Secure Network Coding against Content Pollution Attacks in Named Data Network

Tao Feng, Xiaomei Ma, Xian Guo, and Jing Wang

***Abstract*—Named Data Network (NDN) is one of the future Internet architecture, all nodes (i.e., hosts, routers) are allowed to have a local cache, used to satisfy incoming requests for content. However, depending on caching allows an adversary to perform attacks that are very effective and relatively easy to implement, such as content pollution attack. In this paper, we use a method of secure network coding based on homomorphic signature system to solve this problem. Firstly, we use a dynamic public key technique, our scheme for each generation authentication without updating the initial secret key used. Secondly, employing the homomorphism of hash function, intermediate node and destination node verify the signature of the received message. In addition, when the network topology of NDN is simple and fixed, the code coefficients in our scheme are generated in a pseudorandom number generator in each node, so the distribution of the coefficients is also avoided. In short, our scheme not only can efficiently prevent against Intra/Inter-GPAs, but also can against the content poisoning attack in NDN.**

***Index Terms*—Named data networking, content pollution attack, network coding signature.**

I. Introduction

With the increasingly rich of applications and calculation modes, and with the enhancement of the social dependence on the Internet, Internet access and network function orientation has undergone tremendous change. In terms of scalability, mobility and security, TCP / IP architecture has been unable to satisfy the requirements of sustainable development of the Internet. Therefore, in order to better serve the future Internet, researchers trying to redesign the existing Internet architecture, and propose the Future Internet Architecture (FIA) [1].

Named Data Network (NDN) [2], [3] is one of the future Internet architecture, now is considered as a viable replacement for the current IP-based Internet, which uses the methods of name-based routing, forwarding and caching to optimize network transmission efficiency. In NDN, there is not the concept of connection, only the content publishers and content consumers. Content publishers need to encrypt and sign the content, content consumers need to decrypt and verify legal content. Moreover, all nodes (i.e., hosts, routers) are allowed to have a local cache, used to satisfy incoming requests for content. This makes NDN a good architecture for efficient large scale content distribution. However, depending on caching allows an adversary to perform attacks that are very effective and relatively easy to implement, such as content pollution attack [4], [5].

In theory, content signatures provide an effective and simple means for detecting content poisoning attacks in NDN [6], [7]. Currently, most of the signature algorithm are based on homomorphic hashing function.For example, Korhn *et al*. [8] using homomorphic hash function to construct the verification algorithm for the first time. However, the total size of the hash values of the scheme is proportional to the number of blocks, which could be very large and the cryptographic hash function is computationally expensive. Li *et al.* [9] employed a batch content distribution verification scheme, which reduced the computational cost of each node. Unfortunately, their scheme unable to realize the network max-flow and can bring delay to the sinks. Zhao *et al*. [10] from the perspective of linear space, presented a lower computational complexity signature scheme, but their scheme required long start-up latency. Yu *et al*. [11] proposed an RSA-based scheme, which firstly used the homomorphism hash function to calculate the hash value of the source message, then used RSA algorithm to calculate signature of the hash value, then send message with signature. Rosario *et al*. [12] improved the Yu's scheme, they designed the RSA-based homomorphic signature scheme in integer field, and used the random oracle model to prove the security of the scheme.

With the deepening of the research, researchers found that the schemes of all the above only designed to prevent against Intra-Generation Pollution Attacks (intra-GPAs) do not work well for multiple generation propagations. In the case of multiple generation propagations, these schemes may exsit inter-Generation Pollution Attacks (inter-GPAs). The so-called inter-GPAs, refers to that an adversary can take advantage of a valid message W of the k-th generation, to act as the message of the $k+i$-th generation. Because this message does not belong to the $k+i$-th generation, so it is clearly a fake content. But the signature of this message is calculated by the source (calculated in the k -th generation), so this message can passed the verification of intermediate nodes, so that it can successfully forge a message of the $k+i$-th generation, and destroy the transmission of the $k+i$-th generation message Guangjun L. *et al*. [13] used the dynamic public key technique, proposed a novel homomorphic signature scheme, in which the source does not update the system key frequently. This scheme can defeat Intra-GPAs and Inter-GPAs effectively.

