Integrated Intelligent Research (IIR)
International Journal of Communication and Networking System
Volume: 05 Issue: 02 December 2016, Pages No.123-125
ISSN: 2278-2427

Content Search Control for Named Data Networking

V.Kavitha
M.E Computer Science and Engineering, P.B. College of Engineering
Email: kavi.kavitha.v78@gmail.com

Abstract: Named Data Networking (NDN) is a new paradigm for future internet, data packet carry name rather than current IP paradigm of source and destination addresses, to provide light integrity verification architecture for security in NDN system. Content based search is common where the issue of security lie low than expectation. Different Systems are connected in different networks where the information of the system will be stored in the router and the content of the system in its temp memory so that the data response will be redirected from the router cache itself. The main mechanism of LIVE lies in generating different content integrity status for a single content object, which allows a Content Provider to control content access performed by NDN nodes. Pending Interest Table (PIT), stores all the Interests that a router has forwarded but not satisfied yet. Each PIT entry records the data name carried in the Internet, together with its incoming and outgoing interface(s). Forwarding Information Base (FIB), a routing table which maps name components to interfaces. The FIB itself is populated by a name-prefix based routing protocol, and can have multiple output interfaces for each prefix. Content Store (CS), a temporary cache of Data packets the router has received. Because an NDN Data packet is meaningful independent of where it comes from or where it is forwarded, it can be cached to satisfy future interests. Replacement strategy is traditionally least recently used, but the replacement strategy is determined by the router and may differ.

Index terms: Content Confidentiality, access control, data security

I. INTRODUCTION

Present signature generation and verification algorithms are heavyweight such that universal content integrity verification is hard to achieve for network nodes, especially for Internet-scale content routers. Secondly, the current NDN design allows arbitrary content caching and accessing such that any network node of a domain (e.g., an Internet Service Provider) that enables NDN can arbitrarily cache contents when the contents are delivered by them, without any approval from Content Providers (CP).Content based search does not provide accurate content search result more over the result is not secure in network channel. Communication in network is based on source to destination address. RSA or DSA Algorithm is used which is heavy weight.

Lightweight integrity verification architecture (LIVE), an extension to the NDN protocol. LIVE enables universal content signature verification in NDN with lightweight signature generation and verification algorithms. Further, it allows a content provider to control content access in NDN nodes by selectively distributing integrity verification tokens to authorized nodes. Content based search is established instead of IP based search. LIVE prevent NDN routers and users from accessing "corrupted" or "fake" contents. Low overhead as the search reduces normal traffic. We use Triple Data Encryption Standard for encryption and decryption process. We provide a Pailier signature algorithm, to produce tokens for signature generation.

II. RELATED WORKS

2.1 Content Confidentiality

For highly sensitive content, confidentiality is a desired requirement, i.e., only authorized end users can obtain the content. Access control relying on integrity verification is not sufficient for this requirement. LIVE adopts a lightweight encryption mechanism, where encryption keys are derived from integrity verification tokens. With this option, a CP can seamlessly support strong content access control for confidentiality by controlling who can obtain the tokens.

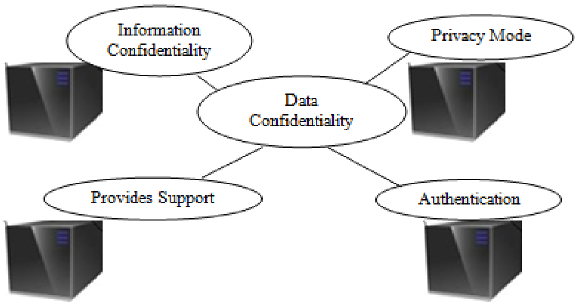

Fig.1. Content Confidentiality

2.2 Access Control

The goal of LIVE is to enable a generic and lightweight content verification and cache access control in NDN nodes. However, it cannot prevent attacks from malicious NDN nodes in network. For instance, an attacker can access sensitive contents by compromising NDN nodes and launching manin-the-middle (MITM) attacks. In particular, MITM attacks can be launched by malicious nodes between two benign NDN nodes, and the malicious nodes can capture contents by content packet sniffing.To address this type of attacks, we extend the basic verification scheme and incorporate content encryption in LIVE. If content is sensitive, CP can encrypt the content before it is distributed, such that the whole content cannot be read without a decryption key even if an unauthorized node obtains it. The encryption key is embedded in the private token. Therefore, an attacker cannot access the content, even if he can obtain the content by bypassing the content verification logic. However, an authorized NDN node can still correctly decrypt the correct content blocks during signature verification according to the information embedded in the tokens. the performance does not reduce significantly. Only users who have correct tokens can verify and decrypt the contents. Therefore, the mechanism enables ensured content access control.

