DESIGN AND IMPLEMENTATION OF THE EFFICIENT AND SECURE CONTENT DISTRIBUTION SCHEME IN NAMED DATA NETWORKING

GRADUATE SCHOOL OF NATURAL SCIENCE & TECHNOLOGY

DIVISION OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE

INFORMATION SECURITY LAB

HTET HTET HLAING

Abstract

NDN is one of the new emerging and promising Future Internet Architectures that alternates from the current host-based communication approach of TCP/IP architecture to a content-centric communication model. NDN brings up new solutions over today's internet architecture, facilitating content distribution, in-network caching, mobility support, and multicast forwarding. NDN's ubiquitous in-network caching allows data to be cached by intermediate routers so the consumers can access data directly from the cache. However, it opens content privacy problems since data packets replicated in the router are always accessible by every consumer. Sensitive and confidential data should be protected before being distributed to the network and accessed only by authorized consumers. Although the content protection problem can be solved by applying an encryption-based access control policy, it still needs an efficient content distribution scheme with lower computational overhead and content retrieval time. We propose an efficient and secure content distribution (ES_CD), by combining symmetric encryption and identity-based proxy re-encryption. ES_CD achieves content confidentiality, faster content retrieval time for cached contents, and slight computational overhead while leveraging NDN features. Our scheme ensures that only legitimate consumers can access the contents during a predefined time without a trusted third party and an always online content producer.

DESIGN AND IMPLEMENTATION OF THE EFFICIENT AND SECURE CONTENT DISTRIBUTION SCHEME IN NAMED DATA NETWORKING

With the growing number of Internet usage and content distribution services on today's Internet, researchers proposed a better way to distribute the content using the name instead of using the address or location. Consequently, Information-Centric Networking (ICN) becomes the ultimate Future Internet Architecture to replace the host-centric TCP/IP architecture with content-based architecture. NDN is one of the dominant candidates in the ICN architecture in which contents become the priority elements to address the current Internet architecture limitations. Data access control turns out to be even more problematic since the cached contents are widely available at the intermediate routers, and a malicious consumer can easily access the cached contents from the cache and attempt unauthorized decryption without the content producer's permission. Hence, this dissertation aims to design and implement an efficient and secure content distribution solution (ES_CD) for NDN architecture, which provides content confidentiality by encryption and a limited access time for each consumer.

In our implementation, the original content is securely encrypted with a randomly selected symmetric key at the content producer. The corresponding symmetric key k is then encrypted with IB-PRE, which is implemented using the parameters from Type A pairing with the group order 224-bit on a *secp224k1*elliptic curve. We set up a compact NDN environment with one content producer, one consumer, one intermediate router, and one edge router to evaluate the computational overhead of our system. The consumer requests for a 2KB content file to the content producer by sending the interest request as /netflix/movie/001. Then the content producer performs content encryption, corresponding key encryption, and re-encryption key generation and append all the keys along with the encrypted data and returns to the consumer in a data packet as /netflix/movie/001/enc_data/enc_key/RK/. The edge route first extracts /enc_key/RK/ part from the data packet to perform re-encryption. It re-appends to the data packet as /netflix/movie/001/enc_data/reenc_key/ and forwards to the consumer. Finally, the consumers can get the symmetric key by decrypting the re-encrypted key, and then the requested content can be recovered.

We execute the simulation by running it 30 times repeatedly by requesting the same file size by the consumer. Then, we measure the total time complexity from the same simulation for content encryption and decryption operations at the content producer, and the consumer side starts from the content request until decryption of the original content. After a number of executions, the overall time becomes linear as the number of implementation executions for the same size content as plotted in Figure.1.

