Journal of Network and Systems Management (2023) 31:13
https://doi.org/10.1007/s10922-022-09689-x

RESEARCH

An Advanced Hierarchical Identity-Based Security Mechanism by Blockchain in Named Data Networking

Bing Li[1] · **Maode Ma**[2]

Received: 18 April 2022 / Revised: 15 August 2022 / Accepted: 20 September 2022 /
Published online: 17 November 2022

Abstract

Named data networking (NDN) has been viewed as a promising future Internet architecture due to its data-centric design. It requires a new security model that is orienting data but not devices. In this paper, an advanced hierarchical identity-based security mechanism by blockchain (AHISM-B) is to be proposed for the NDN networks. On one hand, the hierarchical identity-based cryptology is used to bind the data name to a public key. The valid public parameters would be requested by consumers with the Interest packets so that consumers would compose producers' public keys to authenticate producers and verify the integrity of the Data packets. On the other hand, a blockchain is employed to manage public parameters to avoid catastrophes due to a single node failure. Both of the security proof result and the formal validation result indicate that the proposed AHISM-B is secure. Moreover, the simulation results show that the performance of our AHISM-B outperforms that of the classic NDN scheme. Especially, the average response delay of the AHISM-B scheme is less by 8% than that of the classic NDN scheme. With the increase of the average arrival rate of Interest packets, the advantage of the AHISM-B could be enhanced further to 11%.

Keywords Named data networking · Security · Blockchain · Hierarchical identity-based cryptography

✉ Maode Ma
acadmmd@gmail.com

Bing Li
libingice@szu.edu.cn

[1] Shenzhen University, Nanhai Ave 3688, Shenzhen 518060, Guangdong, People's Republic of China

[2] College of Engineering, Qatar University, P. O. Box 2713, Doha, Qatar

1 Introduction

Named data networking (NDN) [1] has been viewed as a promising future Internet architecture because its data-centric design has been proved with more advantages compared to the device-centric design of the traditional IP network. The data in the NDNs will be accessed by their names rather than the IP addresses of the hosts, which hold the data. The users of data are consumers, who request data according to data names using Interest packets. The requested data would be encapsulated in Data packets by data sources, which are producers. All the routers are allowed to cache Data packets so that they are able to reply consumers' requests directly. As a result, the load of producers can be alleviated and the efficiency of the data distribution can be enhanced largely.

The data-centric character results in new security requirements for secure NDN communication [2–4]. Due to the device-centric design, the traditional IP network optionally requires a secure session to address the security issue. In a secure session, an authentication will be performed by a receiver to authenticate a sender [5]. Different from traditional IP networks, NDN pays more attention to secure data. Consumers will not care who has replied to their data requests. However, they mainly concentrate on the security of the received Data packets. Particularly, they require that the Data packets must be published by an authenticated producer without being modified by others. Therefore, the NDN is facing the demands of the data-oriented authentication, which holds two respects, including the data source authentication and the data integrity. The data source authentication ensures that the received Data packets are published by the authenticated producers no matter which routers they are replied by. The data integrity ensures that the received Data packets can't be changed by attackers.

In order to support the data-oriented authentication service, the NDN requires that a signature must be encapsulated in a Data packet to establish a trust model [6]. The producer would sign over the Data packet to obtain a signature. Both the location of the producer's public key and the signature value would be included in the *Signature* filed of the Data packet. As a result, consumers could retrieve producers' public keys to verify the Data packet for the data-oriented authentication. However, the trust model works based on two assumptions: (1) there is a mapping from the data name to the producer's public key. (2) the producer's public key could be retrieved easily for each consumer. But in a real network environment, the two assumptions are not satisfied easily. Firstly, in a Data packet, the data name is recorded in the *Name* field and the producer's public key is indicated in the *key locator* field of the *Signature* portion. There is no scheme to guarantee that the public key fetched according to the *key locator* is the public key of the producer who has published the Data packet named by the data name. The mismatch between the data name and the producer's public key may be utilized by an attacker to camouflage an authenticated producer to publish false Data packet. The attacker could use its private key to sign the false Data packet that has the right data name to construct a false signature and then reply a consumer with the false Data packet that encapsulates the right data name, the false data, the false

signature and the false key locator indicating the location of the attacker's public key. Therefore, the consumer would verify the Data packet using the attacker's public key and be deceived that the false Data packet would have been published by an authenticated producer. Secondly, in order to verify the Data packet, the retrieval of producers' public keys must be convenient for consumers. The traditional Public Key Infrastructure (PKI) seems to be a candidate solution to manage the public key certification. But in the context of PKI, a compromise of the Certificate Authority (CA) would break the trust in all certificates issued by the CA and its descendants [7]. Therefore, a decentralized solution for the public key distribution should be explored to efficiently relieve the risk.

Moreover, the data-oriented authentication is the basic security service, which is essentially required by other security solutions For example, works in [8, 9] have designed a reputation-based blockchain mechanism to tackle poisoning attacks in NDN networks. In order to update the reputation-value of the cache store, it is assumed that the consumers could verify the received Data packets, i.e., data-oriented authentication. Similarly, Ref. [10] has also employed the data-oriented authentication at all the consumers. A warning Interest packet would be sent to detour attackers when an unauthenticated Data packet is found. Therefore, it is popular to employ the data-oriented authentication to prevent other security attacks in the NDN networks.

In this paper, we propose an advanced hierarchical identity-based security mechanism by blockchain (AHISM-B) for NDN networks with the aim to satisfy the above two assumptions to realize the data-oriented authentication. Firstly, the hierarchical identity-based cryptography (HIBC) is used to guarantee the mapping from the data name to the producer's public key. Secondly, the blockchain is employed to manage public parameters, which are important components of producers' public keys, to avoid the catastrophes due to the single node failure. Moreover, all the producers located at the same domain would share the same public parameters. Therefore, the number of the public parameters would be much smaller than the number of the producers' public keys so that the length of the blockchain could be shorter to make the overhead of the blockchain network smaller. By the AHISM-B, consumers could request the valid public parameters from the blockchain as they request data from producers and then compose producers' public keys to authenticate producers and verify the integrity of the Data packets. Compared to our previous work which has proposed the scheme of hierarchical identity-based security mechanism by blockchain (HISM-B) [11], the AHISM-B scheme employs only one signature in the Data packet so as to take less bandwidth and maintain less response delay.

Our main contributions in this paper can be summarized as follows. (1) A new proposal, AHISM-B, has been presented, which could provide security service for the data source authentication and data integrity protection. By the AHISM-B, the HIBC has been employed to bind the data name to the producer's public key while the blockchain has been used to achieve the distributed management of producers' public keys. (2) Both of the security proof and validation on the AHISM-B have been conducted. Their results show that the AHISM-B is SAFE. (3) The simulation experiments have been carried out to evaluate the performance of the AHISM-B. The results indicate that the average response delay at consumers could be less than

that by the classic NDN scheme and the HISM-B scheme. Moreover, the number of satisfied Interest packets is no less than that by the classic NDN scheme and the HISM-B scheme.

The rest of the paper is organized as follows. Sections 2 and 3 would exhibit the related work and the network model. Section 4 proposes our AHISM-B scheme. Section 5 would present formal validation for the AHISM-B. Section 6 evaluates the performance of the AHISM-B. Section 7 concludes the paper with a summary.

2 Related Work

Some NDN security schemes have been designed to provide the security service including data integrity and data source authentication. Some proposals target to satisfy the assumption (1) in Sect. 1. In [12], the Identity-Based Cryptography (IBC) [13] has been used to generate keys for the producers to map the data name to the public key. The data name, the prefix of the data name, or the identity of the producer, would be employed directly as a public key. In [14], a security extension works based on the Hierarchical Identity-Based Cryptography (HIBC) [13] has been presented to reflect the hierarchical network structure. In [15], the field of *PublisherPublicKeyDigest* (PPKD) has been made mandatory in the Interest packet. The software APP_C has been installed at the consumer to provide the root public keys. However, the above proposals have not mentioned how to manage the public keys or certifications.

Moreover, some protocols have been proposed to manage public keys used in the NDN networks. In [16], the public-key authentication protocol for NDN has been stated. It works at a designated host to store and provide the certificate. The certificate would bind the producer identifier to its public key. CertCoalesce certificates are proposed in [17] to efficiently manage virtually unlimited pools of short-term certificates. The validity periods of the certificates have been reduced to hours to eliminate the certificate revocation requirement. Ref. [18] has presented an overview of the security mechanism in the NDN. The trust policy, which is specified by the NDN application to limit the signing key with specific name, has been encapsulated in the Data packet. The signing key would share the same name prefix with the data that would be signed by the signing key. The security mechanism in [18] is called the classic NDN scheme in this paper. The DCAuth scheme works based on the suspension chain model to integrate certificate collection and packet forwarding [19]. It has merged the hash-based self-certifying names with hierarchical naming. In [20], hash chains have been used to authenticate data source for a large size data object. In [21], a Lightweight Verification Mechanism based on a Pre-cached Hash value of Requested Content (LVM-PHRC) has been proposed. The multiparty authentication bas been argued in [22] over NDN. Each party has obtained identity with a certificate issued by the system. Signers verify a signature generated by the producer's identity private key and publish new signatures for the data object. Multiple signatures would be aggregated, which would be verified at the consumer. A collaborative, secure and efficient content validation protection (CSEVP) framework has been

presented in [23] to implement a multi-router collaborative content authentication. A certificate, which has associated a producer's public key with the content name prefix, would be delivered with the content chunks by the producer. As a result, all the forwarding routers could verify a Data packet, which has included the producer signature. However, these proposals have mainly relied on a trust anchor to issue the certificates. Once the trust anchor e.g. CA, fails, all the consumers and producers would be exposed to security threats.

