Research on Security and Privacy Issues of NDN

Zengwu Zhang
Research Institute Electronic Science and Technology
UESTC
Chengdu, China
zzw19881117@163.com

Ke Zhang
Research Institute Electronic Science and Technology
UESTC
Chengdu, China
zhangke@uestc.edu.cn

***Abstract*—In the study of the future network architecture NDN, security and privacy problem has always been a very important research topic. Aiming at this problem, this paper analyzes and discusses the security and privacy issues in NDN network security, content security and privacy, signature and credit management, and explores its signature mechanism and trust model. Combining the characteristics of the data structure of NDN, tentatively proposes a security mechanism based on dynamic password, to further improve the security of NDN architecture in security and privacy protection, which is especially suitable for the application of high security requirement in NDN.**

Keywords-NDN; Security and privacy; Signature; Trust management; Dynamic password; Simulation

I. INTRODUCTION

As people increasingly attach importance to security and privacy problem, and the IP network has exposed the security and privacy problems more and more at the current time, so that we have to consider how to improve network security and privacy protection. IP system has stronger privacy property compared with the NDN (named data network), but IP network itself is not conducive to the spread of information, also has the problem of exposing location privacy. The main objective of NDN design is in order to spread the information better, in the NDN [1] network system, the system structure is content oriented, not related to the user information, so it could reduce the direct damage to the user to some extent. But the NDN's enhancing spreading information and limiting the range of dissemination (Privacy definition) is always a contradiction. NDN has its own security and privacy issues, such as the name privacy, signature privacy, and cache privacy. Based on the signature privacy we have proposed a security mechanism related to the dynamic password, with which user can request and receive the data more securely.

II. NDN

Named data network is one of the research topics of future network architecture that NSF supports recently, which is a data centric network system [2]. NDN system design has six principles [3]:1) retain the "waist" sandglass model, 2) retain the end-to-end principle, 3) reserve routing and forwarding plane separation, 4) flow self-regulating, 5) ensure the architecture neutral, 6) consider the safety.

In NDN there are only two kinds of data message: the Interest Packet and Data Packet, as shown in Figure 1. If the intermediate routing nodes cache the contents or the server receives the Interest message, Data message will be returned which contains the content data.

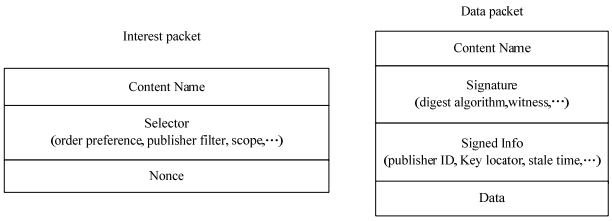

Figure 1. NDN packet type

The forwarding model of NDN consists of three main types: forwarding information base (FIB), content store (CS) and pending interest table (PIT). FIB save next interface that the routing node to the content server, a "face" representing an interface the router packet, the CS have save routing node, PIT record the name of not responding Interest packets of information and get the reaching face, so data packet can return along the way. In NDN forwarding model, the routing node receives an Interest packet first looks at CS, return data packets and end if a record is matching; or looking at PIT, end if a record is matching, record Interest packets in PIT if there is no match and forwarded Interest packets by the FIB search results. (Figure 2)

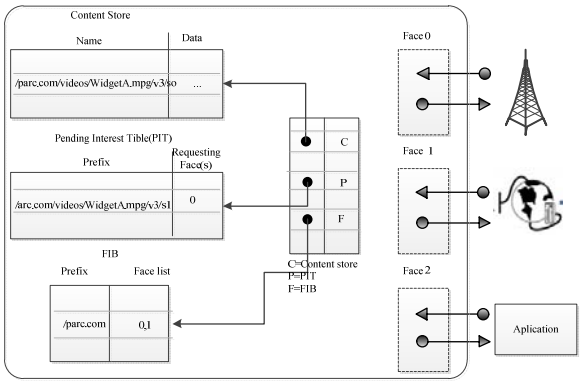

Figure 2. NDN forwarding model

III. SECURITY AND PRIVACY OF NDN

A. *Network security protection*

Any future Internet architecture must offer improved protection and resilience over today's network, which is subject to pervasive and persistent attacks. NDN network security is established based on the reliable routing network, routing information depends on the signature, and trust model is appropriate, it is different with the current network. The NDN packet is aimed at the content rather than the terminal, thus to a specific host for the target of the attack is very difficult [4], in fact, NDN is only in response to receiving the request to transmit the data packet, which makes the NDN network through the flood of unwanted data is not possible. However, research on the security of NDN network is facing challenges: 1) designing a trust model to defend against attacks on the routing mesh while supporting common providers' practices and policies, and 2) designing defenses against new types of attacks. We will design trust models appropriate to each of our routing research approaches, and implement and evaluate them in prototype routing components and experimental deployments. The processing of the request flooding and pollution mechanism is as follows:

Request flooding attack (mirroring traditional denial of service attack [5], DoS), such a request will send a large number of unique request, generally can't find the corresponding data in the cache. For flooding request attack, can do the experiment with routers, kill the request that can't meet the certain quantity, the request will meet the target domain given set of conditions, such as delete some request type, or a number of the request .