In practice, however, the overhead of signature verification is a challenge in NDN router. The ref. [5] and [7] also show that the traditional signature verification have a high requirements of the router interface and computing power. So, when we choose signature scheme, not only consider the

Manuscript received January 28, 2015; revised November 23, 2015.

The authors are with the School of Computer and Communication, Lanzhou University of Technology, CO 730050 China (e-mail: fengt@lut.cn, mxm1129@126.com, iamxg@163.com, wangjing@lut.cn).

security, but also consider the overhead. The ref. [14] presented a network coding signature algorithm of low communication overhead, which made the signature as redundant added into the source messages, then hashed the padded messages to the public parameters. This scheme has a lower communication overhead than other schemes. However, this method designed to prevent against Intra-GPAs, do not work well for multiple generations.

Inspired by the idea of ref. [13] and ref. [14], we propose a novel method with low communication overhead, particularly, that can efficiently prevent against Intra/Inter-GPAs. Eventually, we apply this method to named data network (NDN), to solve the content poisoning attack in NDN. Firstly, we use a dynamic public key technique, our scheme for each generation authentication without updating the initial secret key used. Secondly, employing the homomorphism of hash function, intermediate node and destination node verify the signature of the received message. In addition, when the network topology of NDN is simple and fixed, the code coefficients in our scheme are generated in a pseudorandom number generator in each node, so the distribution of the coefficients is also avoided.

II. Homomorphic Hash Function

Currently, most of the homomorphic signature algorithm are based on homomorphic hash function, Korhn *et al*. [8] using homomorphic hash function to construct the verification algorithm for the first time. The homomorphic hash function is as follows:

A trusted party globally generates a set of hash parameters $G = (p, q, g)$, where p and q are two large random primes such that $q \mid p-1$. The hash parameter $\mathbf{g}$ is a $1\times n$ row-vector, composed of random elements of F_p, all order q. That is, $\mathbf{g} = (g_1, \cdots, g_n)$, where $g_i^q \equiv 1 \bmod p$, $g_i \in F_p$, $1 \le i \le n$.

Let h_1, h_2,…, h_m denote the hash value for messages V_1, V_2,…, V_m, that is the hash value for messages V_1, V_2,…, V_m, is generated as follows:

$$h_i = H(V_i) = \prod_{j=1}^{n} g_j^{v_{ij}} \bmod p, 1 \le i \le m$$

This hash function is homomorphic. It has the additive homomorphism, because for arbitrary $X, Y \in F_q^n$, we have

$$\begin{aligned} H(X+Y) &= \prod_{i=1}^{n} g_i^{(x_i+y_i)} \\ &= \prod_{i=1}^{n} g_i^{x_i} \cdot g_i^{y_i} = \left(\prod_{i=1}^{n} g_i^{x_i}\right)\left(\prod_{i=1}^{n} g_i^{y_i}\right) \\ &= H(X) \cdot H(Y) \end{aligned}$$

Therefore, for arbitrary network node receives a message $W = (w_1,\ldots, w_n)$, $\alpha_1,\ldots, \alpha_m$ is a set of linearly independent vectors, then the hash value of the message $W = \sum_{j=1}^{m} \alpha_j V_j$ is generated as follows:

$$\begin{aligned} H(W) &= \prod_{j=1}^{n} g_j^{w_j} \bmod p \\ &= \prod_{j=1}^{n} g_j^{\sum_{i=1}^{m} \alpha_i v_{i,j}} \bmod p = \prod_{j=1}^{n}\prod_{i=1}^{m} g_j^{\alpha_i v_{i,j}} \bmod p \\ &= \prod_{i=1}^{m} \left(\prod_{j=1}^{n} g_j^{v_{i,j}} \bmod p\right)^{\alpha_j} \bmod p \\ &= \prod_{i=1}^{m} h_i^{\alpha_i} \end{aligned}$$

III. NDN Content Poisoning Attack

This section describes content poisoning attack scenarios.

