Scientific Journal of Impact Factor (SJIF): 4.14
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 3, March -2016

Novelty Cache Concept in Named Data Network

C. Bharathipriya[1], A.Daphnil Madhunita[2] S.Anusha[3]

[1,2]Student , Dept. of Computer Science and Engineering, Dhanalakshmi College of Engineering
[3]Assistant professor, Dept. of Computer Science and Engineering, Dhanalakshmi college of engineering

Abstract-*Named Data Networking is a new paradigm for future internet here data packet carry name rather than current IP paradigm of endpoints. Thus we provide light weight 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 stores all the Interests that a router has forwarded but not-satisfied yet. Forwarding Information Base is a routing table which maps name components to interfaces. The FIB itself is occupied by a name- affix routing protocol, and have multiple output interfaces for each prefix. Content Store is a transient cache of Data packets that the router has accepted. Because data packet of an NDN is meaningful autonomous of where it comes from or where it is forwarded thus it can be cached to satisfy upcoming Interests. Replacement strategy is traditionally having already been used, but the replacement strategy is determined by the router and may differ.

Keywords- *access control, data security, content provider, reduced traffic, low overhead.*

I INTRODUCTION

NDN routers stores the state of newly forwarded packets, which allows smart dispatch, loop detection, flow balance, ubiquitous caching, etc. Address assignment and management is no longer required in local networks. NDN namespace is unbounded. The Router PIT table is key for load balancing where the multiple requests from the same system will be reduced and so Denial of Service attack is reduced. Bandwidth performance is increased.

CCN enables the network to scale by allowing caching and facilitating resource planning. Interests match Content Objects deploy on name prefixes. NDN treats network routing and control messages like all NDN data which requires signature. This issue a stable foundation for securing routing protocols against attack, e.g., spoofing and tampering. Thus Endpoints communicate based on named data instead of IP addresses.

II EXISTING SYSTEM

Present signature generation and verification algorithms are heavyweight such that universal content integrity verification is hard to achieve for nodes, especially for Internet-scale content routers. The current NDN design allows random content caching and gaining such that any network node of a domain (e.g., an Internet Service Provider) that enables NDN can randomly cache contents when the contents are delivered by them, without any approval from Content Contributer or provider. 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.

III PROPOSED SYSTEM

Lightweight integrity verification architecture is an extension to the NDN protocol. In NDN, LIVE enables universal content signature verification with lightweight signature generation and verification algorithms. Further, it allows a content provider to provide 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 blocks fake data being accessed by NDN router and users. Low overhead as the search minimizes normal traffic. We use Triple Data Encryption Standard for encryption and decryption process. We provide a hash tree based signature algorithm, to produce tokens for signature generation.

IV EXPERIMENTAL WORK

A. NDN Node and Router Formation

@IJAERD-2016, All rights Reserved

In this module we initialize each system contents and set up a Network configuration Here router is a networking device that forwards data packets between networks. Router Stores the information of the neighbour systems that are connected in their same network and also of the different routers in different networks. The communication between Systems and routers will be by secret key which will be provided by random in a network. We specify different features of the router and NDN system like system name, system port number etc. but not IP-address.

B. NDN Content Search

System communication will be based on content only not the IP based search or communication. In this module there is 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 node 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.

C. Live Response for Content Search among routers

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 mordenize these table. We evaluate the delay of two-hop content forwarding with and without caching.

D. Live Response for Cache Content

If the search content does not exists in the any of peer systems as well as peer routers. The search begins at the server, as similar search in the peer nodes, and routers. The found content will be given as a encrypted content to the node. The router has the copy of encrypted content in it. While next search being for the same content the router provides the content.

V ALGORITHM

A. Key Generation

The public key and the private key of the each Node and the Routers are generated by the efficient Algorithm –My Pailier Algorithm.

Choose two large prime numbers p and q randomly and independently of each other such that gcd (pq,(p 1)(q 1)) = 1 . This goods is assured if both primes are of equal length.

1. Compute n = pq and $\lambda = \text{lcm}(p-1, q-1)$.
2. Choose any integer g where $g \in Z^*_{n2}$
3. Ensure n divides the order of g by checking the alive of the following modular multiplicative inverse: $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$,where function L is defined as $L(u) = u-1/n$

Note that the notation $\frac{a}{b}$ does not denote the modular multiplication of a times the modular multiplicative inverse of b but preferably the quotient of a divided by b , i.e., the largest integer value $v \geq 0$ to satisfy the relation $a \geq vb$.