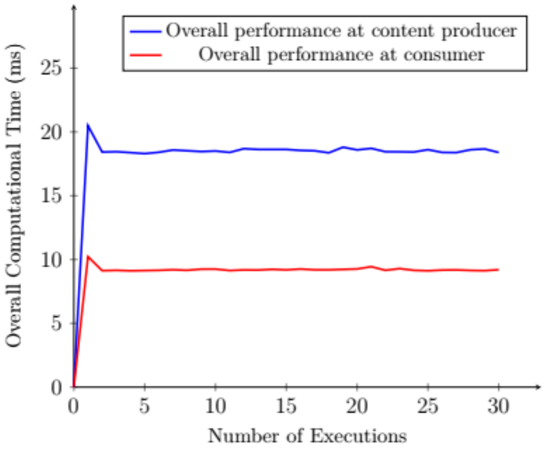
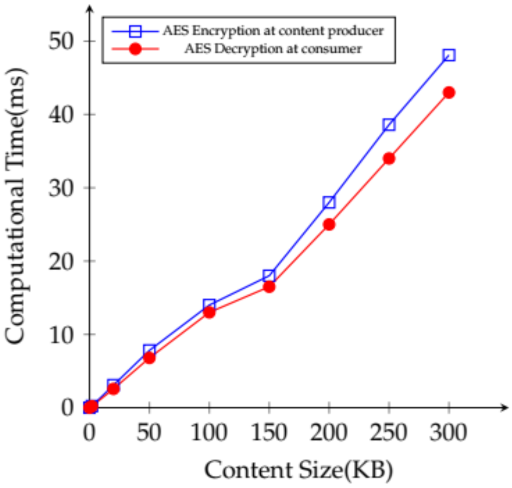


Figure 1. Average overall computational time for retrieving 2KB content.

We conduct another simulation with different file size where the results were statistically significant that AES performance time increase with respect to the content file sizes, which is illustrated in Figure.2. We also measure the overall cryptographic time with different file sizes at the content producer and the consumer in Figure.3.



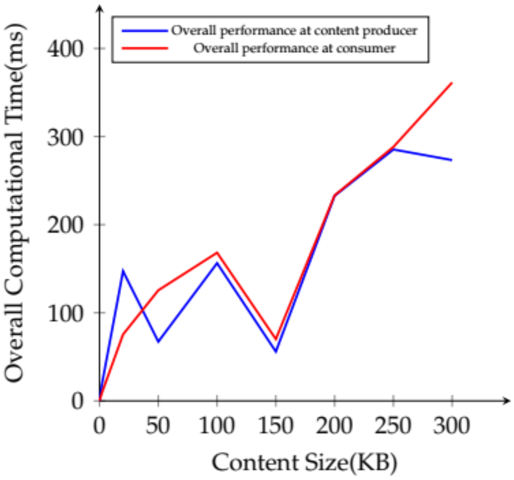


Figure 2. Average computational time for AES operations with different file sizes.

Figure 3. Overall computational time for different file sizes

When revocation occurs, we do not need to re-encrypt and re-publish the entire content, and it only needs to perform the content decryption key re-encryption at the edge router at an acceptable cost and lower communication overhead in NDN environment. For the first request with no cache in the router, a consumer needs to obtain both encrypted content and encrypted key directly from the content producer, and it may take more time on the content retrieval.

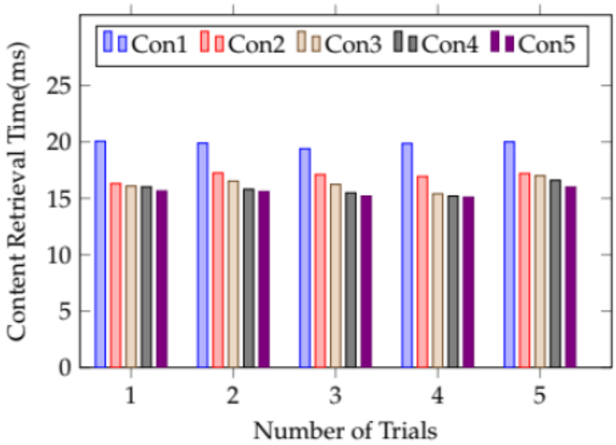


Figure 4. Content retrieval delay for different number of consumers with different id

