under the limited transmission resource is still puzzling NDN researchers.

Recently, access control has been emerged as a new approach of congestion control, whose typical representative is Access Class Barring (ACB)[6]. In ACB, requesters are divided into different priorities, while the priority information is attached to the request message. When the network suffers congestion, the router admits the arrival flow with different level probability according to the priority of its requester. This design can guarantee the QoS of high-priority requesters through accessing control. For most Internet services, users with specific identities (such as paying/authorized users) should have priority access to the network and get better online experience[7]. Meanwhile, the authorized users are also immune from congestion under ABC method.

Based on the idea of ACB, this paper proposes an Identity Authentication based Congestion Control Mechanism for Named Data Networks (named as IACCM in short). In IACCM, the authorized user can obtain a digital certificate from its network service provider (NSP). Using the information of this certificate and re-encryption technology, a signature is generated and inserted into the interest packet sending by the authorized user. Once the network congestion occurs, routers will verify the signature to distinguish the identity of requesters and then control the access traffic. By refusing the unauthorized user to access the congestion link, the authorized user can remain normal QoS from the network congestion.

The rest of this paper is organized as follows. Section II discusses the research status of congestion control in NDN. Section III is devoted to the design of IACCM. Section IV evaluates the performance of IACCM with ndnSIM. Finally, we conclude the paper and future works in Section V.

II. CONGESTION CONTROL IN NDN

Focusing on the congestion problem in NDN, most of current solutions are inherited from the window-based mechanism of TCP/IP[8]. A typical scheme named Explicit Control Protocol (ECP) was proposed by Y Ren et al.[9]. which adjusts the sending rate of interest packet in the receiver side according to the congestion level feedbacking by the routers. Otherwise, an improved Explicit Congestion Control Algorithm was proposed by S Xing[10], in this algorithm, intermediate router computes a "load factor" which indicates the level of network congestion by detecting the Data queue length of each interface, then the client can actively adjust its request-sending rate according to the "load factor" carried by data package. Mejri[11] et al. proposed a hop-to-top

Yi Zhu is with Jiangsu Key Laboratory of Security Tech. for Industrial Cyberspace, School of Computer Science and Communication Engineering, Jiangsu University, Zhen Jiang, China. e-mail: (zhuyi@ujs.edu.cn).

Qiang Luo, Yu Tao and Ruilan Huang are with School of Computer Science and Communication Engineering, Jiangsu University, Zhen Jiang, China.

congestion control mechanism by monitoring the output queue length of each router, then notify the downstream routers to adjust their sending rates. Although the aforementioned solutions can alleviate the congestion state by reducing the arrival traffic of bottleneck link, the method of undifferentiated limitation of sending rate seriously degrades the QoS of authorized user.

Another way to solve congestion is to optimate the forwarding strategy. In literature[12], a case for stateful forwarding plane (ASFP) was given. By ranking the interface status according to the congestion information from upstream routers, the router selects an interface with best working status to forward interest. Abdelkader et al[13]. proposed a new mechanism called Parallel Multi-Path Forwarding Strategy (PMP-FS). Considering the features of in-network caching and interest packets aggregation in NDN, the PMP-FS actively splits traffic into multiple routes to optimize the network throughput while avoiding congestion. Carofiglio et al.[14] further introduced a dynamic forwarding strategy, by setting up a receiver-driven multipath controller, to monitor the network status with congestion window and each path delay, and then dynamically select the best forwarding path. The way of dynamic forwarding can effectively optimize the network congestion. However, under the situation of limited link resources, it still cannot guarantee the QoS of authorized user.

Nowadays, access control has gradually become a significant solution of congestion control in network research. Argoubi S et al.[15] suggested a QoS-based scheme for wireless sensor network. This scheme divides the network traffic into different priority level. Using the scheduling mechanism of earliest deadline first, the urgent traffic will be first served. Nawel et al.[16] oriented to the M2M scenario and introduced a multi-ACB (MACB) algorithm. According to the priority of devices, this algorithm ensures the QoS of the device with high priority by implementing access control using different ACB factors. For current NDN researches, access control is mainly used to solve the network security problems. For example, Zhi al.[17] proposed an interest flow control method, in which, the router limits the requests from malicious users by recognizing the malicious interest prefix. Although this method is used to against in-network malicious attacks, it also reduces the access traffic and alleviates the network congestion indirectly.