The content pollution attack is the malicious content matching the legitimate requests. For content pollution attacks, the consumer should always use signature verification to reject malicious content, but we also plan to evaluate the burden of ingress filtering and egress filtering in (non-core) routers to protect against simulated attacks.

B. *Content protection and privacy*

The source of the content, integrity, and reliability is necessary for the requester, but is usually not sufficient. Content providers want to have access to restricted fine texture in the sensitive and valuable content, and users want to maintain their privacy without exposing themselves to achieve what kind of content. This is a long-standing contradiction of communication both sides. Since NDN consumers are likely to obtain desired content from caches rather than the original publisher, the latter cannot rely on entities (hosting caches) to enforce its access control policies. Therefore, NDN adopts the familiar content-based approach to access control, obtained primarily via content encryption. Encryption is end-to-end and largely opaque to the network layer, handled by applications or libraries. Most of the use of encryption technology content protection (broadcast encryption and access control based on encryption) [6] by naming scheme and data cryptography suitable can be adopted by NDN. In order to enhance the security of NDN as possible as we can, we plan to select and implement appropriate schemes for specific applications, prioritizing efficiency and compatible support for revocation. We will also examine content firewalls, whose atomic unit of protection is content referenced by name, and which provide another method of user-friendly perimeter control for restricted content.

Although an NDN interest refers to a potentially human-readable name, NDN implicitly offers better end-to-end privacy, since it only tracks what data is being requested, and not who is requesting it. However, NDN poses three important privacy challenges: (1) cache privacy, because as with current web proxies, network neighbors may learn about each other's content accesses using timing information to identify cache hits; (2) name privacy, since the more meaningful NDN content names are, the more sensitive they may be; and (3) signature privacy, because the identity of a content signer and its revocation status may leak sensitive information about individuals and organizations. Various methods of addressing these challenges, e.g., VPN-like tunnels for Name Privacy, offer different trade-offs between privacy and cache ability. We can draw the outline of possible use in the architecture of NDN privacy related on the surface of the model, in order to explore the limits of privacy, can design and complement is similar to Tor [7]in NDN and mixed network diversity to maximize the data route cache and communication. The practical application of group signature [8] scheme can also be in NDN, any member of a group which can represent a group signature, any member can verify a group signature, but the signer is still to maintain privacy, connection between multi group signatures is not available.

C. *Signature and usable trust management*

Some data signature is added in the data unit, or cryptographic transformation of data unit. The data receiver or transform allows data unit to confirm the source of the data, units of data integrity and data protection, prevent to be forgery. The signature is established between the data requester and provider, it is also a way of guaranteeing the network security and

privacy. There are similarities of digital signature and the written document signature, the digital signature, can also confirm that the following two points: first, the information is sent by the signer information; second, after the issue has not been modified when received. So the digital signature can be used to prevent the electronic information to be modified and fake easily.

The maximum convenience to use RSA [9] or other public key cipher algorithm is that not having the key distribution problem. The more complex network, the more network user, its advantage is more obvious. Because the public key encryption uses two different keys, one of which is open to the public, another is confidential. The public key can be stored in the system directory, no encrypted e-mail messages, telephone directories (commercial telephone) or bulletin board, any user on the Internet can obtain the public key. The private key is dedicated to the user, hold by the user itself, it can decrypt the encrypted by the public key information.