Content poisoning is an attack whereby adversary injects fake content into router caches. To be specific, the adversary attempts to inject fake content or modify the contents of the transmission in NDN, which will seriously interfere with the communications between the publisher and the receiver, in order to destroy the integrity of the content package. The purpose of this attack is to make the legitimate nodes can't identify the false content in the NDN. Due to the transmission mode of NDN, these polluted contents will be continuously spread, so that make the whole network traffic is contaminated.

In this paper, we consider a pro-active content poisoning, i.e., the adversary introducing malicious data into the contents, and injects fake content with the same name into router caches. Fake content can be injected into the network via malicious routers or end-nodes. For example, consider an adversary targeting a specific router R. Assuming that malicious producer sends a fake content to R which is promptly cached. Consequently, R is pre-polluted with fake content. If the router R receives a real interest, it would send the fake content.

IV. Secure Network Coding against Content Poisoning Attacks in NDN

In this paper, we consider a NDN network topology as shown in Fig. 1. It consists of A, t_1,…, t_k and a number of forwarders, where A and t_1,…, t_k can be content publisher and content receiver in NDN. To facilitate the description, in this paper, A is a content publisher, t_1,…, t_k are multiple content receivers. Content publishers produced messages in the form of the following:

$$\mathbf{V} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{pmatrix}$$

Let each source message V_i is randomly picked from a finite field F_q, where prime q is a pre-determined security parameter. So, each source message V_i for i =1,…, m can be regarded as a row vector such as $V_i = (v_{i1},\ldots, v_{in})$, where $v_{ij} \in F_q$ for j =1,…, n denote the codewords.

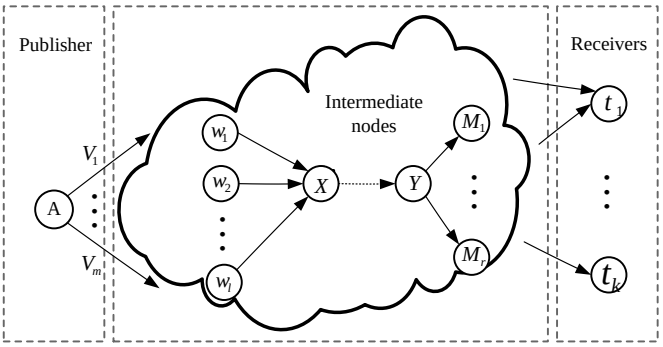


Fig. 1. A NDN network topology.

In this paper, our secure network coding based on homomorphic signature is mainly composed of four parts: Setup, Sign, Combine and Verify.

- **Setup**.

1) Given the system parameters 1^τ, m, n, p, q, g, where p and q are prime, and $q > 2^\tau$. Let $o(g)$ denotes the order of g in the field F_p of prime order, F_p is a subfield of F_p.
2) Choose n+1 random numbers $u_i(i=0, 1,\ldots, n)$ from F_p such that

$$sk = \{u_i \in F_q \mid i = 0,1,2,\ldots,n\},$$

and compute

$$pk = \{p_i = g^{u_i} \mid i = 0,1,2,\ldots,n\}.$$

- **Sign**.

To generate the signature tag using the secret key for the i-th basis vector $V_i = (v_{i1},\ldots,v_{in}) \in F_q$ belonging to the forwarding generation, the content publisher works as follows:

1) Choose a unique generation identifier id from $\{0,1\}^\tau$ arbitrarily, which are used to scramble the above initial secret key sk to S, i.e.,

$$S = (s_0, s_1,\ldots, s_n) \in F_q$$

where

$$s_0 = u_0$$

and

$$s_i = u_i + id \cdot u_0, (i = 1,2,\ldots,n)$$

2) Compute the signature tag of V_i by:

$$\sigma_i = \frac{s_i - \sum_{j=1}^{n} s_j v_{ij}}{s_0} \in F_q, (1 \le i \le m)$$

That is, V_i is signed as $\upsilon_i = (V_i, \sigma_i)$.