III. IACCM: IDENTITY AUTHENTICATION BASED CONGESTION CONTROL MECHANISM

The congestion control mechanism named IACCM proposed by us is motived by ACB idea. In IACCM, the interest packet sending by authorized user is embedded a digital signature, which is used to indicate the identity of requester. When network suffers congestion, the router will control the access traffic according to the results of verifying the signature. Considering that the routine signature method always uses private key of user to generate signature, and uses public key of user for verification. If following this way, every router needs to store the public keys of all authorized users. As show in Fig.1, there are three authorized users in this scenario and access routers should store three public keys to check the permission of received interest packets. It is unrealistic when the number of authorized users is massive.

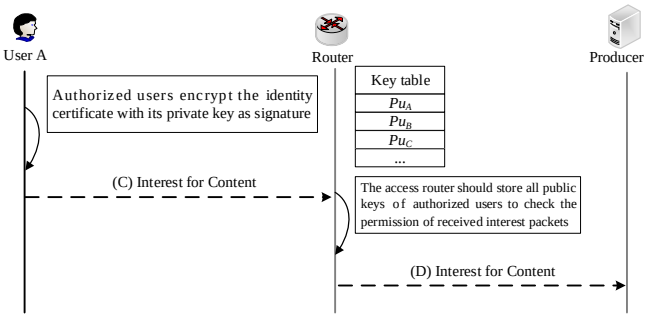

Fig. 1: Traditional signature technology

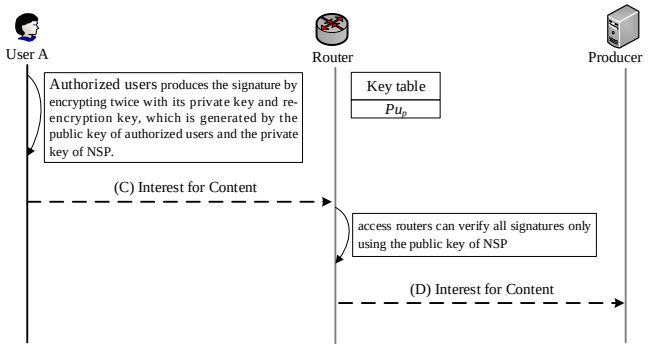

Fig. 2: Re-encryption technology

To improve the feasibility of access control by signing in interest packet, IACCM adopts the re-encryption technology to generate signature. With the private key of user and the re-encryption assigned from NSP, the authorized user produces the signature by encrypting twice. Then access routers can verify all signatures only using the public key of NSP. As shown in Fig.2, although there are still three authorized users existing in the scenario, the router only needs to store one public key for verification. This design solves the storage cost problem of router under the realistic network scenario.

A. Parameter settings

The detailed design of IACCM is depended on the following settings[18].

1) To generate the public/private key pairs, the public environment parameters can be expressed as $param = \{H_0, H_1, SE\}$, where H_0 is a one-way hash function, $H_0 : \{0,1\}^l \rightarrow G$ (l is a positive integer), H_1 is a XOR operation function, $H_1(M,N) = H_0(M) \oplus H_0(N)$, SE is a secure symmetric encryption algorithm.
2) Based on the public parameters, users and NSP generate their public/private key pairs independently. We define (Pu_A, Pk_A) as the public/private key pair of user A, which can be calculated with $Pu_A = H_0(ID_A)$, $Pk_A = H_0(ID_A) \oplus H_0(s)$, where $s \in Z_p^*$ is a random number, ID_A is user's identification. Similarly, the public/private key pair of NSP is defined as (Pu_p, Pk_p), where $Pu_p = H_0(ID_p)$, $Pk_p = H_0(ID_p) \oplus H_0(q)$ and ID_P is the identification of NSP and $q \in Z_p^*$ is a random number. For implementing IACCM, Pu_p will be pre-deployed in each router.

B. Detailed design of IACCM

IACCM is consist of three parts: permission application, identity verification and traffic access control.

1) Permission Application: If user A want to be an authorized user, he/she must submit an application to NSP and wait for assigning the permission, the detailed application process as shown in Fig.3.

User Side: User A sends an interest packet including his/her public key Pu_A to NSP.