Digital signatures general practice is: A first calculate the document M's HASH code, and then the code is encrypted HASH (this step is the signature), then M (M Do not encrypt files, third-party can access) and encrypted HASH code will be sent to B, B then use the public key to decrypt the encrypted HASH code just get, if it can decrypt shows that this document is issued by A, and has legal effect. Then calculate the resulting file of M HASH code, and then get out of the HASH just decryption code comparison (this step is called to verify the signature), if accord, shows that documentation M has not been modified in transit. (Figure 3)

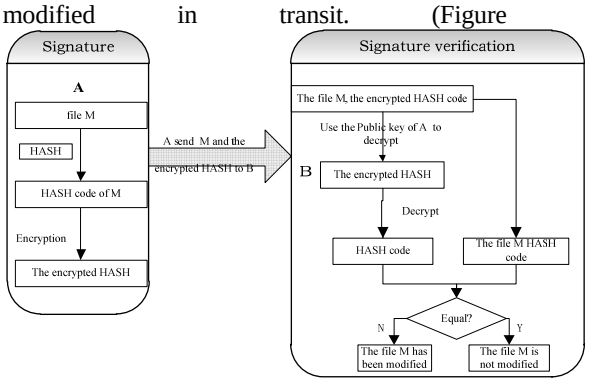

Figure 3. Signature and signature verification process

Signature verification of NDN content only shows this is a kind of special signature, so that this information is useful for application to the trust management--allows consumer judgment the given signature key. For example, a consumer might verify the front page of the New York Times because it is signed with a well-known certified key. She can then verify individual articles because the front page links securely to them. One advantage of NDN is that it does not require a "one size fits all" trust model: trust is end-to-end, between producer and consumer. Different consumers and different content may require varying levels of assurance. However, to make NDN accessible and deployable, it must come "out of the box" with a set of usable trust mechanisms applicable to a wide range of applications.

Prior research in trust management for large-scale deployment of public key cryptography has resulted in two main approaches: hierarchical Public Key Infrastructure (PKI) [10] and the peer level PGP web of trust [11], there are significant usability problems. Recent studies have shown that these methods can be in the NDN system easier to use, you can create a new way to automatically identify key through observation and experience. A suitable NDN model is SDSI/SPKI[12][13] (Figure 4), it is a small world model which maps a small-world model of trust onto a notion of local "namespaces" for naming keys, which in turn can map directly into the NDN notion of content namespaces.

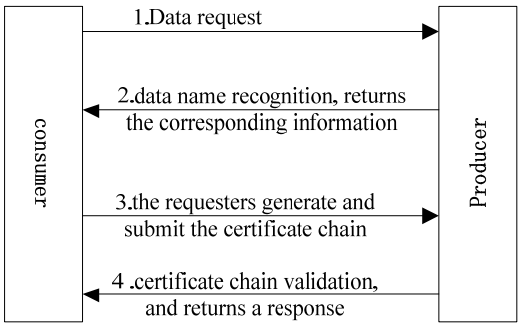

Figure 4. The requesters and providers that use the SPKI/SDSI protocol data flow diagram

IV. A Security Mechanism Based on Dynamic Password

A. *The working principle*

From the structure of data can be seen in Figure 1, the signature of the data is in the Data packet, Interest packet has no related components about security and trust. This NDN package type setting can guarantee the communication process smoothly, but has loopholes in safety such as the request flooding problems mentioned above. When such data request that can't match in network is large enough, it will decrease the entire network communication quality, even make it paralysis.

For such a situation may arise, combined with the characteristics of NDN package that each Interest packet NDN has a nonce, which is to facilitate to distinguish weather the receipt request has already received by the node. If this random number is for different applications, and even different data providers has a particular algorithm generated random number that need to make a dynamic password authentication, when the reception of this node that contain the dynamic password decrypt the password, then it will find in your cache whether has the requested data, if it is in the cache, it will return the data and the name according to the original road, or choose to forward or delete.

Here we do such a small change in nonce, the request flooding and privacy problems will have a better solution. When there are many requests that cannot be satisfied, the router can according to the random number weather meets a defined algorithm (or a library file) to delete some malicious requests. If user does not want others know what data it request in addition to the data provider, then the random number for a specific algorithm can have a good anonymous effect. Based on the process mechanism of dynamic password security as shown in Figure 5:

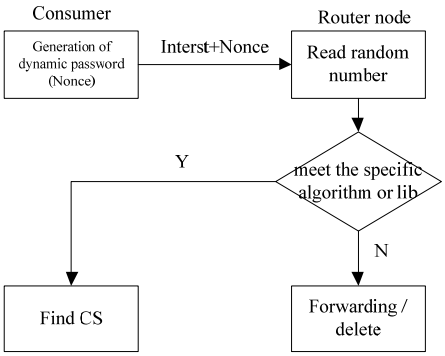

Figure 5. Security mechanism based on dynamic password

B. *Performance analysis of security mechanism based on dynamic password*

By the analysis above, the dynamic passwords into Interest packet structure of NDN can enhance security in the process of data transmission, but we need to consider its performance, therefore, we carries on the simulation of the communication process in the architecture of NDN to see the delay and data rate. Some scene and parameter configuration as follows:

Scene: all nodes constitute a class of tree structure, including a root node, two level 2 child nodes, 4 level 3 child nodes.