- **Combine**.

After receiving l forwarding vectors $\upsilon_i = (V_i, \sigma_i)(i=1,2,\ldots, l)$, an intermediate node outputs:

$$\boldsymbol{\upsilon} = (W, \sigma_W) = \sum_{i=1}^{l} \alpha_i \upsilon_i = (\sum_{i=1}^{l} \alpha_i V_i, \sum_{i=1}^{l} \alpha_i \sigma_i)$$

where α_1, α_2,…, α_l is code coefficients which are generated by the seed α_X of the node X received (as show in Fig. 1), and X send the seeds and message packets $\boldsymbol{\upsilon}$ to all descending node.

- **Verify**.

Given a forwarding vector $\boldsymbol{\upsilon} = (W, \sigma_W)$ belonging to the generation denoted by id, $W = \sum_{i=1}^{l} \alpha_i V_i$, a verifier (including the receivers) computes

$$H_1 = g_0^{\sigma_W} \cdot H(W)$$

$$H_2 = \prod_{i=1}^{l} g_i^{\alpha_i} \bmod p$$

and checks if $\frac{H_1}{H_2} = 1$. where

$$g_0 = p_0, g_i = p_i \cdot p_0^{id} (i = 1,2,\ldots,n)$$

If $\frac{H_1}{H_2} = 1$ holds, the message is through the verification, otherwise, the verifier discard it.

V. Correctness and Security

A. Correctness

This section shows the correctness property of the constructed scheme.

Theorem 1: $W = (w_1,\ldots, w_n)$ is a combination of the received packets in a node, i.e.,

$$W = \sum_{i=1}^{l} \alpha_i V_i$$

and

$$H_1 = g_0^{\sigma_W} \cdot H(W),\ H_2 = \prod_{i=1}^{l} g_i^{\alpha_i} \bmod p$$

If $\frac{H_1}{H_2} = 1$, W is not polluted.

Proof*:* Let

$$H(W) = \prod_{i=1}^{n} g_i^{w_i} \bmod p$$

We have

$$g_0^{\sigma_i} \cdot H(V_i) = g_0^{\sigma_i} \cdot \prod_{j=1}^{n} g_i^{v_{i,j}} \bmod p$$

$$= g^{s_0 \sigma_i} g^{\sum_{j=1}^{n} s_i v_{i,j}} \bmod p$$

$$= g^{s_0 (s_i - \sum_{j=1}^{n} s_j v_{i,j}) s_0^{-1}} g^{\sum_{j=1}^{n} s_j v_{i,j}} \bmod p$$

$$= g^{s_i} \bmod p = g_i$$

Due to $W = \sum_{i=1}^{l} \alpha_i V_i$, thus

$$H_1 = g_0^{\sigma_W} \cdot H(W) = g_0^{\sigma_W} \cdot \prod_{j=1}^{n} g_j^{w_j} \bmod p$$

$$= g_0^{\sum_{i=1}^{l} \alpha_i \sigma_i} \cdot \prod_{j=1}^{n} g_j^{\sum_{i=1}^{l} \alpha_i v_{ij}} \bmod p$$

$$= \prod_{i=1}^{l} g^{\alpha_i s_0 \sigma_i} \cdot \prod_{i=1}^{l} g^{\alpha_i \sum_{j=1}^{n} s_i v_{ij}} \bmod p$$

$$= \prod_{i=1}^{l} g^{\alpha_i (s_0 \sigma_i + \sum_{j=1}^{n} s_i v_{ij})} \bmod p$$

$$= \prod_{i=1}^{l} g^{\alpha_i s_i} \bmod p$$

$$= \prod_{i=1}^{l} g_i^{\alpha_i} \bmod p$$

And by the known public parameters, we have $H_2 = \prod_{i=1}^{l} g_i^{\alpha_i} \bmod p$, and then $\frac{H_1}{H_2} = 1$. This demonstrates the correctness of the scheme.