In summary, the above proposals cannot satisfy the assumption (2) mentioned in Sect. 1. In order to avoid the paralysation due to the single point failure, the works in [24, 25] have used a blockchain to manage public keys in NDN networks. Since the blockchain is a decentralized solution, they could guarantee that the public keys could be retrieved easily. However, these proposals cannot satisfy the assumption (1) because they have not provided a mapping from the data name to the public key. In [26], an Access Control (AC) framework based on blockchain to provide Data-oriented authentication has been proposed, which exploits transaction and smart contracts to provide a trusted and neutral environment in information-centric networks. A special node, a data dam blockchain node, has been designed to locally control registration and restrict data flow. But this framework could result in additional traffic load due to the AC. In [27], an efficient certificateless group signature scheme has been presented. A gateway would undertake the responsibility to assist the authenticated producer in generating a compete signature for the data content. By the solutions in [24–26], the blockchain must store the public keys for all the users so that the length of the chain would be very long. It could cause inefficient queries for users' public keys. All of the above reviewed solutions are summarized in Table 1.

An efficient security solution is urgently required to realize the data-oriented authentication in a NDN network. The data-oriented authentication is critical to provide important security service. Once authentication is vulnerable, other security services may be threatened. Since the existing proposals cannot provide data-oriented authentication service to satisfy the two assumptions mentioned in Sect. 1 and avoid additional traffic load due to the AC, further attentions should be paid to the authentication issues to produce an efficient solution.

Instead of one signature required in [18], the HISM-B scheme in our previous work [11] has used two signatures in the Data packets to satisfy the two assumptions. However, two signatures require a producer to sign twice and a consumer to verify twice so that a consumer would suffer from the higher response delay. In order to satisfy the two assumptions with less additional costs, in this paper, we plan to propose a novel security mechanism, named AHISM-B, by which only one signature is required in a Data packet to achieve the data-oriented authentication while the two assumptions can be satisfied. Proved by the simulation results, the AHISM-B scheme could hold the same security properties as the HISM-B scheme and presents a lower response delay.

Table 1 Summary of existing related works

Proposals number	Proposal description	Satisfying assumption (1)	Satisfying assumption (2)		Independence of AC
			Key management	Independence of CA	
Ref. [12, 14, 15]	IBC, HIBC or key digest in interest packet to bind the data name to producer's public key	✓	×	×	✓
Ref [16, 17]	PKI for the certificate management or short term certificates	×	✓	×	✓
Ref. [18–23]	Hash-based method and the certificate to bind keys and content name prefixes	✓	✓	×	✓
Ref. [24, 25]	Blockchain for key management	×	✓	✓	✓
Ref. [26, 27]	Access control for data packets	✓	✓	✓	×

3 Network Model

The network model under the study is shown in Fig. 1. There are four types of entities including user hosts, data sources, routers and special servers (Information Service Entities, ISEs). In this network, the user hosts would play the roles of consumers, which would send Interest packets to request named data. The data sources are the producers, which would generate Data packets to reply to the request from the consumers. All routers have the forwarding function to deliver Interest packets and Data packets. They also have the response functions to reply to the requests using their cached Data packets. The ISEs and some designated routers would take the role of private key generator (PKG) to generate key pairs including private keys and public keys for producers. With the four types of entities, the network can be modelled as an integration of two kinds of networks, i.e., one blockchain network and one secure NDN network. On one hand, the blockchain network is a multi-domain network, where an ISE is deployed in each domain. It would manage the cryptography information, e.g., the public parameter and its validity period. Each block in the blockchain would bind the domain name to its cryptography information to response to the request from the NDN network. On the other hand, the secure NDN network would be responsible for distribution of the named data with the data-oriented authentication service. The ISEs and some designated routers working as the PKGs, provide the security service together at their located domains. The producers would fetch the producer's private key from the PKGs while the customers would retrieve

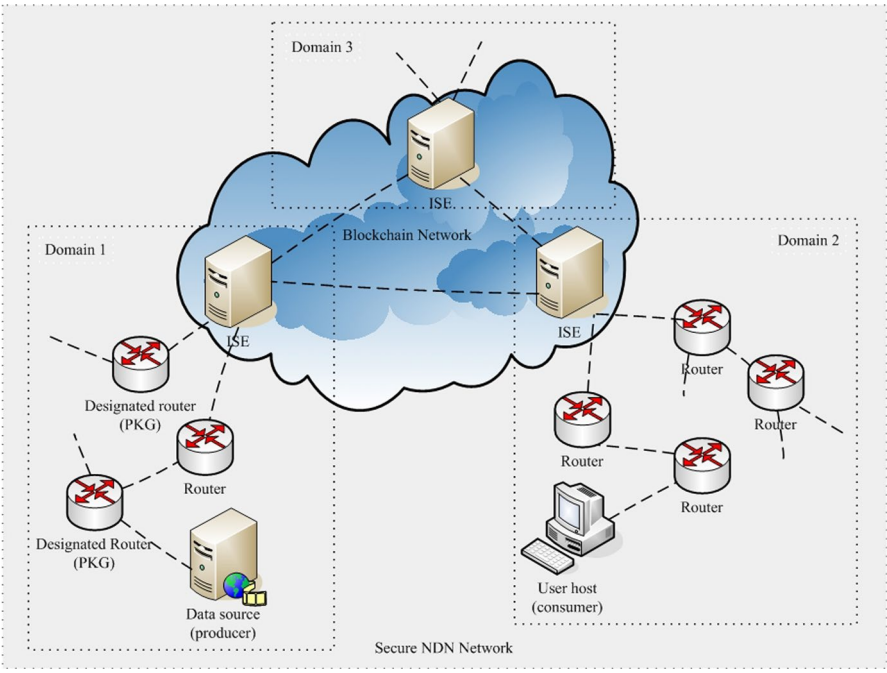

Fig. 1 Network model

the public parameters from the ISEs. With the help of producers' private keys and public parameters, the Data packet would be signed at the producer and be verified at the customer to guarantee the data source authentication and the data integrity.

3.1 HIBC

The HIBC algorithm is employed to generate cryptographical elements required by the data-oriented authentication in the NDN networks. An ISE and some designated routers are organized in a hierarchy to play the role of the PKG in each domain. They function for the producer authentication and the private key generation for the authenticated producers. The private keys would be distributed to the producers from the closest PKG over a secure channel. The way to construct a secure channel between a producer and its PKG is beyond the scope of this paper.

3.2 Data Naming

Similarly to Ref. [6], the AHISM-B scheme assumes hierarchically structured naming scheme. The hierarchical name is composed of three fields, which begin with the string '*//*'. The first field is the prefix that indicates which class the name belongs to. The second field is the identifier information and the third one is the data information. Each field is organized hierarchically with one or more components, delimited by the character '*/*', similar to the Uniform Resource Locator (URL). In the model, the public parameters are viewed as special data so that data names are divided into two classes. The first one is to name the data published by producers and the second one is to name the public parameters published by the ISEs.

For the first class, the prefix of the name is '*//ndn/data*', which indicates that the named data are published by a producer. Therefore, its identifier information indicates the routing identifier of a producer. And the data information usually includes the file name, the file version and the segment number. One example of the name is shown in Fig. 2. A producer, rather than an ISE, publishes the named data if the name begins with '*//ndn/data*'. And the producer could be routed using '*szu.edu.cn/et*'. Here '*szu.edu.cn*' is the name of the domain where the producer is located. The published file and its version are '*course_cs.mp4*' and '*v1*' respectively. The segment number in the published file is '*s*1'. The second field of the data name, i.e., the producer's routing identifier, could be viewed as the producer's identity, i.e., ID_p, which would play an important role in the HIBC algorithm. The ID_p would become a part of the public key and is also used to calculate the secret of the private key by a PKG.

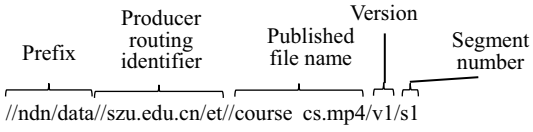

Fig. 2 Example of data names in class 1

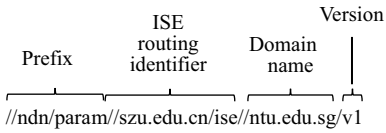

Fig. 3 Example of data names in class 2

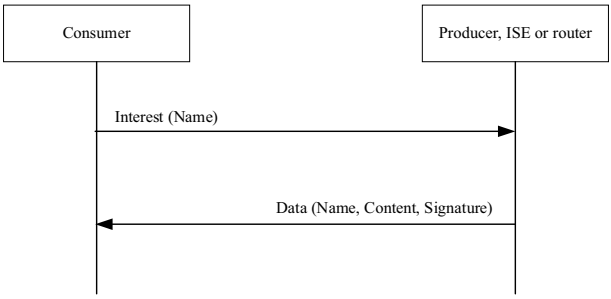

Fig. 4 Communication procedure in AHISM-B

For the second class, the prefix of the name is '*//ndn/params'*, which implies that the named data are the public parameters published by an ISE. Therefore, its identifier information indicates the routing identifier of an ISE. And the data information is the domain name and its parameter's version. One example is shown in Fig. 3. '*//szu.edu.cn/ise*' is the ISE routing identifier because the name begins with '*//ndn/params*'. '*ntu.edu.sg*' is the domain name and '*v1*' is the version of the public parameter. By the AHISM-B, the consumer would initiate an Interest packet with the data name of the second class when the public parameter cannot be found at its local cache to verify a Data packet. Take the data name, as shown in Fig. 3, for example. It states that a consumer locating in the domain '*szu.edu.cn*' requests the public parameter with version '*v1*' of the domain '*ntu.edu.sg*'.

4 The Proposed AHISM-B

The proposed AHISM-B scheme provides the data-oriented authentication service for the NDN networks. It consists of four phases including network initiation, Interest packet publication, Data packet publication, and Data packet verification. The network initiation phase takes charge of the key pair generation, the key pair distribution and the cryptography information management. The key pairs used by the data-oriented authentication would be generated by the PKGs and be distributed to the authenticated producers. The cryptography information would be managed by a blockchain. The Interest packet publication phase, the Data packet publication phase and the Data packet verification phase would directly serve the communication in the secure NDN as shown in Fig. 4. The consumers send the Interest packets to request while the producers, the ISEs and routers send the Data packets, as the responses. In the Interest packet publication, an Interest packet is published to

request named data according to the NDN application at the consumer or to request the valid public parameter according to the authentication requirement. In the Data packet publication phase, a Data packet is signed by the producer or the ISE using its private key. In the Data packet verification phase, a Data packet would be verified at the consumer using the public key of the producer or the ISE. If the public parameter is not available locally, the phase of Interest packet publication would be triggered to request the public parameter to the ISE.