Part parameters: the inter node bandwidth is 10Mbps; each node queuing delay is set to 1ms; node per second can send 100 Interests, the simulation time is 20s; the node verification of dynamic password time is a random value between 0~20ms.

The results of simulation in Network simulation version 3 and R as follows:

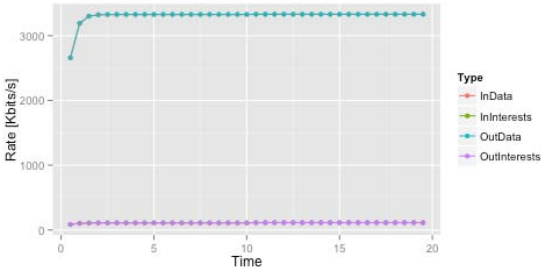

Figure 6. Data rate

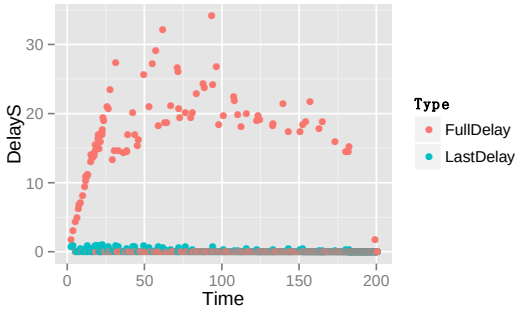

Figure 7. delay

As can be seen from Figure 6, the data transmission rate reached a stable level in a short period of time, this is consistent with the simulation parameters of 100 Interest/s configuration, and it is not affected by delay; as can be seen from Figure 7, security mechanism using dynamic random number generated unstable delay, obviously this is because the origin verification of the random number, the delay will gradually decrease as the process of communication. Through the simulation results we can conclude that, the security mechanism of the dynamic random number does not affect the data rate, but will have a certain impact on delay. Therefore, the mechanism is suitable for the applications that demand for high security but not for a good delay requirement.

V. CONCLUSION

This paper mainly analyses the security and privacy issues under the architecture of NDN, preliminarily has discussed the network security protection, content security and privacy, signature and credit management. According to the structure of data packet in NDN, has proposed a security mechanism based on dynamic password, better improved security and privacy issues under the structure of NDN, provided the basis on the study of NDN in order to solve the security and privacy issues.

REFERENCES

[1] Named data networking project(NDN).http://named-data.net

[2] Van Jacobson, Diana K. Smetters, James D. Thornton, Michael F. Plass, Nicholas H. Briggs, and Rebecca L. Braynard. Networking named content. In Proceedings of the 5th ACM International Conference on Emerging Networking Experiments and Technologies, pages 1–12, 2009

[3] Minerlong, Chenzhen, xuhongfeng, liangyong. Research progress of CCN ll 1 content centric networking of information network security, 2012, (02):6 10

[4] Dan Jen, Michael Meisel, He Yan, Daniel Massey, Lan Wang, Beichuan Zhang, and Lixia Zhang. Towards A Future Internet Architecture: Arguments for Separating Edges from Transit Core. In ACM Workshop on Hot Topics in Networks, 2008.

[5] John Ioannidis and Steven M. Bellovin. Router-based defense against ddos attacks. 2002.

[6] Selim G. Akl and Peter D. Taylor. Cryptographic solution to a problem of access control in a hierarchy. ACM Trans. Comput. Syst., 1(3):239–248, 1983.

[7] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In Proceedings of the 13th USENIX Security Symposium, August 2004.

[8] Xuhua Ding, Gene Tsudik, and Shouhuai Xu. Leak-free group signatures with immediate revocation. In IEEE ICDCS, pages 608–615, 2004.

[9] Xuhua Ding and Gene Tsudik. Simple identity-based cryptography with mediated rsa. In CT-RSA, pages 193–210, 2003.

[10] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.Carl

[11] Philip R. Zimmermann. The Official PGP User's Guide. MIT Press, Cambridge, MA, USA, 1995. ISBN 0-262-74017-6.

[12] M. Ellison, Bill Frantz, Butler Lampson, Ron Rivest, Brian M. Thomas, and Tatu Ylonen. SPKI Certificate Theory, September 1999. RFC2693.

[13] Ronald L. Rivest and Butler Lampson. SDSI-A Simple Distributed Security Infrastructure. Technical report, MIT, 1996.