B. Security

In this section, we show that our scheme is secure against Intra/Inter-GPAs respectively. First, we define the contaminated message:

Definition 1: If W is a contaminated message (or fake content) in the id -th generation, such that this message is not belong to the linear subspace of id -th generation source message.i.e., $W \notin span\{V_1^{(id)}, \ldots, V_m^{(id)}\}$,where $V_1^{(id)}, \ldots, V_m^{(id)}$ denote all the source message of the id -th generation, $span\{V_1^{(id)}, \ldots, V_m^{(id)}\}$ denote the linear subspace of $V_1^{(id)}, \ldots, V_m^{(id)}$.

We prove the security of this algorithm in two ways as follows. Next, we will prove the security of this algorithm for Intra-GPAs and Inter-GPAs.

C. The Security for Intra-GPAs

In this section, we consider all the messages are from the *id*-th generation.

Theorem 2: $W = (w_1, \ldots, w_n)$ is a combination of the received packets in one node, i.e., $W = \sum_{i=1}^{l} \alpha_i V_i$, and $H_1 = g_0^{\sigma_W} \cdot H(W)$, $H_2 = \prod_{i=1}^{l} g_i^{\alpha_i}$, W is not polluted if and only if $\frac{H_1}{H_2} = 1$.

Proof: If W is not polluted, by the Definition 1, W is a linear combination of the source message, and by the correctness proof in above section *A*, $\frac{H_1}{H_2} = 1$. Therefore, we mainly prove if $\frac{H_1}{H_2} = 1$, W is not polluted.

Using reduction to absurdity, we assum that the adversary $\mathcal{A}$ has found a fake content W that make $\frac{H_1}{H_2} = 1$, we discuss the possibility in this case.

1) Given the fake content $W = (w_1, \ldots, w_n)$ that make the equation $\frac{H_1}{H_2} = 1$ holds, then we have:

$$g_0^{\sigma_W} \cdot \prod_{i=1}^{n} g_i^{w_i} = \prod_{i=1}^{l} g_i^{\alpha_i}$$

This is equivalent to solve the problem of discrete logarithm.

2) Given σ_W , computes $W \notin \text{span}\{V_1, V_2, ..., V_m\}$ that make the equation holds, i.e.,

$$g_0^{\sigma_W} \cdot \prod_{i=1}^{n} g_i^{w_i} = \prod_{i=1}^{l} g_i^{\alpha_i}$$

We assume that the n-1 elements before $W = (w_1, \ldots, w_n)$ have been confirmed, thus the last element w_n is computed as follows:

$$g_n^{w_n} = \frac{\prod_{i=1}^{l} g_i^{\alpha_i}}{g_0^{\sigma_W} \cdot \prod_{i=1}^{n-1} g_i^{w_i}}$$

Obviously, if we want to compute w_n, we still solve the discrete logarithm problem. Therefore, the adversary $\mathcal{A}$ cannot construct a message $W \notin \text{span}\{V_1^{(id)}, V_2^{(id)}, ..., V_m^{(id)}\}$, so that $g_0^{\sigma_W} \cdot \prod_{i=1}^{n} g_i^{w_i} = \prod_{i=1}^{l} g_i^{\alpha_i}$. So, as long as $g_0^{\sigma_W} \cdot \prod_{i=1}^{n} g_i^{w_i} = \prod_{i=1}^{l} g_i^{\alpha_i}$, we can consider W as a unpolluted message.

D. The Security for Inter-GPAs

The adversary $\mathcal{A}$ can take advantage of a valid message W of the k-th generation, to act as the message of the k+i-th generation. Because this message does not belong to the k+i-th generation, so it is clearly a fake content. But the signature of this message is calculated by the source (calculated in the k-th generation), so this message can passed the verification of intermediate nodes, so that it can successfully forge a message of the k+i-th generation, and destroy the transmission of the k+i-th generation message. Next, we will prove this method does not pose a threat for our scheme.