NSP side: After receiving this application, NSP check the identity of requester according to the information in application layer. Next, NSP generates a re-encryption key (identity credential) R_key_A for user A, where $R\_key\_A = Pk_p \oplus Pu_A$. That means the re-encryption key assigned to user A is determined by the private key of NSP and public key of user. Then R_key_A is encapsulated as a digital certificate and then return to user A. The user owning this digital certificate has the special permission to access network.

2) Signature and Verification:

User side: The authorized user A uses his/her username $NAME_A$, private key Pk_A, re-encryption key R_key_A and public parameters $\{H_0, H_1, SE\}$ to generate the signature $R\_Enc\_m = (C_1, C_2, U_{R\_en})$ according to formula group (1).

$$\begin{cases} H\_NAME_A = hash(NAME_A) \\ m = H_1(H\_NAME_A, k) \\ C_1 = SE_{H_0(k)\oplus H_0(s)}(H\_NAME_A) \\ C_2 = m \oplus H_0(s) \\ U_{en} = H_0(k) \oplus Pk_A \\ U_{R\_en} = U_{en} \oplus R\_key\_A \end{cases} \tag{1}$$

$$\Rightarrow R\_Enc\_m = (C_1, C_2, U_{R\_en})$$

where, H_NAME_A is the hash value of username, $k \in Z_p^*$ is a random number selected by user A, $H_0(k)$ is the symmetric key of algorithm SE, C_1 is the ciphertext of H_NAME_A encrypted by $H_0(k)$, U_{en} is the ciphertext of $H_0(k)$ encrypted by the private key of user A, U_{R_en} is the second encryption output using the re-encryption key from the certificate, C_2 is used to hiding k for verification.

Obviously, R_Enc_m is a one-time signature. When an interest packet sending from user A, R_Enc_m will be dynamically generated by randomly selecting a number k. Then R_Enc_m and username $NAME_A$ are inserted into the interest packet and sent to the network.

Router side: If the network is in the predicament of congestion, the routers will verify the signature of received interest packets and distinguish the authorized users. First, the symmetric key can be decrypted from U_{R_en} using the public key of NSP, calculated as $H_0(k) \oplus H_0(s) = [U_{R\_en} \oplus H_0(q) \oplus Pu_p]$. Next, H_NAME_A is restored by decrypting C_1 through the formula $H\_NAME_A = SE_{H_0(k)\oplus H_0(s)}(C_1)$. Based on H_NAME_A and $H_0(k) \oplus H_0(s)$, the router verifies whether $H_1(H\_NAME_A, k) \oplus H_0(s)$ is equal to C_2 or not. If true, the router further extracts the username D_NAME_A from received interest packet, and then compares $hash(D\_NAME_A)$ with H_NAME_A. If two hash values are same, the router determines the requester is an authorized user. Otherwise the requester will be judged as an unauthorized user.

The reason we encrypt the symmetric key twice in the signature stage is to avoid of storing too many public keys of users in the router. By adopting re-encryption, the router only needs to store one public key of NSP and effectively reduces the storage and management cost. It is the key improvement