The public key is (n ,g)

The private key is (λ ,μ)

If using p,q of equivalent length, a simpler variant of the above key generation steps would be g = n+1,$\lambda = \varphi(n)$ and $\mu = \varphi(n)^{-1} \bmod n$, where $\varphi(n) = (p-1)(q-1)$.

B. Signature Generation

We provide a hash tree based signature algorithm, to produce tokens for signature generation.

Stage (I): Token generation

@IJAERD-2016, All rights Reserved

1. Cohort key vectors $X^k = \{x_1^k, \ldots, x_j^k, \ldots, x_n^k\}$, where $x_j^k \in \{0, 1\}^\lambda$, given $n \in Z$, where k = 0,1, 2;
2. $P^k \leftarrow h(f(h(x_1^k)) \| f(h(x_2^k)) \| \ldots \| f(h(x_n^k)))$, where P^0 is in the category of public token P^-, P^1 and P^2 are in the category of private tokens $P^\dagger$ and P , respectively

Stage (II): Policy generation

3. Generate two categories of the router sets R_C and R†C with respect to content C, where R_C denotes the set of routers receiving public token P0 to verify C, and R†C denotes the router set receiving private token P1 to verify C;
4. Generate the categories of authorized user sets R_C receiving private token P^2 to verify content C;

Stage (III): Token distribution

5. Receive token request from node i that are in $R_C^\dagger$ or R_C ;
6. $P^k \leftarrow ENC_{PKi}(P^k)$, where k is equal to 1 if i is in $R_C^\dagger$, otherwise it equals to 2;
7. Send out P^k to node i ;

Stage (IV): Token refreshment

8. Generate new key vectors $X^k = \{x_1^k, \ldots, x_j^k, \ldots, x_n^k\}$, for R^- , $R^\dagger$, and R, where $x_j \in \{0, 1\}^\lambda$, given $n \in Z$;
9. $P^{k\prime} \leftarrow h(f(h(x_1^{k\prime})) \| f(h(x_2^{k\prime})) \| \ldots \| f(h(x_n^{k\prime})))$;
10. $P^{k\prime} \leftarrow ENC_{P^k}(P^{k\prime})$ if k = 1 or 2;
11. Embed $P^{k\prime}$ in the content and distribute them to different requesters.

C. Encryption and Decryption

We provide Triple Data Encryption Standard for encryption and decryption process which deploys a key pile that is made up of three DES keys, A1, A2 and A3, each of 56 bits (excluding parity bits). The encryption algorithm is:

$$\textbf{ciphertext} = EA_3(DA_2(EA_1(\text{plaintext})))$$

i.e., DES encrypt with A1, DES decrypt with A2, then DES also encrypt with A3.
Decryption is the reverse:

$$\textbf{plaintext} = DA_1(EA_2(DA_3(\text{ciphertext})))$$

i.e., decrypt with A3, encrypt with A2, then decrypt with A1.
Each triple encryption encodes one block of 64 bits of data. In each case the middle operation is the reverse of the first and last. This increases the
strength of the algorithm when using keying option 2, and provides backward agreement with DES with keying option 3.

VI DESIGN AND IMPLEMENTATION CONSTRAINTS

A. Constraints in Analysis

1. Constraints as Informal Text
2. Constraints as Operational Restrictions
3. Constraints Integrated in Existing Model Concepts
4. Constraints as a Separate Concept
5. Constraints Implied by the Model Structure

B. Constraints in Design

@IJAERD-2016, All rights Reserved

1. Determination of the Involved Classes
2. Determination of the Involved Objects
3. Determination of the Involved Actions
4. Determination of the Require Clauses
5. Global actions and Constraint Realization