4.1 Network Initiation

By the AHISM-B, two kinds of key pairs are required: (a) ISEs' key pairs, including ISEs' public keys and ISEs' private keys, and (b) producers' key pairs, including producers' public keys and producers' private keys. The PKGs are responsible for the generation of the key pairs. And then the blockchain is built to manage the public parameters which are parts of producers' public keys.

4.1.1 Generation of ISEs' Key Pairs

An ISE would take the duty of generation of the ISE's key pair, including the ISE's public key, PK_I, and the ISE's private key, SK_I. The algorithm for the key pair generation can be any algorithm that can provide high security strength. On one hand, the SK_I is kept secret strictly by the ISE and would be used to sign the cryptography information as described in Subsect. 4.3. On the other hand, the PK_I would be delivered to all the network entities at the same domain with the ISE over a secure channel.

4.1.2 Generation of Producers' Key Pairs

In a domain, the PKGs are organized in a hierarchy to generate the producers' key pairs, including the producer's public key, PK_p and the producer's private key, SK_p. The HIBC algorithm [13], as a generalisation of identity-based crypto to reflects an organisational hierarchy, is used, where meaningful identities are designed as public keys. The producer's public key is composed by the public parameter, *PARAM*, and the identifier of the producer, ID_p, while the producer's private key is compose by the *PARAM* and a secret of the producer, $SID_{p.}$. The ID_p refers to the routing identity of the producer, which is included in the second field of the data name. An ISE would act as the root PKG in a domain to generate a *PARAM* for the domain. The ISE or the designate router would generate the SID_p and distribute it to the producer. The way to generate producers' key pairs is shown as follows.

An ISE runs the root setup procedure of the HIBC algorithm to generate the *PARAM* and main session key, MSK_{root}, with the input value k as shown in (1). According to the security strength, the ISE specifies the validity period of the *PARAM* and the MSK_{root} as (t_1, t_2). It means that the *PARAM* and the MSK_{root} are considered as valid only in the time interval (t_1, t_2). The *PARAM* and k would be delivered to lower layer PKGs over a secure channel. The secure channel could be

an online channel or an offline channel. Since the lower layer PKGs and the ISE are located in the same domain, the secure channels usually have been configured by the domain administrator.

$$RootSetup(k) -> \left(PARAM, MSK_{root}\right) \tag{1}$$

The designate router, as the lower layer PKG, would generate its main session key, MSK_{lower}, in the lower layer setup procedure following (2). All the PKGs in the same domain would share the same initial input value k and $PARAM$.

$$LowerHierarchySetup(k) -> MSK_{lower} \tag{2}$$

After the setup procedure, the PKG could perform producer authentication and key generation for the authenticated producers locating at its layers. It calculates a secret of a private key for a producer, SID_p, according to (3) after the successful producer authentication. The MSK refers to MSK_{root} if the PKG is an ISE. Otherwise, it refers to MSK_{lower}. For an authenticated producer, its private key is composed by the $PARAM$ and the SID_p, and its public key is composed by the $PARAM$ and the ID_p. The producer's key pair would be used to guarantee the data-oriented authentication.

$$KeyGen\left(MSK, ID_p\right) -> SID_p \tag{3}$$

4.1.3 Management of Cryptography Information using Blockchain

A blockchain network would be maintained among the ISEs. The Hyperledger Fabric could be considered as a candidate infrastructure for the blockchain network. Each ISE would request to join in the blockchain network. The request would be checked by the nodes that have joined in the blockchain network. If it has been approved, the ISE would synchronize the block information and install a chaincode to become a new node in the blockchain. After joining in the blockchain network, the ISE would announce its domain information, including the $PARAM$ and its validity period. If the announcement has been approved by the consensus algorithm, a new block, which encapsulates the domain name, the $PARAM$ and its validity period, would be added into the blockchain. Since the blocks in the blockchain would been synchronized among all the ISEs that have been joined in the blockchain network, the ISE could obtain the $PARAM$ and its validity period of any domain from its local blockchain. There have been some solutions proposed to implement blockchain in NDN networks [28, 29] so that we need not to design communication details among ISEs.

4.2 Interest Packet Publication

As specified by Ref. [6], the field *Name* is compulsory in the Interest packet by our AHISM-B scheme. There are two conditions to initiate a new Interest packet at a consumer: (a) the NDN application at the upper layer requires data, and (b) there is no valid $PARAM$ to verify the received Data packet locally.

In condition (a), the field *Name* would encapsulate a data name of the first class shown in Subsect. 3.2, whose prefix is '*//ndn/data*'. As a result, the Interest packet would be used to request the data produced by a producer. Since the consumer and the producer may be located at different domains, the Interest packet could be delivered among domains.

By contrast, in the condition (b), the field *Name* would encapsulate a data name of the second class shown in Subsect. 3.2, whose prefix is '*//ndn/params*'. The Interest packet would be used to request the *PARAM* and its validity period known by the local ISE. The other fields of a data name are filled as follows. The second field would contain the routing identifier of the ISE who is in the same domain as the consumer is located. Therefore, the Interest packet could only be delivered in the current domain. The third field would include the name of the domain where the producer is located who publishes the verified Data packet. It indicates which valid *PARAM* a consumer is requesting.

4.3 Data Packet Publication

By the AHISM-B scheme, both producers and ISEs would publish Data packets as responses when they have received Interest packets. The fields of *Name*, *Content* and *Signature* are compulsory in the Data packet. The other fields could be added into the Data packet if necessary. Producers would respond to an Interest packet requesting the data named with the prefix of '*//ndn/data*'. And ISEs would respond to an Interest packet requesting the data named with the prefix of '*//ndn/params*'. As a result, the Data packets with the name prefix of '*//ndn/data*' could be delivered among different domains while Data packets with the name prefix of '*//ndn/params*' could only be delivered within one domain. There are two kinds of signatures in the Signature field, including the signature which is calculate by the ISE, σ_I, and the signature which is calculated by the producer, σ_p.

4.3.1 Publication by Producers

A producer would publish a Data packet when its local data is requested by a received Interest packet with the name prefix '*//ndn/data*'. Similar to Ref [6], the data name in the received Interest packet and the requested local data would be encapsulated into the *Name* field and the *Content* field respectively. And a signature, σ_p, is calculated according to (4) and is encapsulated into the Signature field. The details of the signature calculation are explained as follows. The message digest is calculated on the Name field and the Content field using a hash function. And then the message digest is encrypted by the producer's private key, i.e., SID_p and *PARAM*. The producer's private key has been delivered to the producer at the network initiation. The process of Data packet publication at a producer is shown in Fig. 5(a).

$$Sign\big(\big(SID_p, PARAM\big), (Name, Content)\big) -> \sigma_p \tag{4}$$

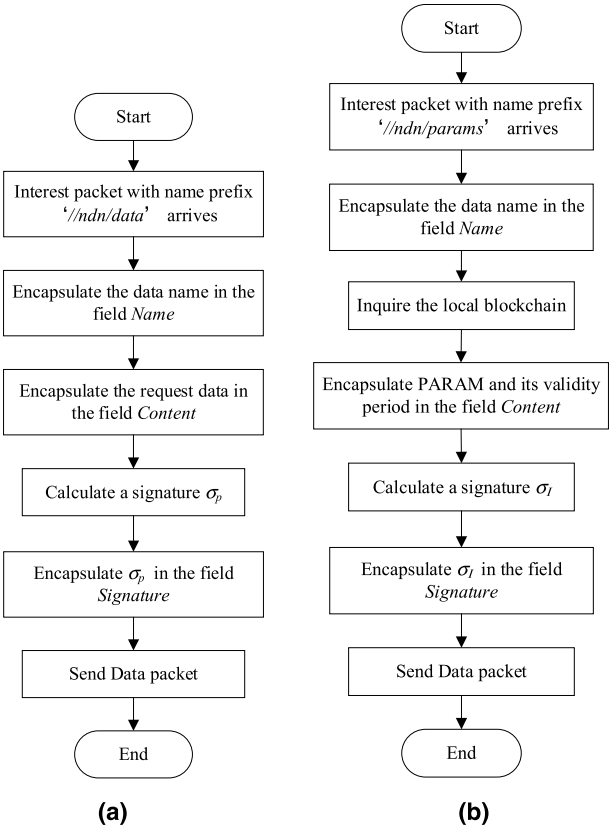

Fig. 5 Process to publish a data packet by a producer (**a**) and by an ISE (**b**)

The signature σ_p would be used to guarantee the data-oriented authentication. The valid producer's public key is required to verify the Data packet according to the signature σ_p.

4.3.2 Publication by ISEs

An ISE would publish a Data packet when the *PARAM* and its validity period are requested by a received Interest packet with the name prefix "*//ndn/params*". Similar to Ref. [6], the Name filed would encapsulate the data name in the received Interest packet. And then, an ISE would inquire the local blockchain to find the domain information according to the third field of the data name. And the found *PARAM* and its validity period (t_1, t_2) would be encapsulated in the *Content* field. At last, a signature, σ_I, would be calculated according to (5) by the ISE and encapsulated into the Signature field. The details of the signature calculation are explained as follows. The message digest is calculated on the *Name* field and the *Content* field using a hash function. Then the message digest is encrypted by the ISE's private key, i.e., SK_I.

The SK_I has been generated at the network initiation and has secretly been saved by the ISE. The process of Data packet publication at an ISE is shown in Fig. 5b.

$$Sign\big(SK_I, (Name, Content)\big) -> \sigma_I \tag{5}$$

The signature would bind the producer's identifier to the producer's public key. It is obvious that the signature could bind the data name to the valid *PARAM* because the signed fields encapsulates the data name and the valid *PARAM*. The domain name is included in the third field of the data name so that the domain name is bound to the valid *PARAM*. The ID_p, as the producer's identifier, contains the name of the domain where the producer is located so that the ID_p would be bound to the valid *PARAM*. Moreover, the producer's public key is composed by the *PARAM* and the ID_p so that the producer identifier would be bound to the producer's public key.