We consider a message W of the k-th generation, where $\sigma_W^{(k)}$ denote the signature of the message W in the k-th generation. By the construction of the signature in Section IV, we have

$$\sigma_W^{(k)} = \frac{(s_i - \sum_{j=1}^{n} w_j s_j^{(k)})}{s_0} \bmod q, 1 \le i \le m$$

where $s_i^{(k)} = u_i + k \cdot u_0$, s_i denote the private key of the k-th generation, so we have:

$$S^{(k)} = (s_0^{(k)}, s_1^{(k)}, \ldots, s_n^{(k)})$$
$$= (u_0^{(k)} + k \cdot u_0, u_1^{(k)} + k \cdot u_0, \ldots, u_n^{(k)} + k \cdot u_0)$$

If an adversary $\mathcal{A}$ take advantage of this message W of the k-th generation, to forge a message of the *id*-th generation, assume that the private key of the *id*-th generation

$s_i^{(k)} (i = 0,1,\ldots,n)$, and

$$S^{(id)} = (s_0^{(id)}, s_1^{(id)}, \ldots, s_n^{(id)})$$
$$= (u_0^{(id)} + id \cdot u_0, u_1^{(id)} + id \cdot u_0, \ldots, u_n^{(id)} + id \cdot u_0)$$

Obviously, $S^{(id)} \neq S^{(k)}$, therefore, when the intermediate nodes verify this message, have:

$$g_0^{\sigma_W^{(k)}} \cdot \prod_{i=1}^{n} g_i^{w_i} = g_0^{\sigma_W^{(k)}} \cdot \prod_{i=1}^{n} g^{s_i^{(k)} \cdot w_i}$$
$$= g^{s_0 \cdot (s_i^{(k)} - \sum_{j=1}^{n} w_j \cdot s_j) \cdot s_0^{-1}} \cdot g^{\sum_{i=1}^{n} s_j^{(k)} \cdot w_j}$$
$$= g^{s_i^{(k)}} = g^{u_i^{(k)}} \cdot g^{id \cdot u_0}$$

For the given *id*, by the above proof, the possibility of the equation $g_0^{\sigma_W^{(k)}} \cdot \prod_{i=1}^{n} g_i^{w_i} = g^{u_i^{(k)}} \cdot g^{id \cdot u_0} = \prod_{i=1}^{l} g_i^{\alpha_i}$ can be ignored. As a result, we consider $g^{u_i^{(k)}} \cdot g^{id \cdot u_0} \neq \prod_{i=1}^{l} g_i^{\alpha_i}$, i.e., the message *W* cannot be verified.

In conclusion, our scheme is secure against Intra/Inter-GPAs respectively.

VI. Conclusion

Some researches [5]-[7] shows that the signature is an effective means to solve the content poisoning attack in NDN. In this paper, we try to integrating network coding to NDN, using a secure network coding method which is based on homomorphic signature to solve a potential attacks — content poisoning attack in NDN, while enhancing the data transmission efficiency, improve the security of network data. Of course, we proved content signatures provide an effective means to detect content poisoning attack only in theoretically.

Currently NDN network and network coding have carried out extensive research coding in theory and practice [15]-[18], and have confirmed from the theoretical model that using network coding can improve network performance, but the verification steps or simulated environment, mostly based on assumptions or idealized model still have a gap with the actual application environment, so some conclusions have limitations. In addition, the process is mostly quantitative research. Therefore, building application evaluation model and practical system under NDN network combined with NC, remains to be further researched.

Acknowledgment

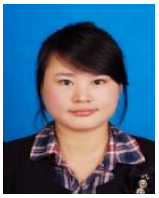
The research work was supported by National Natural Science Foundation of China under Grant No. 61461027 and No.61462060, and supported by Science and technology program of Gansu Province under Grant No. 1308RJZA277 and No.145RJZA078.