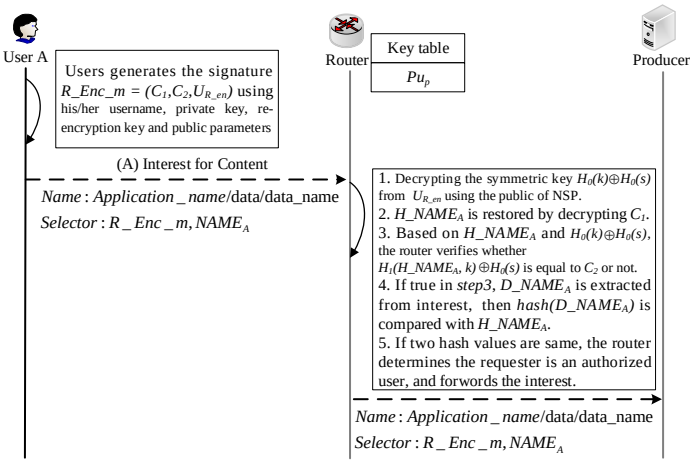

Fig. 3: Process of permission application

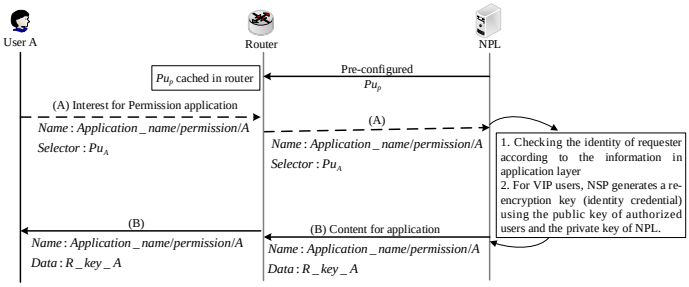

Fig. 4: User identity verification

of IACCM. Fig.4 clearly gives the entire interaction between user and router.

3) Traffic Access Control: Based on the identification results, the router can implement the traffic access control according to link state. To detect the congestion level, we adopt a scheme proposed by literature[9], In this scheme, the output queue length of an interface will be measured n times within a period T, and each measurement result is recorded as $0 < i \leq n$. Due to the credibility of Q_i gradually increases with the measurement time approaches to present, a monotonic increasing weight $W_i (0 < i \leq n)$ is defined to indicate the corresponding credibility of Q_i. In the end of period T, the congestion level of each interface will be given, which is calculated by $Q_T = \sum_{i=1}^{n} Q_i W_i$.

Next, as shown in Algorithm 1, the router classifies the link status into three level by introducing two thresholds Q_{free} and Q_{busy}, and then further adjusts the traffic of congestion link, where $0 < Q_{free} < Q_{busy} \leq Q_{\max}$, $Q_{\max}$ is the maximum length of output queue.

1) If $Q_T \leq Q_{free}$, there is no congestion occurred in the link. That means the link bandwidth is enough to satisfy all users' requirements. Under this situation, the router ignores the signature inside the interest packet and executes normal processing.
2) If $Q_{free} < Q_T < Q_{busy}$, there is mild congestion occurred in the link. To deal with it, the router verifies the signature to distinguish the identity of requester, then implements different accessing mechanisms to different requesters. For the authorized users, they have the privilege of accessing the congestion link normally. For the unauthorized users, they only access

Algorithm 1 IACCM access control algorithm

function $PARAINITIAL()$
  Initialization of Q_{free}, Q_{busy}, p
end function
function $CONGESCONTROL()$
  while $Receivedaninterest$ **do**
    if $Q_T < Q_{free}$ **then**
      $ACCCONTROL(free)$
    end if
    if $Q_{free} \leq Q_T < Q_{busy}$ **then**
      $ACCCONTROL(busy)$
    end if
    if $Q_T \geq Q_{busy}$ **then**
      $ACCCONTROL(congestion)$
    end if
  end while
end function
function $ACCCONTROL(state)$
  switch $state$ **do**
    case $Free$
      All interests are forwarded
    case $Busy$
      Interests of authorized users are directly forwarded, but forwarded with probability for unauthorized users
    case $Congestion$
      Interests of unauthorized users are denied to access, but interests of authorized users are directly forwarded
end function

the congestion link with probability p, where p is determined by the formula (2).

$$p = \begin{cases} 1 & Q_T \leq Q_{free} \\ 1 - \frac{Q_T - Q_{free}}{Q_{busy} - Q_{free}} & Q_{free} < Q_T < Q_{busy} \\ 0 & Q_T \geq Q_{free} \end{cases} \quad (2)$$

3) If $Q_T \geq Q_{busy}$, that means the link is suffering serious congestion. To guarantee the QoS of the authorized users, the router will decline the interest packets from unauthorized users to access the congestion link. Meanwhile, the interest packets from authorized users still normally forward through the congestion link.

IV. PERFORMANCE EVALUATION

A. Simulation conditions

In this section, we evaluate the performance of IACCM comparing with no congestion control and ASFP[12], a forwarding strategy of congestion control. The simulation tool is ndnSIM[19] which is runs on a high-performance computing platform with Intel(R)Xeon CPU E7-4830, 256GB memory and CentOS 6.5 system[20]. The topology used in simulation is shown in Fig.5.

According to the literature[9][20], we set the following simulation conditions.

1) There are two users groups in this scenario, where Group A represents the authorized users and Group B represents the unauthorized users. The authorized users only request contents from producer $P1$, the unauthorized users can request contents from producer $P1$ or $P2$. In our simulation, the number of users in each group will be changed according to the experiment conditions.