As a result, the Data packet could indirectly provide the producer's public key that has bound to the producer's identifier. Therefore, the producer's public key could aid the data-oriented authentication of the Data packet published by producers.

4.4 Data Packet Verification

When a Data packet arrives, a consumer will verify it as shown in Fig. 6. The content in the *Content* field would be considered useful only when the Data packet has passed the verification.

Firstly, the *Name* field would be examined. If the prefix of the data name in the *Name* field is '*//ndn/params*', the Data packet is published by an ISE to notify a valid *PARAM*. Otherwise, if the prefix is '*//ndn/data*', the Data packet is published by a producer to provide the data for an NDN application. Otherwise, the Data packet would be discarded because its data name is illegal.

Secondly, a consumer would retrieve the corresponding public key to verify the signature encapsulated in the *Signature* field. The verification process would be classified into two cases: (a) verification for the Data packet published by a producer, and (b) verification for the Data packet published by an ISE.

In Case (a), the *Name* field indicates the Data packet published by a producer. A consumer inquires its local cache of the valid *PARAM* issued by the ISE locating in the domain whose name is shown in the second field of the data name of the *Name* field.

If a consumer could not find the valid *PARAM* locally, the consumer would construct a new Interest packet whose name prefix is '*//ndn/params*' to request the valid *PARAM*. The details of the new Interest packet have been stated in Subsection 4.2.

Otherwise, if the valid *PARAM* is found locally, the verification would start immediately according to (6) as follows. The producer's public key would be composed by the ID_p and the found *PARAM*. The ID_p has been included in the second field of the data name in the *Name* field. Two message digests, h_{p1} and h_{p2}, are calculated by two methods. The signature σ_p encapsulated in the *Signature* field is decrypted by the producer's public key, i.e., ID_p and *PARAM*, as h_{p1} while the *Name* field and the *Content* filed in the receive Data packet are hashed as h_{p2}. If h_{p1} is equal to h_{p2}, the Data packet has successfully passed the verification so that the data encapsulated

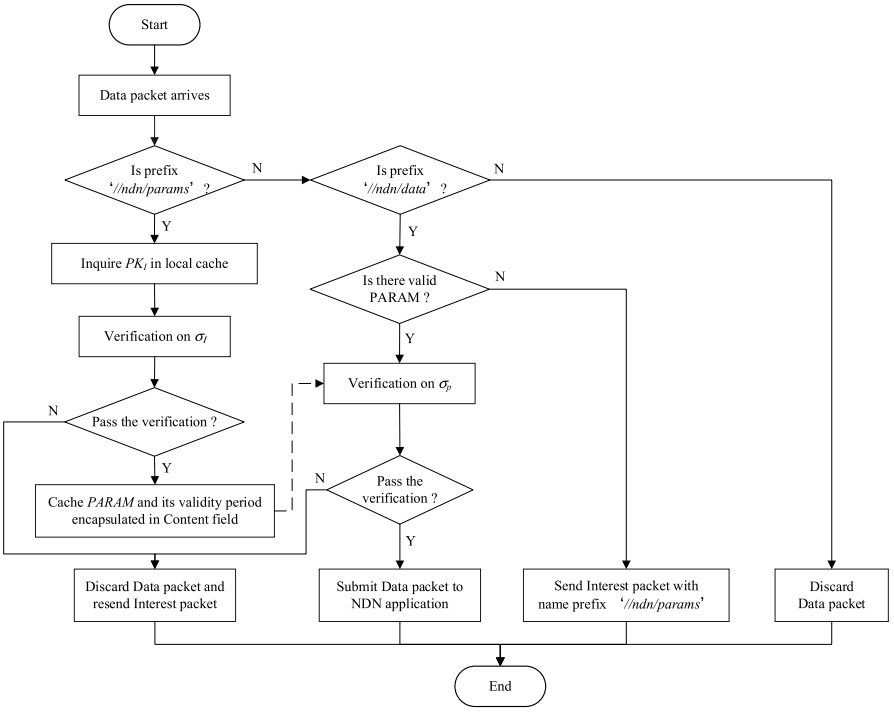

Fig. 6 Process to verify a Data packet by a consumer

in the *Content* field would be submitted to the NDN application at the upper layer. Otherwise, the verification fails. The Data packet has been modified or published by an illegal producer. Therefore, it would be discarded directly and resend the Interest packet with the same data name as the discarded Data packet.

$$Verify(\left(ID_p,\ PARAM\right), \sigma_p,\ (Name,\ Content)) - >\ \left(h_{p1},\ h_{p2}\right) \tag{6}$$

In Case (b), the *Name* field indicates the Data packet published by an ISE. A consumer would inquire its local cache to find the ISE's public key, PK_I, which has been distributed to all the network entities in the same domain shown in Subsection 4.1. Then, the found PK_I is used to verify the Data packet according to (7). Two message digests, h_{I1} and h_{I2}, are calculated by two methods. The signature, σ_I, encapsulated in *Signature* field is decrypted by PK_I as h_{I1} while the *Name* field and the *Content* field are hashed as h_{I2}. If h_{I1} is equal to h_{I2}, the Data packet is considered to have passed the verification successfully. As a result, the *PARAM* and its validity period encapsulated in the *Content* field are viewed to be issued by a legal ISE which is located in the domain whose name is indicated in the third field of the data name. If the validity period shows that the *PARAM* is valid, the *PARAM* would be used to verify the Data packet published by a producer immediately and the *PARAM* and its validity period would also be cached locally for further use. Otherwise, if h_{I1} is not equal to h_{I2}, the verification of the Data packet fails. The Data packet would be published

by an illegal ISE or has been modified during its delivery. Therefore, a consumer should discard the Data packet directly and resend the Interest packet with the same data name as the discarded Data packet to request the legal valid *PARAM*.

$$Verify(PK_I, \sigma_I, (Name, Content)) -> \left(h_{I1}, h_{I2}\right) \tag{7}$$

By the two verification cases, it is believed that all the data submitted to the NDN application at the upper layer would be published by authenticated producers and never be misrepresented during their delivery. In other words, the data are source-authenticated and integral. On one hand, the Case (b) guarantees that a consumer could retrieve the legal valid *PARAM*s. Therefore, in Case (a) a consumer could compose a valid producer's public key, i.e., the *PARAM* and the ID_p. If it is verified successfully, the Data packet must be published by a producer whose identifier is the ID_p. It indicates that the producer must own its private key which is derived from ID_p. When the producer obtains its private key from a PKG, the PKG has authenticated the producer. Consequently, the Data packet must be published by an authenticated producer. On the other hand, since the Data packet has passed the verification, its integrity can be achieved. In summary, the verification in the two cases would guarantee the data-oriented authentication.

5 Formal Verification

In order to demonstrate the security properties held by the proposed scheme, a formal verification on the AHISM-B scheme has been performed by using the formal validation tool of Automated Validation of Internet Security-sensitive Protocols and Applications (AVISPA) [30]. The AVISPA provides a modular and expressive formal language, called High Level Protocol Specification Language (HLPSL), to model security protocols and specify their security properties. Although it was designed for Internet, AVISPA could easily be extended to be used for the NDN networks.

5.1 Modelling Using HLPSL

We use the HLPSL to describe the secure communication following the AHISM-B scheme to verify the authentication and the integrity.

In the AHISM-B, there are two kinds of participants in the secure communication including the requester and the replier. The requester refers to the consumer obviously. The replier may be a producer, an ISE or a router. However, the producer and the ISE could publish the Data packet while the router functions as the Data packet cache. Different from the IP authentication, the NDN authentication is to authenticate the publisher but not the replier. As a result, the router is ignored in our model. Therefore, the modelling would be classified in two cases:

(a) Modelling the communication between the consumer and the producer.

(b) Modelling the communication between the consumer and the ISE.

Since Case (a) is very similar to Case (b), our model just presents Case (a). Case (b) could be formally verified similarly.

5.1.1 Basic Roles

Two basic roles of a consumer and a producer have been created. The consumer would request named data using Interest packets while the producer would reply with Data packets. The basic roles receive parameters from the composed roles, declare their local variables and perform the transitions to model the interactions of the Interest and Data packets.

Two parameters are created besides the parameters to name the basic roles and to provide transmission channels for the basic roles. The first one, named *H*, models the hash functions used in the signature. Another one, named *PK*, models the producer's public key, e.g., ID_p and *PARAM*. Since the suitable *PARAM* has been distributed to the consumer via the communication between the consumer and its ISE, the producer's public key has bound to the producer identifier at a consumer. As a result, in the communication between a consumer and a producer, it is reasonable to assume that a consumer owns the correct public key of the producer whose identifier is in the second field of the data name of the *Name* field.

Local variables in the basic roles model most of the fields in the Interest packet and Data packet, including *Name* and *Content*. They are viewed as local fresh values at runtime generated by the *new ()* operation in HLSPL. The variables of *Name* and *Content* model the requested data name and the published data, respectively.

The transitions are used to model the transmission and the reception of packets. The basic role of the consumer would has two transitions to send the Interest packets and to receive the Data packets. Moreover, the basic role of the producer would also has two transitions to receive the Interest packet and to send the Data packets.

5.1.2 Composed Roles and Goals

The composed roles instantiate one or more other roles, "gluing" them together so that they execute together, either in parallel or in sequence. In the modelling, two composed roles are defined, i.e., *session* and *environment*. The *session* role instantiates the model of two basic roles. The *environment* role is a top-level role, which declares global variables, a statement and a composition of two instantiated sessions. The first session provides the expected interaction. The second one includes an intruder playing the role of the producer.

In the validation the goals are modelled as the packet integrity and the data source authentication.