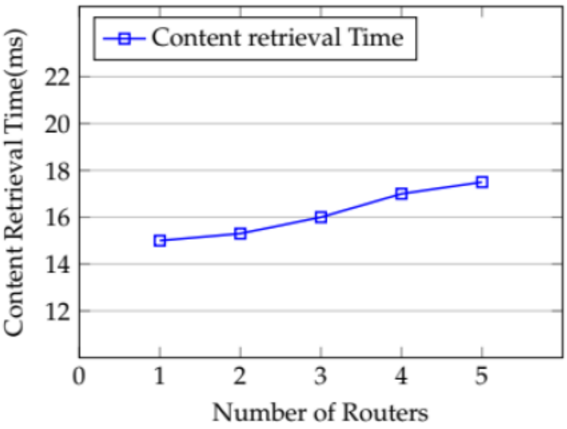


Figure 5. Content retrieval delay for n-number of routers

We simulate numbers of executions and compare the content retrieval time for both fresh and cached content for different consumers which perform successive requests in Figure.4. The comparison reveals that it can reduce the content retrieval time for cached content by 10% to 25% on average in total. Finally, we measure the effects of adding many routers in our simulation scenario to highlight the impact of communication overhead on the consumer to retrieve the content. As shown in Figure.5, we can clearly see that the content retrieval time for the consumer slightly increases with the number of routers in the network. The consumer needs to pass through *n* numbers of routers to register at the content producer, requests the content and retrieves the content.

Additionally, we compare ES_CS with other related encryption-based access control schemes and implement the most relevant scheme. These additional experimental results show that our proposed system offers a lower computational overhead and faster content retrieval time while protecting content confidentiality in NDN architecture. The simulation analyses prove that ES_CD performs better with a 10% lower computational time at the consumer and 6% lower communication time under our simulation topology.

Finally, we apply our scheme in a large-scale more realistic NDN network with a tree topology by using the simulator ndnSIM as shown in Figure.6. We conduct various simulations and analyze the content retrieval time with multiple consumers and content retrieval time for retrieving large file sizes. The simulation results and performance evaluation described in Figure.7 shows the feasibility and efficiency of our proposed architecture, which ES_CD can be at least used to retrieve the content with the file size of up to around 0.2 MB in the real deployment.

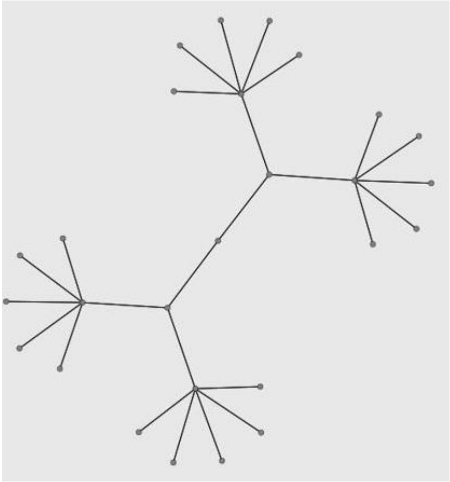


Figure 6. Network topology for ndnSIM simulations

The second experiment shows the retrieval time performance as the topology size grows in the number of consumers. In the real system environment, the number of users or consumers in the network may be increased with time. We collect the simulation results for adding 20 consumers, 40 consumers, 60 consumers, 80 consumers, and 100 consumers and run each simulation for 10 repetitive times. The average content retrieval time for retrieving 2 KB content is plotted in Figure. 8 in which each consumer randomly starts the content request.

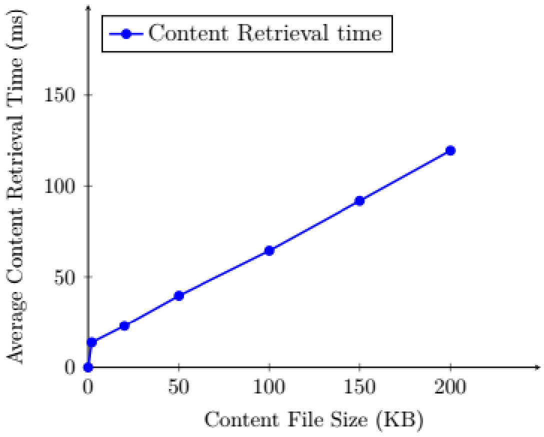


Figure 7. Average content retrieval time for consumers retrieving different file sizes.