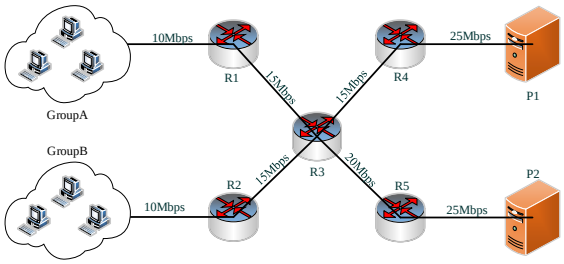

Fig. 5: Simulation topology

2) The bandwidth between neighbor nodes is annotated in Fig.5, and the fundamental transmission delay of each link is set as 10ms. To simulate the network congestion, we set a narrow bandwidth (15Mbps) between $R3$ and $R4$, and there will be the bottleneck in this topology.
3) The content files provided by producer are classified into 100 classes by popularity of Zipf distribution with parameter 0.7, each class has 100 files, and the average size of each file is 40 kbit.
4) The router adopts the Least Recently Used(LRU) policy for cache replacement. The cache size of each router is same, set as 1/20 of the total amount of content files. And the maximum output queue length of router is 100.
5) Both authorized and unauthorized user sends interest packets according to Poisson process with intensity 100 interest/sec. The size of interest packet is 40 bit and the size of data packet is 40kbit.
6) For generating signature, the $MD5$ digest algorithm and $AES-128$ symmetric encryption algorithm are used.
7) To detect congestion in simulation, two thresholds of IACCM are configured as $Q_{free} = \frac{1}{3}Q_{\max}$, $Q_{busy} = Q_{\max}$.
8) The running time of each experiment is 45 simulation seconds. During the experiment, the authorized users send requests from begin to end, but the requests from unauthorized users start at 10s and end at 35s.

B. Comparison of the performance between IACCM and ASFP

In this experiment, we set that Group A has three authorized users and Group B has three unauthorized users. To disclose the QoE (Quality of Experience) of authorized user and unauthorized user under congestion, we evaluate the network performance from three aspects: average interest satisfaction rate, average interest retransmission rate and average round-trip delay. According to aforementioned settings, the link between R3 and R4 will fall into congestion from 10s after the beginning of simulation.

1) Fig.6 shows the average interest satisfaction rate of three mechanisms. During the first 10s of the simulation, due to the unauthorized users don't access, no congestion occurs, and the three mechanisms achieve