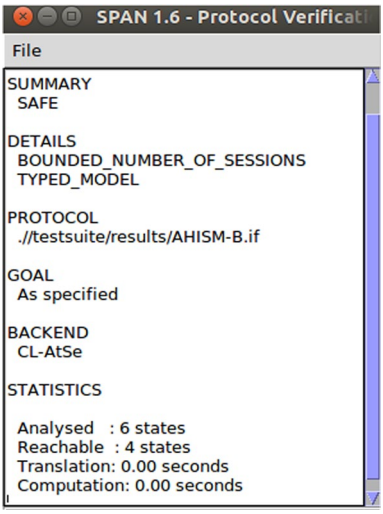

Fig. 7 Validation result using backend of CL-AtSe

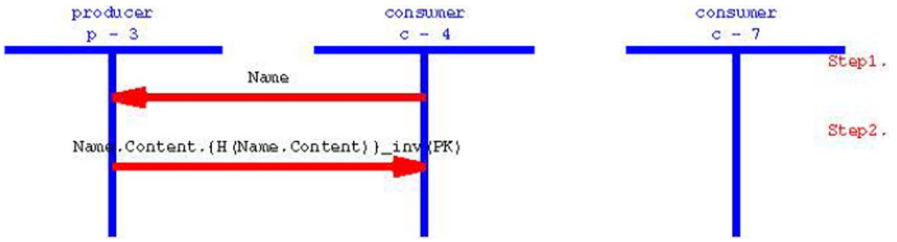

Fig. 8 Protocol verification for NDN secure communication

5.2 Validation Results

The backend of CL-AtSe has been adopted for validation of the AHISM-B. The result is "*SAFE*", as shown in Fig. 7. The verification result on the protocol at the sender side in a principal position is shown in Fig. 8 and a snapshot of the intruder verification is shown in Fig. 9. As the result shows "*SAFE*", the goal specified in our model has been achieved, i.e., packet integrity and data source authentication.

In the model, the only assumption is that a consumer owns the correct producer's public key. This assumption is satisfied by the communication between a consumer and its ISE, which is modelled by Case (2). The formal verification in Case (2) is very similar to that in Case (1). Differently, one basic role would be ISE in Case (2) instead of producer and the *PK* in Case (2) refers to the ISE's public key. Since every network entity has retrieved the ISE's public key when network initiates, a consumer will own the ISE's public key to verify the signature for sure. In summary, the Case (2) would be "*SAFE*" without any assumption.

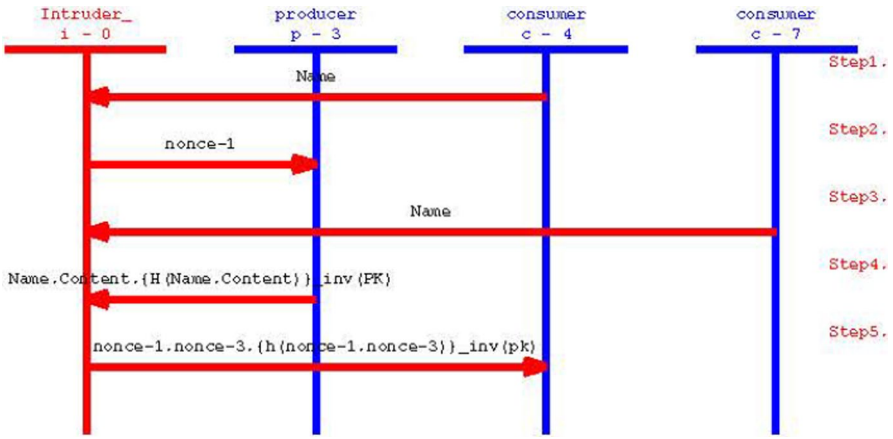

Fig. 9 Intruder verification for NDN secure communication

6 Performance Evaluation

In order to evaluate the performance, the AHISM-B scheme has been implemented to compare with the classic NDN scheme and our previous proposal. The blockchain network would be maintained among the ISEs. In a domain, there is only one ISE but many consumers and producers. Therefore, the scale of the blockchain network would be much smaller than that of the secure NDN. Moreover, the transaction in the blockchain is only triggered when the *PARAM* is generated or is updated. The event of the *PAPAM* generation or update occurs every a few months or one year so that the amount of transactions would be much smaller. In the case of the small scale and the small transaction amount, the performance of the blockchain network would have less impact to the performance of the secure NDN. We have implemented the block chain network based on *Hyperledger Fabric*, by which a transaction to update the *PARAM* would just take about one second. It shows that the operations of the implemented blockchain could incur less delay compared to those of the NDN. Based on the fact, in the performance evaluation, we just focus on the performance evaluation on the secure NDN in this section.

6.1 Experiment Design

The ndnSim simulator introduced in [31] has been extended to implement to simulate the AHISM-B scheme, the HISM-B scheme and the classic NDN scheme. By the AHISM-B scheme and the HISM-B, both producers and ISEs could publish Data packets. The Data packet published by an ISE is responsible for distributing the *PARAM* and its validity period. Once being accepted, the *PARAM* and its validity period would be cached at consumers for subsequent verification. Therefore, the Data packet overhead published by ISEs would be very small. Hence, our experiment only focuses on the Data packet published by producers.

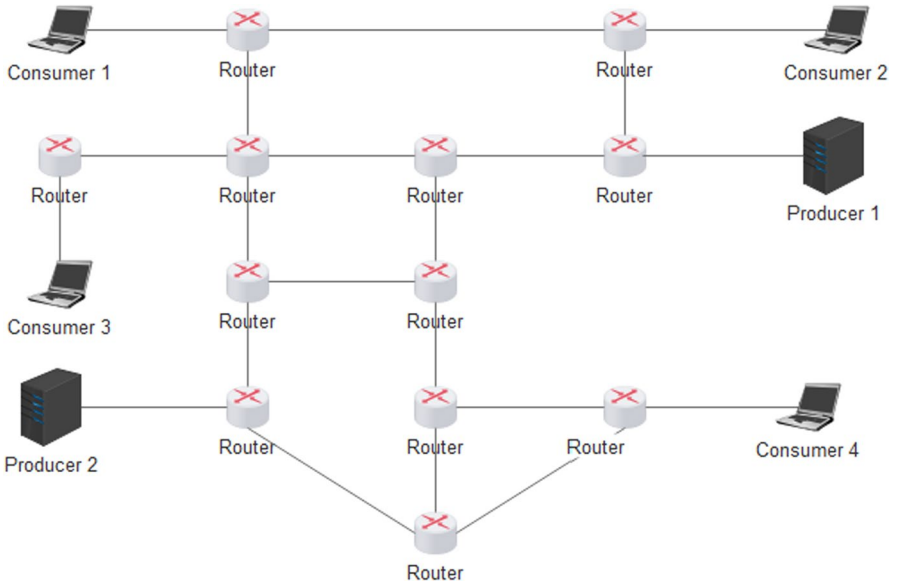

Fig. 10 Network topology in the simulation

Table 2 Topology parameters in the simulation

Parameter	N	e	N_c	N_p
Value	12	15	4	2

6.1.1 Network Topology

In order to study the performance of the AHISM-B scheme, the Abilene network topology [32] has been used in the simulation experiment as shown in Fig. 10. The parameters of the network topology are summarized in Table 2. There are N routers in the Abilene network and e bi-direction links among routers. N_c routers that have the minimal number of the links are chosen to connect to N_c consumers, respectively. Moreover, N_p routers that have the second minimal number of the links are chosen to connect to N_p producers, respectively.

6.1.2 Network Configuration

In the simulation experiment, the network parameters are summarized in Table 3. The simulation time is t minute. The propagation delay of one hop link is d ms and the link bandwidth is b Mbps.

Two producers would publish Data packets and sign them independently. The number of the Data packets that each producer would publish is o. The population of these Data packets follows the Zipf-Mandelbrot distribution with parameters of q and s. The cache size of routers is directly measured by the number of Data packets. The maximum number of cached Data packets in each router is equal to c. The

Table 3 Configuration parameters in the simulation

Parameter	t	d	b	o	q	s	c	l_i	l_d
Value	30	1	1	1000	0.7	0.7	200	27	1024

arrival rate of the Interest packet at each consumer follows Poisson distribution with mean value of r packet per second (packet/s). In our simulation, the value of r will change to show the performance with different traffic intensities. The data name and the data encapsulated in a Data packet are simply considered to own the fixed length so that the Interest packet and the Data packet have the fixed length. In our simulation, the size of the Interest packet is l_i bytes and the size of the data encapsulated in the Data packet is l_d bytes.

6.1.3 Parameter Evaluation

In the network simulation, 2 parameters are important: (1) signature time, which is the time taken to sign a Data packet by a producer and (2) verification time, which is the time taken to verify a Data packet by a consumer. An experiment has been designed and implemented as follows to evaluate the two parameters by the AHSIM-B scheme, the HISM-B scheme and the classic NDN scheme, respectively.

In the experiment, the AHISM-B scheme has employed the HESS algorithm [33] as a typical identity-based signature algorithm. By the HESS algorithm, both the length of *PARAM* and the length of secret private key are *128* bytes and the Secure Hash Algorithm SHA-256 is selected to calculate the message digest. In contrast, the HISM-B has used the same algorithms and parameters for the producer's signature and has employed the Rivest-Shamir-Adleman (RSA) algorithm and the Message-Digest 5 (MD5) algorithm for the domain signature. The classic NDN scheme has taken the Elliptic Curve Digital Signature Algorithm (ECDSA) with the key size of *571* bits. The algorithms and their parameters are listed in Table 4.

The HESS is coded using the pairing-based cryptography library while the ECDSA and the RSA are coded using the OpenSSL which is a full-strength general purpose cryptography library. The HESS algorithm, the RSA algorithm and the ECDSA algorithm are implemented over the operating system of Ubuntu 16 with the compiler of GCC to sign and verify the multiple Data packets.