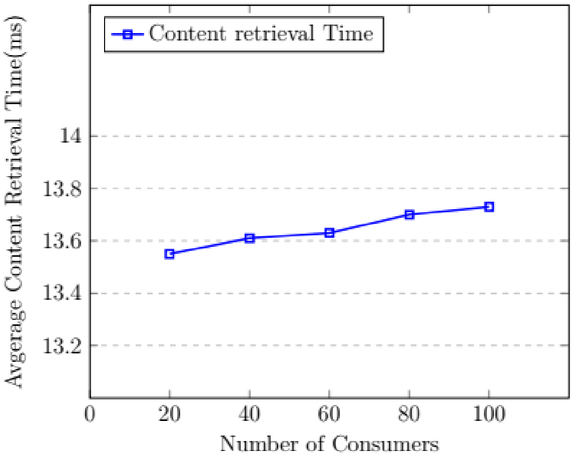


Figure 8. Average content retrieval time for retrieving 2KB content with l-consumers

The present analyses under our topology and simulation environment with ndnSIM show that our proposed scheme's average content retrieval time increases only by at least 0.2% to at most 0.5% with respect to the number of consumers increase in the network. Even if the number of consumers increases in the system, ES_CD incurs only a small content retrieval overhead to retrieve the desired contents as long as the same content is requested. Based on the results of the experiment with ndnSIM, we can say that ES_CD for the retrieval of the same content can be applied in NDN architecture with content confidentiality and security without affecting the performance of each NDN entity so much under the tree network topology.

Our scheme provides flexible access control in distributing content through the network so that the content producer can take advantage of its control over the cached contents. ES_CD incurs lower computational and communication overhead since it needs to modify the decryption key only, not the entire content for re-encryption or redistribution to the network. Finally, our analysis reveals that ES_CD is suitable for the application to the NDN architecture with acceptable cost and still utilizing the NDN in-network caching feature.

令和３年８月４日

学位論文審査報告書（甲）

１．学位論文題目（外国語の場合は和訳を付けること。）

Design and Implementation of the Efficient and Secure Content Distribution Scheme in Named Data Networking （名前に基づくネットワーキングにおける効率的で安全なコンテンツ配信方式の設計と実装）

２．論文提出者　(1) 所　　属　電子情報科学専攻

(2) 氏　　名（ふりがな）~~[illegible]~~　てぇ てぇ らいん
Htet Htet Hlaing

３．審査結果の要旨（600～650字）

令和３年８月~~5~~4日に第１回学位論文審査委員会を開催した。同日に口頭発表を実施し、その後に第２回学位論文審査委員会を開催した。慎重審議の結果、以下の通り判定した。なお、口頭発表における質疑を最終試験に代えるものとした。

インターネット上の膨大なコンテンツの送受信の問題を解決する手法として、データ名アドレッシングとインネットワークキャッシングを用いる名前付きデータネットワーキングが提案されている。そのコンテンツ保護のために暗号を適用したアクセス制御の仕組みが導入されているが、既存方式では、インネットワークキャッシングが十分に活用されていない、もしくは、コンテンツ作成者が常にコンテンツ配信に関与しなければいけないという課題が生じていた。本論文では、代理人再暗号化方式を活用した鍵管理の仕組みを、消費者、エッジルータ、コンテンツ作成者の間に適用することにより、キャッシュされたコンテンツを安全かつ効率的に活用できることなどを示している。

以上このように、本研究は名前付きデータネットワーキングにおける効率的で安全なコンテンツ配信に係る有益な知見を与えており、当該分野の発展に貢献するものである。よって、博士（工学）に値すると判断した。

４．審査結果　(1) 判　　定（いずれかに○印）　[✓ 合　格]　・　不合格

(2) 授与学位　博　士（工学）