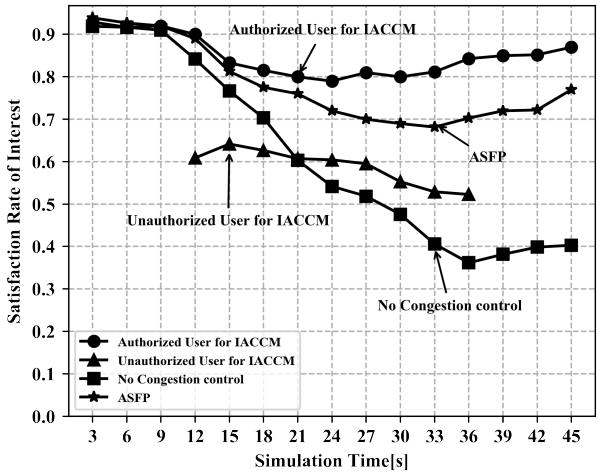

Fig. 6: Average satisfaction rate of interest

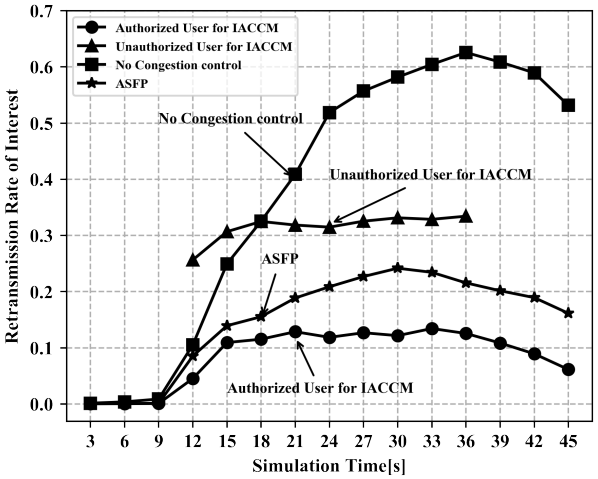

Fig. 7: Average retransmission rate of interest

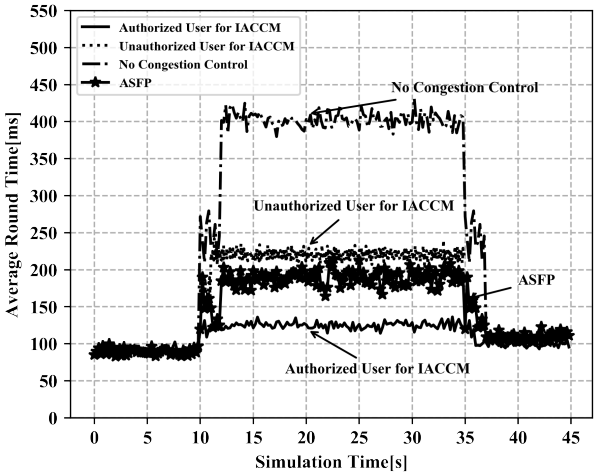

Fig. 8: Average round trip time

the same interest satisfaction rate about 90%. After 10s, congestion occurs in the link between R3 and R4 with the coming traffic from the unauthorized users. Consequently, the interest satisfaction rate under no congestion control begins to drop continuously, from 90% to 35%, until the unauthorized users stop their requests. For ASFP, although it is also affected by congestion, its performance degradation is relative low. As seen from the figure, the average interest satisfaction rate of ASFP is at least 70%. The reason is that the ASFP has inherent mechanism to defend congestion by selecting the forwarding interface with low congestion status. For the authorized users of IACCM, they only suffer slight influence from congestion due to the access privilege, and their interest satisfaction rate is more than 80% overall, which is more than twice that of the non-congestion control mechanism. But for the unauthorized users of IACCM under this simulation settings, the router will totally reject their interest packets to access the congestion link, so the events of dropping data packets become frequently for them. An interesting thing is the performance of the unauthorized user of IACCM is better than no congestion control, this phenomenon discloses that the direct rejection will accelerate the speed of resending request, it is superior than inanely waiting in the output queue until time out.

2) As seen from Fig.7, the variable law of interest retransmission rate is in the opposite of interest satisfaction rate. For no congestion control, the interest retransmission rate increases rapidly, and it reaches 65% at 36s. With ASFP, although it can partially defend the congestion, it also reaches 25% at the worst. For IACCM, it protects the rights of the authorized users and sacrifices the rights of the unauthorized users. So, the interest retransmission rate of the authorized users keeps about 10% under congestion, but the unauthorized users must face the interest retransmission events with probability about 30%.
3) Fig.8 further discloses the average RTT for three mechanisms. Similarly, the authorized users under IACCM achieve the best performance, the ASFP obtains the suboptimal performance, and the users without any congestion protection only complain the terrible network.

Overall, ASFP improves the network performance by adjusting the forwarding path, but it forwards interest packets without regard to requester's identity, so the authorized users only experience the same network service as the unauthorized users. But for IACCM, its design makes the authorized users to avoid the disturbing of congestion.

C. The effect of the number of unauthorized users

To analyze the impact of the number of unauthorized users under IACCM, we design two experiments in this section. In the first experiment, we assume that Group A and Group B still has three authorized users and three unauthorized users respectively. But in the second experiment, the number of Group B increases to six.

1) Fig.9 shows the average RTT of two experiments. Obviously, after 10s, when more unauthorized users access, the network performance becomes worse. For authorized users, the effect they suffered is slight, the RTT only increases from 120ms to 150ms. But for unauthorized users, the network status is terrible, the RTT reaches 310ms. It is shown that more unauthorized users will exacerbate network congestion. But