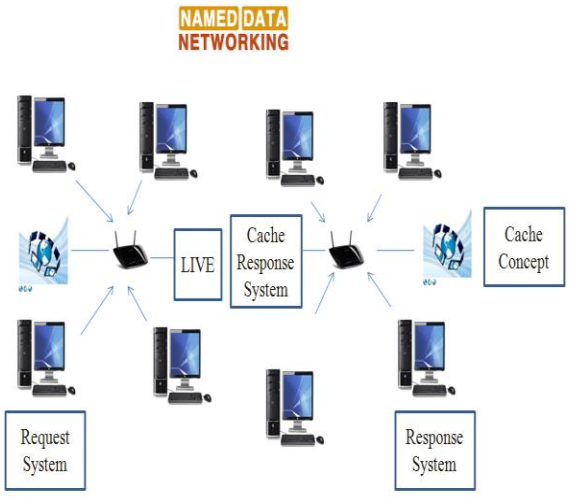
C. Constraints in Implementation

A hierarchical structuring of relations may provide an outcome in more classes and a more complicated structure to implement. Therefore it is recommended to transform the hierarchical relation structure to a simpler structure such as a classical flat one. It is rather easy to transform the developed hierarchical model into a bipartite, flat model, consisting of classes on the one part and flat relations on the other. Flat relations are preferred at the design level for reasons of simplicity and execution ease. There is no identity or functionality associated with a flat relation. A flat relation compatible with the relation concept of entity-relationship pattern and many object oriented methods.

VII SYSTEM FEATURES

NDN routers retain the state of recently forwarded packets, which allows smart forwarding, loop detection, flow balance, ubiquitous caching, etc. Address assignment and management is no longer required in local networks. NDN namespace is unbounded. The Router PIT table is key for load balancing where the multiple requests from the same system will be reduced and so Denial of Service attack is reduced. Bandwidth performance is increased.CCN enables the network to scale by allowing caching and facilitating resource planning. Interests match Content Objects based on name prefixes. NDN serve network routing and control messages like all NDN data, requiring signatures. This provides a stable foundation for securing routing protocols towards attack, e.g., spoofing and tampering. Thus Endpoints communicate based on named data instead of IP addresses.

VIII ARCHITECTURE DIAGRAM



IX CONCLUSION

LIVE activates universal content signature verification in NDN with lightweight signature generation and verification algorithms. LIVE prevent NDN routers and users from accessing “corrupted” or “fake” contents. Low overhead as the search reduces normal traffic. We propose Triple Data Encryption Standard for encryption and decryption process. The hash tree based signature algorithm is used to produce tokens for signature generation. The Availability of the content of data get increased tremendously when the user starts using it. The content copy get multiplied among the user and the data traffic get reduced totally.

@IJAERD-2016, All rights Reserved

X REFERENCE

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

[2] N. Fotiou, G. F. Marias, and G. C. Polyzos, "Access control enforcement delegation for information-centric networking architectures," in ACM SIGCOMM workshop on Information-centric networking, 2012.

[3] R. C. Merkle, "A digital signature based on a conventional encryption function," in CRYPTO, 1987, pp. 369–378.

[4] M. Conti, P. Gasti, and M. Teoli, "A lightweight mechanism for detection of cache pollution attacks in named data networking," Comput. Netw., vol. 57, no. 16, pp. 3178–3191, 2013.

[5] A. Afanasyev, P. Mahadevany, I. Moiseenko, E. Uzuny, and L. Zhang, "Interest flooding attack and countermeasures in named data cnetworking," in Networking, 2013.

[6] A. Mohaisen, X. Zhang, M. Schuchard, H. Xie, and Y. Kim, "Protecting access privacy of cached contents in information centric networks," in ACM ASIACCS, 2013.

[7] G. Bianchi, A. Detti, A. Caponi, and N. Blefari Melazzi, "Check before storing: What is the performance price of content integrity verification in LRU caching?" SIGCOMM Comput. Commun. Rev., vol. 43, no. 3, pp. 59–67, 2013.

[8] A. Detti, A. Caponi, G. Tropea, G. Bianchi, and N. Blefari-Melazzi, "On the interplay among naming, content validity and caching in information centric network," in Proceedings of IEEE GLOBECOM, 2013.

[9] G. Acs, M. Conti, P. Gasti, C. Ghali, and G. Tsudik, "Cache privacy in named-data networking," in ICDCS, 2013, pp. 41–51.

[10] M. Bellare and P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols," in CCS, 1993, pp. 62–73.

@IJAERD-2016, All rights Reserved