References

[1] J. L. Pan *et al.*, "A survey of the research on future internet architectures," *Commun. Magazine*, vol. 49, no. 7, pp. 26-36, 2011.
[2] V. Jacobson, "Networking named content," in *Proc. the 5th Int. Conf. on Emerging Networking Experiments and Technologies*, 2009.
[3] X. G. Zhang *et al.*, "Future network-the challenges and application of the content center network," *Telecom Science*, vol. 29, no. 8, 2013.
[4] M. Conti, P. Gasti, and M. Teoli, "A lightweight mechanism for detection of cache pollution attacks in named data networking," *Computer Networks*, vol. 57, no. 16, pp. 3178-3191, 2013.
[5] C. Ghali, G. Tsudik, and E. Uzun, "Needle in a haystack: Mitigating content poisoning in named-data networking," in *Proc. NDSS Workshop on Security of Emerging Networking Technologies*, 2014.
[6] L. X. Zhang, "Named data networking (NDN) project," Relatório Técnico NDN-0001, Xerox Palo Alto Research Center-PARC, 2010.
[7] P. Gasti, "Dos and DDOS in named data networking," in *Proc. 22nd Int. Conference on Computer Communications and Networks*, 2013.
[8] M. N. Krohn, M. J. Freedman, and D. Mazieres, "On-the-fly verification of rate less erasure codes for efficient content distribution," in *Proc. IEEE Symposium on Security and Privacy*, 2004.
[9] Q. M. Li, D. M. Chiu, and J. C. S. Lui, "On the practical and security issues of batch content distribution via network coding," in *Proc. 14th IEEE International Conference on Network Protocols*, 2006.
[10] F. Zhao, "Signatures for content distribution with network coding," in *Proc. IEEE International Symposium on Information Theory*, 2007.
[11] Z. Yu, "An efficient signature-based scheme for securing network coding against pollution attacks," in *Proc. the 27th Conference on Computer Communications*, 2008.
[12] R. Gennaro, "Secure network coding over the integers," *Public Key Cryptography*, Springer Berlin Heidelberg, 2010, pp. 142-160.
[13] G. J. Liu *et al.*, "Secure network coding against intra/inter-generation pollution attacks," *Communications*, vol. 10, no. 8, pp. 100-110, 2013.
[14] Y. J. Zhou, H. Li, and J. F. Ma, "Secure network coding against the contamination and eavesdropping adversaries," arXiv preprint arXiv: 0805.2286, 2008.
[15] K. Lei, "Exploring the benefits of introducing network coding into named data networking," in *Proc. 17th International Conference on Computational Science and Engineering*, 2014, pp. 563-568.
[16] S. Miyake and H. Asaeda, "Network coding and its application to content centric networking," 2013.
[17] M. J. Montpetit *et al.*, "Network coding meets information-centric networking: an architectural case for information dispersion through native network coding," in *Proc. the Workshop on Emerging Name Oriented Mobile Networking Design-Architecture, Algorithms, and Applications*, 2012, pp. 31-36.
[18] Q. H. Wu, Z. Y. Li, and G. G. Xie, "Coding cache: Multipath-aware CCN cache with network coding," in *Proc. the 3rd ACM SIGCOMM Workshop on Information-Centric Networking*, 2013, pp. 41-42.

Tao Feng received the B.A and M.S. degrees from Gansu University of Technology, and the Ph.D. degree from Computer Network and Information Security Laboratory, Ministry of Education, Xidian University, China.

He was a visiting scholar of the Information Security Lab in Singapore Management University. He is currently the principal scientist of Computer Network and Information Security Lab in Lanzhou University of Technology. His interests include provable security protocol theory, wireless and mobile network security. He has published more than 50 papers and 4 patents.



Xiaomei Ma was born in 1988. She is a master degree candidate now at Lanzhou University of Technology. Her major research interests focus on named data networks security.

Xian Guo was born in 1971. He has a Ph.D. degree and is now a professor as well as a supervisor of postgraduate with Lanzhou University of Technology. His major research interests focus on mobile ad hoc networks security.

Jing Wang was born in 1984. He is a Ph.D. candidate in Lanzhou University of Technology. His major research interests focus on industrial networking security.