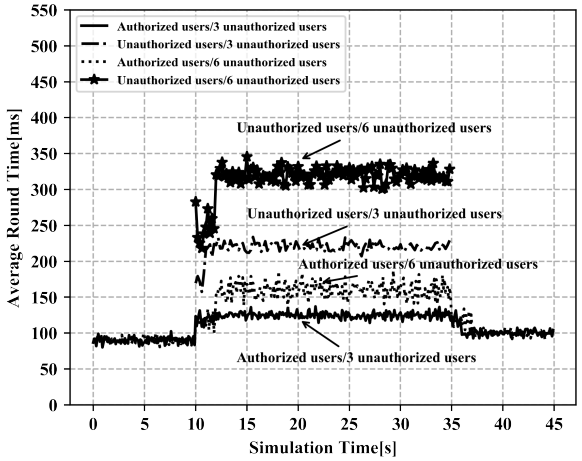

Fig. 9: Average round trip time under 3 and 6 unauthorized users

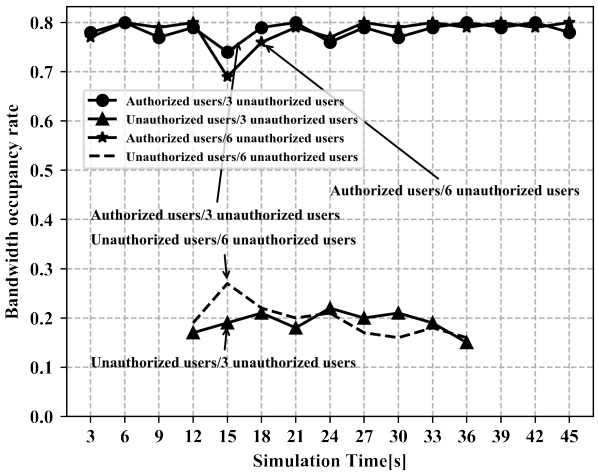

Fig. 10: Bandwidth occupancy of users under 3 and 6 unauthorized users

due to IACCM can protect the VIP users, the impact on the users of Group A can be accepted.

2) As seen from Fig.10, during the simulation period, bandwidth occupancy of authorized users only change a little when the number of unauthorized users increases, and the ratio of bandwidth occupancy between authorized and unauthorized users remains around 4:1. Although after 10s, the delay of the authorized users shows slightly degradation, but it can cover about 80% link bandwidth, and keep effective utilization of link resources.

In order to further evaluate the adaptability of IACCM with different congestion levels, we compare the performance of IACCM and ASFP from the aspect of congestion processing time. In the simulation experiment, we change the number of unauthorized users in group B to make the network working in different congestion levels. The comparison results are shown in Fig.11, we can see that the congestion processing time of IACCM also increases when network faces severe congestion. But this increament is very slight. Comparing with ASFP, the time cost of IACCM is significantly shorter.

From above results, it is proven that the design of IACCM can provide powerful robustness for the VIP group. Moreover, IACCM can quickly response different congestion levels and recover the operation of the network.

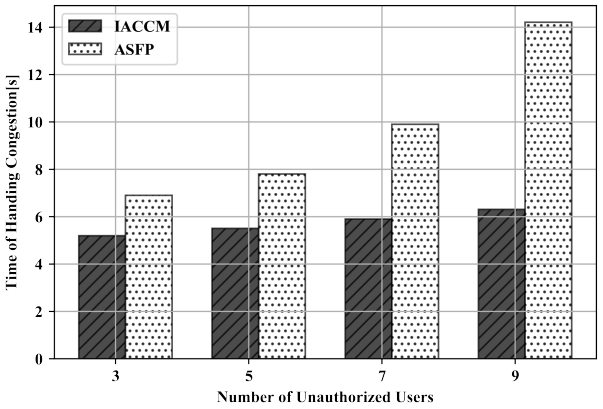

Fig. 11: Congestion processing time of IACCM and ASFP under different congestion levels

V. CONCLUSION

Aiming at the problem of network congestion in NDN, this paper proposes an Identity Authentication based Congestion Control Mechanism. In this mechanism, a signature method of interest packet is suggested for verifying the identity of requester. Based on this design, the routers can distinguish the authorized users and then guarantee the QoS of them by implementing access control when the network occurs congestion. To make the signature mechanism practically, we design the re-encryption technology to generate signature. The simulation results show that the IACCM can effectively protects the authorized users against the influence of congestion than ASFP. But this improvement is based on the performance sacrifice of the unauthorized users. But beyond that, IACCM can also maintain relatively stable network performance and strong stability in case of environmental degradation.