2.3 Data Security

The software may be safety-critical. If so, there are issues associated with its integrity level. The software may not be safety-critical although it forms part of a safety-critical system. For example, software may simply log transactions. If a system must be of a high integrity level and if the software is shown to be of that integrity level, then the hardware must be at least of the same integrity level S. There is little point in producing 'perfect' code in some language if hardware and system software (in widest sense) are not reliable. If a computer system is to run software of a high integrity level then that system should not at the same time accommodate software of a lower integrity level. Systems with different requirements for safety levels must be separated. Otherwise, the highest level of integrity required must be applied to all systems in the same environment.

III. SCENARIO

3.1 System Model

System Model consist of five modules namely

- NDN Node.
- Router Formation.
- NDN content search.
- Key initialization.
- LIVE Response for content search.

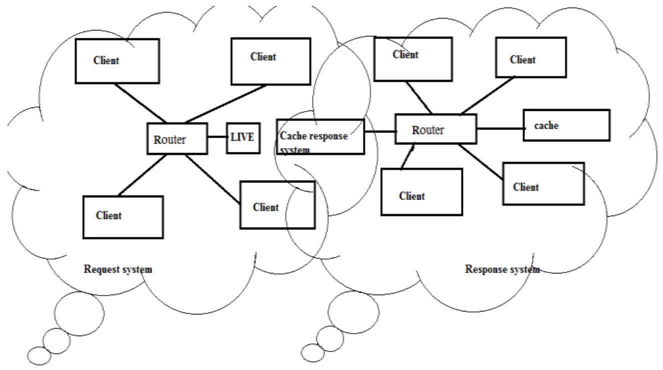

Fig.2. System Overview

A.NDN Node

In this each system contents and set up a Network configuration. Here router is a networking device that forwards data packets between computer networks. Router Stores the information of the neighbor systems that are connected in their network same of the different routers in different networks.

B. Router formation

The communication between Systems and routers will be by secret key which will be provided by random in a network. It specifies different features of the router and NDN system like system name, system port number etc. but not IP-address.

C.NDN Content Search

System communication will be based on content only not the IP based search or communication. There are two possibilities in search process first, the search within same network and second search between different networks. If the search is between same network systems then the content provider in router stores all system information and response will be form same router itself by router key token generation and user system key token. Key token will be two parts public key and private key for every router and user system and encryption or decryption will be done with these keys. If the communication is between different nodes of different networks then the system communication is through the routers of different network and the same signature verification is done efficiently.

D.Key Initialization

Key token will be two parts public key and private key for every router and user system and encryption or decryption will be done with these keys. If the communication is between different nodes of different networks then the system communication is through the routers of different network and the same signature verification is done efficiently.

E.Live Response for Content Search

Here the content search response will be provided to the system in request of particular data. The search content result will be in encrypted form so that man-in-middle attack is prohibited and it has key to be decrypted. Signature verification algorithm will verify the content user and provide the correct decrypt content where content provider monitor Forward Information Base Table, Pending Interest Table and Cache Store Table and updates these table. We evaluate the delay of two-hop content forwarding with and without caching.

IV. LIVE IMPLEMENTATION AND EVALUATION

LIVE generates MHT values to produce token P and signs contents with the signature scheme (P, h), where P is the generated token and h is a collision-resistant hash function. We can obtain the following theorem.

Theorem 1: Given a collision-resistant hash function h and a token P, the proposed signature scheme (P, h) in LIVE is enforceable.

Proof: We prove the theorem by showing that any polynomial time algorithm breaks the enforceability of the proposed signature scheme only with negligible probability in the random oracle model. Recall that the proposed signature scheme is a onetime signature. Without loss of generality, we assume that in some state the token key is X = {x1, . . . , xn} and the public key is P = h(f (h(x1))|| . . . || f (h(xn))), and the adversary is intending to forge a signature scheme corresponding to the token key X. Suppose that the adversary presents (C, S), where C is the content, and S is the forged signature corresponding to C. Given content C, with the token X, we can generate the signature S. We are interested in the probability that S = S given C, because in the verification algorithm the adversary makes the verification algorithm output true only if S = S. Moreover, in order to achieve S = S, then for those g j = 0, the adversary has to correctly compute s j = f (h(x j)), where x j is unknown to the adversary. Therefore, the probability of generating output s j = f (h(x j)) by adversary is 1 2l where h is modeled as a random oracle. In addition, for g j where g j = 1, the adversary has to correctly compute s j = x j, where x j is unknown to the adversary. Therefore, the probability of generating output *s j* = *x j* is 1 2 |*x j* |. Since |*x j*| ≥ *l*, we can obtain that the probability of generating output *S* = *S* by the adversary is less then *(* 1 2*l)l* . We can conclude that *(* 1 2*l)l* is negligible, where *l* = 32.

Therefore, the probability of breaking the enforceability of the signature scheme by the adversary is negligible.

V.PERFORMANCE ANALYSIS

This is the prototype to determine the performance of LIVE. Since content access delay incurred by verification is proportional to length of content packet delivery, for simplicity, we only evaluate the delay of two-hop content forwarding with and without caching. Figure 5 shows the testbed of our experiments, including one user node *R*1 and one CP node *R*4. Also, it includes two machines acting as NDN routers: *R*2 is a CR of the CP and can cache the contents from the CP, and *R*3 is the normal router that cannot cache the contents from CP.