Table 4 Algorithms in the experiment

Scheme name	Hash algorithm	Signature algorithm
AHISM-B	SHA-256	HESS with *PARAM* of 128 bytes and secret private key of 128 bytes
HISM-B	SHA-256 for producer's signature MD5 for domain signature	HESS with *PARAM* of 128 bytes and secret private key of 128 bytes for producer's signature RSA with 1024 bytes for domain signature
Classic NDN	SHA-256	ECDSA with key size of 571 bits

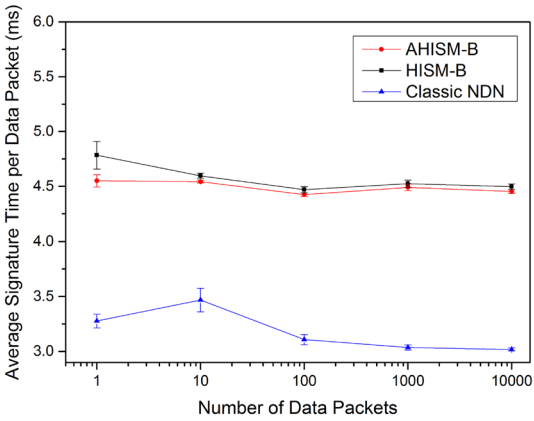

Fig. 11 Average signature time per Data packet

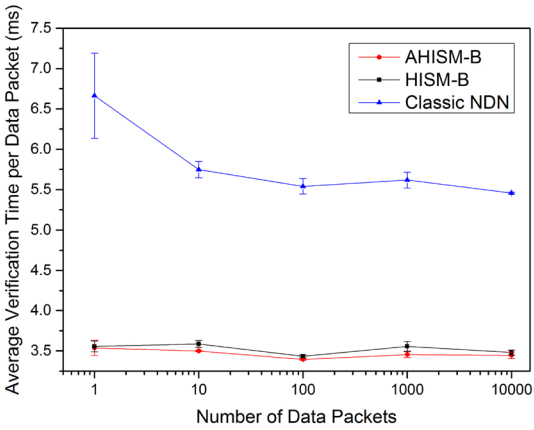

Fig. 12 Average verification time per Data packet

The average signature time per Data packet is shown in Fig. 11. On one hand, as we expected, the proposed AHISM-B scheme would consume less time than that of the HISM-B scheme. The Data packet in the HISM-B would have a larger size than that in the AHISM-B scheme because it contains the additional domain signature and the *PARAM*. The larger size of the packet would cause longer time for the signature. On the other hand, both the AHISM-B scheme and the HISM-B scheme have taken longer time for the signature than that of the classic NDN scheme because the operation of the bilinear pairing consumes much longer time in the HESS algorithm. However, the signature time is still acceptable by the AHISM-B scheme and the HISM-B scheme. The uncompetitive performance brings higher lever security where the producer's identifier is bound to the producer's public key so that the data-oriented authentication can be guaranteed by the AHISM-B.

The average verification time per Data packet is shown in Fig. 12. On the one hand, the proposed AHISM-B scheme would consume less time than that of the HISM-B scheme. By the HISM-B scheme, the additional domain signature must be verified for each received Data so that longer time would be taken for Data packet

Table 5 Parameters in the simulation

Scheme name	Signature time (ms)	Verification time (ms)
AHISM-B	4.492	3.465
HISM-B	4.574	3.522
Classic NDN	3.181	5.805

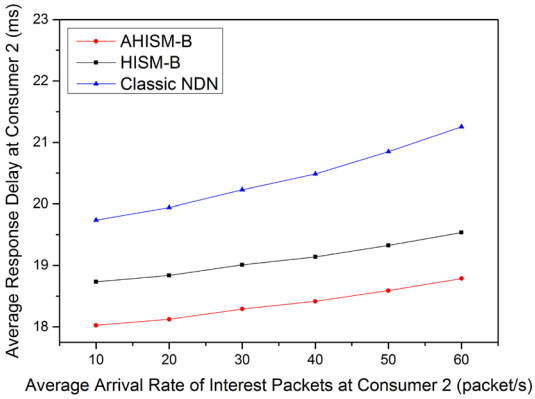

Fig. 13 Average response delay at consumer 2

verification. On the other hand, both the AHISM-B scheme and the HISM-B scheme consume about *3.5 ms* per Data packet while the classic NDN scheme would consume about more than *5.5 ms* on average. It is obvious that the AHISM-B scheme and the HISM-B scheme outperform the classic NDN scheme on the signature verification.

In our simulation, the signature time and verification time per Data packet is set to the average value in our experiment as shown in Table 5.

6.2 Performance

This section shows the performance of the AHISM-B scheme, the HISM-B scheme and the classic NDN scheme based on the simulation experiment. The performance will be evaluated in terms of the average response delay and the number of satisfied Interest packets. The response delay refers to the time required from the moment to transmit an Interest packet by a consumer to the moment to receive a verified Data packet as a response. The average response delay refers to the average value of response delay at each consumer. The number of satisfied Interest packets refers to the number of the Interest packets replied by Data packets at each consumer.

The simulation results at Consumer 2, Consumer 3 and all consumers are shown in Figs. 13, 14, 15, Tables 6, 7 and 8. It is obvious that the proposed AHISM-B scheme has a better performance than the classic NDN scheme because the

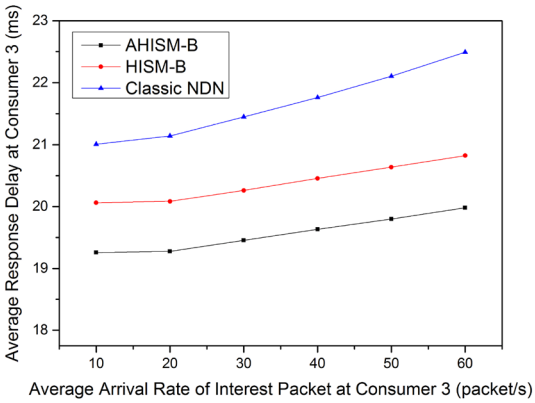

Fig. 14 Average response delay at consumer 3

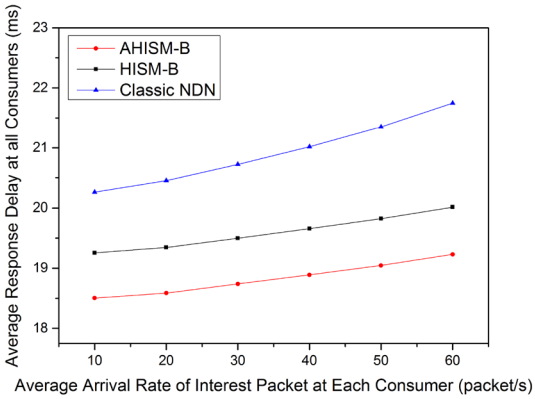

Fig. 15 Average response delay at all consumers

Table 6 Number of satisfied Interest packets at consumer 2

Scheme name	Number of satisfied interest packets					
	r = 10	r = 20	r = 30	r = 40	r = 50	r = 60
AHISM-B	17,866	36,025	53,971	71,781	89,670	107,639
HISM-B	17,867	36,025	53,971	71,781	89,662	107,639
Classic NDN	17,863	36,020	53,961	71,763	89,644	107,613

Table 7 Number of satisfied Interest packets at consumer 3

Scheme Name	Number of Satisfied Interest Packets					
	r = 10	r = 20	r = 30	r = 40	r = 50	r = 60
AHISM-B	17,867	35,960	53,958	71,835	89,874	107,859
HISM-B	17,866	35,959	53,958	71,837	89,871	107,864
Classic NDN	17,867	35,957	53,948	71,814	89,844	107,838

Table 8 Number of satisfied Interest packets at all consumers

Scheme Name	Number of Satisfied Interest Packets					
	r = 10	r = 20	r = 30	r = 40	r = 50	r = 60
AHISM-B	71,627	143,957	215,818	287,525	359,243	431,272
HISM-B	71,627	143,954	215,816	287,522	359,226	431,287
Classic NDN	71,622	143,944	215,780	287,453	359,145	431,172

AHISM-B scheme has presented a smaller average response delay and a larger number of satisfied Interest packets at each consumer.

The average response delay by the AHISM-B scheme is shorter compared to that by the HISM-B and the classic NDN scheme at different arrival rates of the Interest packet transmission as shown in Figs. 13, 14 and 15.

Firstly, the AHISM-B could reduce the average response delay by about 4% over the HISM-B scheme. The reason is obvious that the AHISM-B no longer requires to encapsulate the additional domain signature in a Data packet. Therefore, the length of the Data packet of the AHISM-B could be smaller than that of the HISM-B scheme so that the transmission delay of a Data packet could be shorter. Moreover, as shown in Table 5, the time required for the signature and the verification by the AHISM-B would be less than that by the HISM-B. As a result, due to the less transmission delay, the less signature time, and the less verification time, the AHISM-B scheme could present a lower response delay.

Secondly, the AHISM-B scheme could reduce the average response delay by at least 8% over the classic NDN scheme. Moreover, the advantage of the AHISM-B could be enhanced with the increase of the average arrival rate of Interest packets. When the average arrival rate reaches 60 packet/s, the average response delay by the AHISM-B would be less by 11% than that by the classic NDN scheme. The reason is clear as follows. Since the population of the Data packets follows the zipf's law, the requests from consumers would mainly be replied by the popular Data packets. In the NDN networks, with the help of routers, one popular Data packet would usually be used to respond to the requests from multiple consumers. On one hand, the routers may forward the Data packet to multiple consumers because the Pending Interest Tables (PITs) at routers have converged the requests from multiple consumers. On the other hand, the routers may cache a Data packet and then reply to the subsequent requests from other consumers. When the Data packet is received, all the consumers must verify the Data packet independently. Therefore, the number of verifications is equal to the number of consumers who have requested the Data packet. As a result, a Data packet would be signed once while it would be verified multiple times. For the popular Data packets, the number of rounds of the verifications would be much more than that of the signatures. Although it takes more time to sign a Data packet, the AHISM-B scheme takes less time to verify a Data packet compared to the classic NDN scheme. Due to the popular Data packets, the advantage of a smaller verification delay would be enhanced by the AHISM-B scheme compared to the classic NDN scheme. As a result, the average response delay by the AHISM-B scheme will

be smaller than that by the classic NDN scheme. With the increase of the arrival rate of Interest packets, the popular Data packets would be requested more frequently so that the advantage of the AHISM-B could be amplified.