In this work, we only consider the authority assigned by NSP. But for real network, different Internet service will assign different authority for users. How to design access control with more precise identification is our future work.

REFERENCES

[1] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. Braynard, "Networking named content," *Proc Acm Conext*, vol. 55, no. 1, pp. 1–12, 2009.

[2] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, K. Claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *Acm Sigcomm Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[3] M. Hussaini and R. Mustapha, "A conceptual model of producer mobility support for named data networking using design research methodology," *IAENG International Journal of Computer Science*, vol. 46, pp. 552–563, 11 2019.

[4] D. Saucez, L. A. Grieco, and C. Barakat, "Aimd and ccn: past and novel acronyms working together in the future internet," ser. Proceedings of the 2012 ACM workshop on Capacity sharing, 2012, pp. 21–26.

[5] Y. Ren, J. Li, S. Shi, L. Li, G. Wang, and B. Zhang, "Congestion control in named data networking - a survey," *Computer Communications*, vol. 86, pp. 1–11, 2016.

[6] A. Kunz, I. Tanaka, and S. S. Husain, "Disaster response in 3gpp mobile networks," ser. 2013 IEEE International Conference on Communications Workshops (ICC), 2013, pp. 1226–1231.

[7] Z. Kaleem and K. H. Chang, "Qos priority-based coordinated scheduling and hybrid spectrum access for femtocells in dense cooperative 5g cellular networks," *Transactions on Emerging Telecommunications Technologies*, vol. 29, no. 1, pp. 1–14, 2018.

[8] X. Yang, "Receiver-driven congestion control for streaming video application." ser. Lecture Notes in Engineering and Computer Science, 2007, pp. 1271–1275.

[9] Y. Ren, J. Li, S. Shi, L. Li, and G. Wang, "An explicit congestion control algorithm for named data networking," ser. 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2016, pp. 294–299.

[10] S. Xing, B. Yin, J. Yao, H. Zhang, Q. Zhai, and H. Shi, "A vcp-based congestion control algorithm in named data networking," ser. 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). IEEE, 2018, pp. 463–468.

[11] S. Mejri, H. Touati, N. Malouch, and F. Kamoun, "Hop-by-hop congestion control for named data networks," ser. 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), 2017, pp. 114–119.

[12] C. Yi, A. Afanasyev, I. Moiseenko, L. Wang, B. Zhang, and L. Zhang, "A case for stateful forwarding plane," *Computer Communications*, vol. 36, no. 7, pp. 779–791, 2013.

[13] A. Bouacherine, M. R. Senouci, and B. Merabti, "Parallel multi-path forwarding strategy for named data networking," ser. Proceedings of the 13th International Joint Conference on e-Business and Telecommunications, vol. 1, 2016, pp. 36–46.

[14] G. Carofiglio, M. Gallo, and L. Muscariello, "Optimal multipath congestion control and request forwarding in information-centric networks: Protocol design and experimentation," *Computer Networks*, vol. 110, pp. 104–117, 2016.

[15] S. Argoubi, K. Maalaoui, M. H. Elhdhili, and L. A. Saidane, "Priority-mac: A priority based medium access control solution with qos for wsn," ser. 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016, pp. 1–6.

[16] N. Zangar, S. Gharbi, and M. Abdennebi, "Service differentiation strategy based on macb factor for m2m communications in lte-a networks," ser. 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2016, pp. 693–698.

[17] T. Zhi, H. Luo, and Y. Liu, "A gini impurity-based interest flooding attack defence mechanism in ndn," *IEEE Communications Letters*, vol. 22, no. 3, pp. 538–541, 2018.

[18] C.-I. Fan, I.-T. Chen, C.-K. Cheng, J.-J. Huang, and W.-T. Chen, "Ftp-ndn: File transfer protocol based on re-encryption for named data network supporting nondesignated receivers," *IEEE Systems Journal*, vol. 12, no. 1, pp. 473–484, 2016.

[19] S. Mastorakis, A. Afanasyev, and L. Zhang, "On the evolution of ndnsim: An open-source simulator for ndn experimentation," *ACM SIGCOMM Computer Communication Review*, vol. 47, no. 3, pp. 19–33, 2017.

[20] Y. Zhu, R. Huang, Y. Tao, and X. Wang, "An edge re-encryption-based access control mechanism in ndn," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 6, pp. 1–13, 2019.