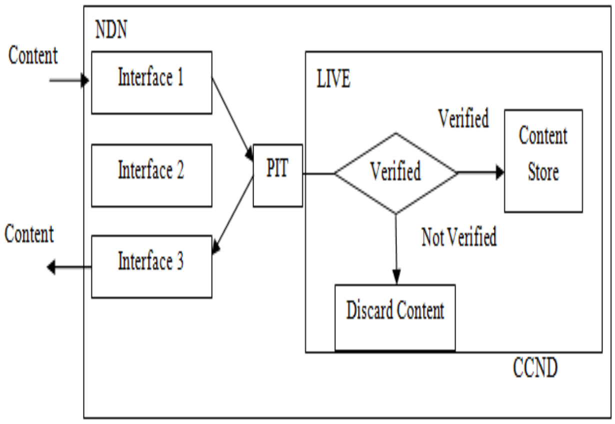

Fig.3. LIVE Implementation

*R*3 forwards content requests received from *R*1 to *R*4. We evaluate the performance of LIVE at *R*1 and *R*4 using Mac laptops with 2.53 GHz Intel CPU, 4GB RAM, and Mac OS 10.6.8. We investigate the token generation performance in the CP and measure the computation and content delivery delays introduced by LIVE in the user node R1. Also, since LIVE increases the content packet size by piggybacking signatures, we measure the communication overhead incurred by LIVE. Evaluate the LIVE performance with different content sizes range from 150 bytes to 1480 bytes. To demonstrate the benefits of lightweight signatures in LIVE, we also implement a signing and verification library with the RSA algorithm with 1024-bit RSA keys by extending the Open SSL library.

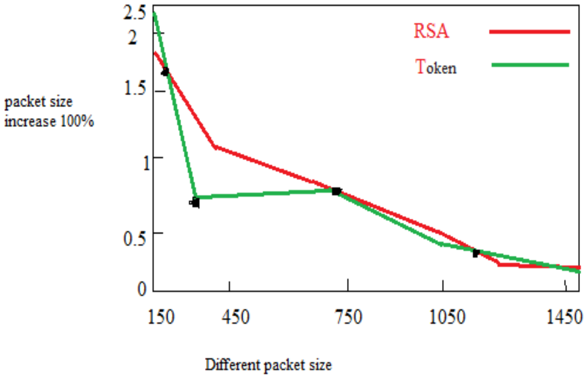

Fig 4. Communication Overhead

VI. DISCUSSION AND CONCLUSION

LIVE, a light weight integrity verification mechanism for Named Data Networking to enable universal content integrity and authenticity verification. Further LIVE to achieve efficient and scalable content access control, which allows a content provider to enforce flexible security policies on content caching and access. In particular, random encryption in the mechanism such that LIVE can prevent or mitigate unauthorized content access. In prototype LIVE in CCNx, and demonstrate its benefits by experimental study, which shows that it introduces acceptable overhead in content access. In future, investigate a more efficient token refresh scheme, and leverage group key management schemes to enable token management for sensitive contents and to implement CP authentication during token refreshment.

References

[1] A.Afanasyev, P.Mahadevany, I. Moiseenko, E.Uzuny, and L. Zhang, “Interest flooding attack and countermeasures in named data networking,” in Proc. IFIP Netw. Conf, May 2013, pp. 1–9.

[2] A.Mohaisen, X.Zhang, M.Schuchard, H.Xie, and Y.Kim, “Protecting access privacy of cached contents in information centric networks,” in Proc. 8th ACM ASIACCS, 2013, pp. 173–178.

[3] P.Gasti, G.Tsudik, E.Uzun, and L.Zhang, “DoS and DDoS in named data networking,” in Proc. ICCCN, 2013, pp. 1–7.

[4] V.Jacobson, D.K.Smetters, J.D.Thornton, M.Plass, N.Briggs, and R.Braynard, “Networking named content,” Commun. ACM, vol. 55, no. 1, pp. 117–124, 2012.

[5] N.Fotiou, G.F.Marias, and G.C.Polyzos, “Access control enforcement delegation for information-centric networking architectures,” in Proc. ACM SIGCOMM Workshop Inf.-Centric Netw., 2012, pp. 85–90.

[6] The Content Centric Networking (CCNx) Project. [Online]. Available: http://www.ccnx.org/, accessed 2012.

[7] S. DiBenedetto, P. Gasti, G. Tsudik, and E. Uzun, “ANDaNA: Anonymous named data networking application,” in Proc. NDSS, 2012. [Online] Available: http://www.internetsociety.org/andana-anonymousnamed-data-networking-application

[8] M. Nabeel, N. Shang, and E. Bertino, “Efficient privacy preserving content based publish subscribe systems,” in Proc. 7th ACM SACMAT, 2012, pp. 133–144.