The number of satisfied Interest packets is a little larger by the AHISM-B scheme and the HISM scheme compared to that by the classic NDN scheme at various average arrival rates of the Interest packet as shown in Tables 6, 7 and 8. Moreover, with the increase of the average arrival rate of the Interest packet at each consumer, the advantage of the AHISM-B scheme will be better shown off. In the NDN networks, majority of the Interest packets would be replied by the routers rather than by the producers. Therefore, the time consumption of signature generation at producers has little impact on the network performance. However, all the replied Data packets must be verified by the consumers. The lower verification speed would cause queuing of the Data packets at the consumer. The Data packets may be discarded due to too many Data packets in a long queue. The more Interest packets arrive at consumers, the greater the possibility of loss would be. Once Data packets are discarded, the re-transmission of the Interest packets would be incurred to request the discarded Data packets. The re-transmitted Data packets would deteriorate the queue performance. Thus, the proposed AHISM-B scheme and HISM-B are able to hold a larger number of satisfied Interest packets at each consumer than that of the classic NDN scheme due to their less time taken for Data packet verification.

The simulation experiment has also been performed in the low-bandwidth, e.g., less than 0.2 Mbps. The result shows that our AHISM-B has also presented a smaller average response delay and a larger number of satisfied Interest packets for consumers. The reason that the AHISM-B has advantages is the same as that presented in the case of the normal bandwidth.

7 Conclusion

In this paper, we have proposed the AHISM-B scheme to provide the data-oriented authentication. By the proposal, an ISE and some routers would play the roles of the PKGs to provide security service together in a domain. On one hand, all the ISEs would form a blockchain network to manage cryptography information. Each block in the chain would bind the domain name to its cryptography information to respond to the requests from the NDN network. On the other hand, producers and consumers would form a secure NDN network where Data packets would be protected by the signatures. The results of formal analysis and formal verification show that our proposal could provide the secure service of the data-oriented authentication. However, our proposal depends on the hierarchical naming mechanism due to the use of HIBC algorithm. Since the identifier of a producer has been embedded in the data name, privacy preservation may be a challenge. Our future work would aim to explore the solution independent of the hierarchical naming mechanism.

Appendix

Security Proof

The extended BAN logic [34] is employed to formally analyze our AHISM-B to show its security property. The well-formed predicate constructs are listed as follows. Here U_i denotes communicating entity. Both X and Y denote predicate constructs.

$U_i| \equiv X$: U_i believes X.

$U_i| \sim X$: U_i once said X.

$U_i \Rightarrow X$: U_i has jurisdiction over X.

$U_i \lhd X$: U_i sees X. Typically, U_i sees X if U_i has received a message that contains X.

$\mathrm{PK}(U_i, K_{U_i})$: U_i has associated a good public key K_{U_i}.

$\Pi(K_{U_i}^{-1})$: U_i has a good private key $K_{U_i}^{-1}$.

$\sigma(X, K_{U_i}^{-1})$: X is signed with U_i's private key $K_{U_i}^{-1}$.

(t_1, t_2): It is a time interval. The start time is t_1 and the end time is t_2.

$(X, (t_1, t_2))$: X holds in the interval (t_1, t_2).

The inference rules are composed by assumptions and the ratiocination, expressed based on the defined formulae as follows. Assumption portions of the rules are numerators while ratiocination portions of the rules are denominators.

R1 indicates that if U_i believes that U_j has jurisdiction over X and U_i believes that U_j believes X, then U_i believes X.

R1. $\frac{U_i| \equiv U_j \Rightarrow X, U_i| \equiv U_j| \equiv X}{U_i| \equiv X}$.

R2 and R3 are the aggregation rule and the segregation rule, respectively. Their intuitive justification should be obvious.

R2. $\frac{U_i| \equiv X,\ U_j| \equiv Y}{U_i| \equiv (X,Y)}$

R3. $\frac{U_i| \equiv (X,Y)}{U_i| \equiv X}$.

R4 is related to public key crypto systems. To check that a message X was signed by U_j, it is sufficient to know U_j's public key. Therefore, it is paramount that U_j's public key is genuine and U_j must be in possession of U_j's private key.

R4. $\frac{U_i| \equiv \mathrm{PK}(U_j, K_{U_j}), U_i| \equiv \Pi(K_{U_j}^{-1}), U_i \lhd \sigma(X, K_{U_j}^{-1})}{U_i| \equiv U_j| \sim X}$.

R5 is related to a timestamp. When uttering a duration-stamped message X, U_i commits itself to believe X for the interval specified by the duration-stamp.

R5. $\frac{U_i| \equiv U_j| \equiv (t_1,t_2), U_i| \equiv U_j| \sim (X,(t_1,t_2))}{U_i| \equiv U_j| \equiv X}$.

Description

By the AHISM-B scheme, the communication occurs between consumers and producers, between consumers and routers, or between consumers and ISEs so that there are four roles including consumers, producers, routers and ISEs. Instead of publishing packets, routers just cache packets and respond with the cached packets. In order to

simplify our analysis, the router role has been ignored. As a result, there are three roles in the model of the AHISM-B, including the consumers (C), the producers (P) and the ISEs. The communication messages are modelled in Fig. 16.

Message (1) models an Interest packet sent from a consumer to a producer. The requested data name in its payload *Name* is viewed as two parts: the routing identifier of the P and the requested file name (*fname*) according to Sect. 3.2. Message (2) models a Data packet sent from a producer to a consumer. Its payload *Name* is same as that in Message (1). And its payload *Content* is viewed as the data (*data*). As a result, its payload *Signature* is considered as the signature that is signed with the P, *fname* and *data* using the producer's private key, i.e., $\sigma((P, fname, data), K_P^{-1})$. Message (3) and Message (4) model an Interest packet and a Data packet between a consumer and an ISE respectively, which is similar to the Message (1) and Message (2). Here, *dname* indicates the domain name in the third field of the data name. *param* and (t_1, t_2) indicate the *PARAM* and its validity period encapsulated in the *Content* payload.

The assumptions are listed as α1 and α2. α1 means that a consumer believes that ISEs have associated their good public keys. And α2 means that a consumer believes that ISEs and producers have good private keys. α1 and the first part of α2 are acceptable because ISEs have generated ISE's key pairs, including ISEs' public keys and ISE's private keys, in the network initiation. The second part of α2 is acceptable because producers' private keys have been delivered to producers via secure channels in the network initiation.

α1: $\{|\checkmark C| \equiv \mathrm{PK}(ISE,\ K_{ISE})\}$

α2: $\{C| \equiv \Pi(K_{ISE}^{-1}),\ C| \equiv \Pi(K_P^{-1})\}$

The Goal is obvious to guarantee the data-oriented authentication. It is described as Γ1.

Γ1: $\{C| \equiv P|\sim(P, fname, data)\}$

Proof is shown as follows:

Since C has received Message (4) that contains the signature, C has seen the signature $\sigma((ISE, dname, param, (t_1, t_2)), K_{ISE}^{-1})$. It would be expressed as M1:

M1.$C \lhd \sigma((ISE, dname, param, (t_1, t_2)), K_{ISE}^{-1})$.

Using α1, α2 and M1, R4 could be written as follows.

$$\frac{C| \equiv \mathrm{PK}(ISE, K_{ISE}),\ C| \equiv \Pi(K_{ISE}^{-1}),\ C \lhd \sigma((ISE, dname, param, (t_1, t_2)), K_{ISE}^{-1})}{C| \equiv ISE|\sim(ISE, dname, param, (t_1, t_2))}$$

As a result, M2 has been proved.

M2.$C| \equiv ISE|\sim(ISE, dname, param, (t_1, t_2))$.

Since C and ISE are in the same domain, it is not difficult to maintain the synchronized clock within one domain. Therefore, M3 is considered to be true.

M3.$C| \equiv ISE| \equiv (t_1, t_2)$.

Using M2 and M3, R5 could be written as follows.

(1) C -> P : *P, fname*
(2) P -> C : *P, fname, data,* $\sigma((P, fname, data), K_P^{-1})$
(3) C -> ISE : *ISE, dname*
(4) ISE -> C : *ISE, dname, param,* (t_1,t_2), $\sigma((ISE, dname, param, (t_1, t_2)), K_{ISE}^{-1}$

Fig. 16 Modelled messages

$$\frac{C| \equiv ISE| \equiv (t_1, t_2), C| \equiv ISE| \sim (ISE, dname, param, (t_1, t_2))}{C| \equiv ISE| \equiv (ISE, dname, param)}$$

As a result, M3 has been proved.

M4. $C| \equiv ISE| \equiv (ISE, dname, param)$.

Using M4, R3 could be written as follows:

$$\frac{C| \equiv ISE| \equiv ((ISE, dname), param)}{C| \equiv ISE| \equiv param}$$

As a result, M5 has been proved.

M5.$C| \equiv ISE| \equiv param$.

The *PARAM* is generated by the local ISE according to the HIBC algorithm so that the local ISE has jurisdiction over *param*. Since all the ISEs have formed a blockchain network, the domain name has been bound to the *PARAM* and its validity period. As a result, an ISE would jurisdiction over the *PARAM* generated by another ISE. In a domain, the ISE takes a role of root PKG so that the consumers and producers would believe the secure service information that their ISE provides. Based on the above, M6 is very reasonable.

M6.$C| \equiv ISE \Rightarrow param$.

Using M5 and M6, R1 could be written as follows:

$$\frac{C| \equiv ISE \Rightarrow param, C| \equiv ISE| \equiv param}{C| \equiv param}$$

As a result, M7 has been proved.

M7. $C| \equiv param$.

Since the data name encapsulated in *Name* payload of the Interest is coming from the NDN application at the upper layer, consumer would believe the data name. *P* and *fname* are the important components of the data name. As a result, M8 is reasonable.

M8. $C| \equiv (P, fname)$.

Using M8, R3 could be written as follows:

$$\frac{C| \equiv (P, fname)}{C| \equiv P}$$

As a result, M9 has been proved.

M9. $C| \equiv P$.

Using M7 and M9, R2 is written as follows:

$$\frac{C| \equiv param, C| \equiv P}{C| \equiv (P, param)}$$

As a result, M10 has been proved.

M10. $C| \equiv (P,\ parma)$.

Since the producer's public key $\mathrm{PK}(P, K_P)$ is composed by *P* and *param*, M10 could be written as M10'.

M10'. $C| \equiv \mathrm{PK}(P, K_P)$.

Since it has received Message (2) that contains the signature, the consumer has seen the signature $\sigma((P, fname, data), K_P^{-1})$. It would be expressed as M11:

M11. $C \lhd \sigma((P, fname, data), K_p^{-1})$.

Using α2, M10' and M11, R4 could be written as follows.

$$\frac{C| \equiv \mathrm{PK}(P, K_P), C| \equiv \Pi(K_p^{-1}), C \lhd \sigma((P, fname, data), K_p^{-1})}{C| \equiv P| \sim (P, fname, data)}$$

As a result, the overall goal has been proved. Therefore, it is believed that our AHISM-B could guarantee the data-oriented authentication.

Authors Contribution The first author of the paper is Li, B., who has made major research work to generate this manuscript including the design of the proposed solution, security verification of the solution, performance evaluation of the solution by simulation experiments, and generation of the first draft of the paper. The corresponding author of this manuscript is Ma, M., who has had his contribution to generate the research initiative, verify the designed solution, validate the results of the security verification and performance evaluation, and make a few rounds of the revision on the manuscript of the submitted paper.

Funding Open Access funding provided by the Qatar National Library. This work was supported by the Shenzhen Education Science Planning Leading Group Funds under Grant ybzz20006, and the Shenzhen Science and Technology Innovation Committee Funds under Grant JCYJ20160422110910282.

Declarations

Competing interest Authors confirm that there are no competing interests between the authors and the organizations of the authors.

References

1. Li, Z., Xu, Y., Zhang, B., Yan, L., Liu, K.: Packet forwarding in named data networking requirements and survey of solutions. IEEE Commun. Surveys Tutor. **21**(2), 1950–1987 (2019)
2. AbdAllah, E.G., Hassanein, H.S., Zulkernine, M.: A survey of security attacks in information-centric networking. IEEE Commun. Survey Tutor. **17**(3), 1441–1454 (2015)
3. Chatterjee, T., Ruj, S., Bit, S.D.: Security issues in named data networks. Computer **51**(1), 66–75 (2018)
4. Borrego, C., Amadeo, M., Molinaro, A., Jhaveri, R.H.: Privacy-preserving forwarding using homomorphic encryption for information-centric wireless ad hoc networks. IEEE Commun. Lett. **23**(10), 1708–1711 (2019)
5. Sagar, R., Jhaveri, R., Borrego, C.: Applications in security and evasions in machine learning: a survey. Electronics **9**(97), 1–42 (2020)
6. Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., Kc Claffy, P., Crowley, C., Papadopoulos, L.W., Zhang, B.: Named data networking. SIGCOMM Comput. Commun. Rev. **44**(3), 66–73 (2014)

7. Maldonado-Ruiz, D., Torres, J., El Madhoun, N., Badra, M.: Current trends in blockchain implementations on the paradigm of public key infrastructure: a survey. IEEE Access **10**, 17641–17655 (2022)
8. Khelifi, H., Luo, S., Nour, B., Moungla, H., Ahmed, S.H.: Reputation-based blockchain for secure NDN caching in vehicular networks. In: Proc IEEE conferece on standards for communications and networking (CSCN). IEEE, Paris (2020)
9. Khelifi, H., Luo, S., Nour, B., Moungla, H., Guizani, M.: A blockchain-based architecture for secure vehicular named data networks. Comput. Electric. Eng. **86**, 106715 (2020)
10. Yang, N., Chen, K., Wang, M.: SmartDetour: defending blackhole and content poisoning attacks in IoT NDN networks. IEEE Internet Things J. **8**(15), 12119–12136 (2021)
11. Li, B., Ma, M., Xia, R.: Hierarchical identity-based security mechanism using blockchain in named data networking. In: Proc 2020 3rd international conference on hot information-centric networking (HotICN), pp. 148–153. IEEE, Heifei (2020)
12. Zhang, X., Chang, K., Xiong, H., Wen, Y., Shi, G., Wang, G.: Towards name-based trust and security for content-centric network. ICNP, Vancouver (2011)
13. Martin, L.: Introduction to identity-based encryption. Artech House, Norwood (2008)
14. Hamdane, B., Boussada, R., Elhdhili, M.E., Fatmi, S.G.E.: Hierarchical identity based cryptography for security and trust in named data networking, pp. 226–231. WETICE, Poznan (2017)
15. Ghali, C., Tsudik, G., Uzun, E.: Network-layer trust in named-data networking. ACM SIGCOMM Comput. Commun. Rev. **44**(5), 12–19 (2014)
16. Yu, Y.: Public key management in named data networking. UCLA, Los Angeles (2015)
17. Ramani, S.K., Afanasyev, A.: CertCoalesce: efficient certificate pool for NDN-based systems. In: Proc of the 7th ACM conference on information-centric networking (ICN '20), pp. 158–160. IEEE, New York (2020)
18. Zhang, Z., Yu, Y., Zhang, H., Newberry, E., Mastorakis, S., Li, Y., Afanasyev, A., Zhang, L.: An overview of security support in named data networking. IEEE Commun. Mag. **56**(11), 62–68 (2018)
19. Li, R., Asaeda, H., Wu, J.: DCAuth: data-centric authentication for secure in-network big-data retrieval. IEEE Trans Netw. Sci. Eng. **7**(1), 15–27 (2020)
20. Refaei, T., Horvath, M., Schumaker, M., Hager, C.: Data authentication for NDN using hash chains. ISCC, Larnaca (2015)
21. Fan, Y., Tao, Y., Zhu, Y.: A lightweight verification mechanism for MPEG-DASH in named data networking. HotICN, Hefei (2020)
22. Zhang, Z., Liu, S., King, R., Zhang, L.: NDN-MPS: supporting multiparty authentication over named data networking. In: Proc of the 8th ACM conference on information-centric networking (ICN '21), pp. 83–94. IEEE, New York (2021)
23. Xue, K., Yang, J., Xia, Q., Wei, D.S.L., Li, J., Sun, Q., Lu, J.: CSEVP: a collaborative, secure, and efficient content validation protection framework for information centric networking. IEEE Trans. Netw. Serv. Manage. **19**(2), 1761–1775 (2022)
24. Lou, J., Zhang, Q., Qi, Z., Lei, K.: A blockchain-based key management scheme for named data networking, pp. 141–146. HotICN, Shenzhen (2018)
25. Liu, H., Zhu, R., Wang, J., Wengang, X., Cui, J.: Blockchain-based key management and green routing scheme for vehicular named data networking. Security Commun Netw. **2021**, 1–12 (2021)
26. Li, R., Asaeda, H.: A blockchain-based data life cycle protection framework for information-centric networks. IEEE Commun. Mag. **57**(6), 20–25 (2019)
27. Huang, H., Wu, Y., Xiao, F., Malekian, R.: An efficient signature scheme based on mobile edge computing in the NDN-IoT environment. IEEE Trans. Comput. Soc. Syst. **8**(5), 1108–1120 (2021)
28. Jin, T., Zhang, X., Liu, Y., Lei, K.: BlockNDN: a bitcoin blockchain decentralized system over named data networking, pp. 75–80. ICUFN, Milan (2017)
29. Guo, J., Wang, M., Chen, B., Yu, S., Zhang, H., Zhang, Y.: Enabling blockchain applications over named data networking. ICC, Shanghai (2019)
30. S. Mödersheim, P.H. Drielsma, IKEv2-MAC, 2003, select tab "The AVISPA library" on AVISPA project website. URL: http://www.avispa-project.org/
31. Mastorakis, S., Afanasyev, A., Zhang, L.: On the evolution of ndnSIM: an open-source simulator for NDN experimentation. ACM SIGCOMM Comput. Commun. Rev. **47**(3), 19–33 (2017)
32. Y. Zhang. Abilene traf_c matrices, http://www.cs.utexas.edu/users/yzhang/research/AbileneTM (2015). Accessed Jan. 2015
33. Hess, F.: Efficient identity based signature schemes based on pairings. LNCS **2595**, 310–324 (2003)

34. Sufatrio, R.H.C.Y.: Extending BAN logic for reasoning with modern PKI-based protocol. In: Din, R. (ed.) IFIP international conference on network and parallel computing, pp. 190–197. IEEE, Shanghai (2008)

Bing Li received her B.E degree and Ph. D degree in computer science and technology from Tianjin University, Tianjin, China, in 2006 and 2010, respectively. She was a visiting research scholar at Nanyang Technological University (NTU), Singapore from 2008 to 2010. During 2012 and 2013, she was a postdoctoral research fellow at Concordia University, Montreal, Canada. In 2014, Dr. Li joined Shenzhen University, Shenzhen, China as a lecture. Her research interests include secure multicast, network architecture, traffic identification and measurement.

Maode Ma a Fellow of IET, received his Ph.D. degree from Department of Computer Science in Hong Kong University of Science and Technology in 1999. Now, Prof. Ma is a Research Professor in the College of Engineering at Qatar University in Qatar. He has extensive research interests including network security and wireless networking. Prof. Ma has more than 470 international academic publications including over 230 journal papers and more than 230 conference papers. His publication has received about 7800 citations in Google Scholar. He currently serves as the Editor-in-Chief of International Journal of Computer and Communication Engineering and Journal of Communications. He also serves as a Senior Editor for IEEE Communications Surveys and Tutorials, and an Associate Editor for International Journal of Wireless Communications and Mobile Computing and International Journal of Communication Systems. Prof. Ma is a senior member of IEEE Communication Society and a member of ACM. He is now the Chair of the ACM, Singapore Chapter.