Named-Data Security Scheme for Named Data Networking

Balkis Hamdane[1,2], Ahmed Serhrouchni[1],Ahmad Fadlallah[1,3],Sihem Guemara El Fatmi[2],
[1]Télécom ParisTech, Paris, France
[2] Higher School of Communications of Tunis (Sup'Com), Ariana, Tunisia
[3]Faculty of Computer Studies, Arab Open University, Beirut, Lebanon
{balkis.hamdane, Ahmed.Serhrouchni, Ahmad.Fadlallah}@telecom-paristech.fr
sihem.guemara@supcom.rnu.tn

***Abstract*—Information Centric Networking (ICN) approach constitutes one of the promising results of Internet of the Future research activities. Content is the central element in this approach. Content Centric Networking (CCN) and Named Data Networking (NDN) are the most emerging ICN projects. They adopt a security model based on named data in which content is signed by the content producer.**

In this paper, we propose to enhance security in CCN/NDN projects. We first define requirements for their naming system in order to provide security services that bind both naming and content. Then, we propose a hybrid scheme which combines public-key infrastructure (PKI) and Hierarchical Identity-Based Cryptography (HIBC) in order to meet the defined requirements. This proposal represents a defense against a potential attack and perfectly fits in with the structures of the various objects of CCN/NDN.

***Index Terms*—Information Centric Networking, Content Centric Networking, Named Data Networking, Hierarchical Identity-Based Cryptography.**

I. INTRODUCTION

Named Data is the central element in the Information Centric Networking (ICN). Content publishing, requesting, managing and reachability are all determined by content name, rather than IP address [1]. ICN-related research projects adopt different approaches for naming information; some projects use hierarchical and human readable naming schemes, whereas others use flat and self-certifying schemes [2] [3]. Content Centric Networking (CCN) [4] and Named Data Networking (NDN) [5] are emerging ICN projects that adopt the first approach. To request data, the consumer sends an Interest packet based on the name of the desired piece of content. It receives in response a Data packet containing the same name as the Interest packet, the piece of data and a digital signature calculated using the content producer private key. This signature is useful for ensuring data security. Indeed, it is calculated on the entire Data packet, thus securely binding a piece of data to its name. However, the validation of the signature requires the public key of the producer. Security is based in part on the validity of this key.

NDN offers an interesting platform to build trust in this key, which supports traditional and new trust mechanisms [4]. Previous research has suggested the possibility of using a Public Key Infrastructure (PKI) [5].

In this paper, we explain the susceptibility of the existing mechanisms to a potential attack. Then, we propose to adapt the NDN naming system to ensure the validity of producers' public keys. This adaptation enhances the security in NDN. The proposed solution is based on a hybrid scheme that combines public-key infrastructure (PKI) and Hierarchical Identity-Based Cryptography (HIBC) [6].

HIBC represents a variation of Identity-Based Cryptography (IBC) that reflects an organizational hierarchy [7]. With the integration of this system, content name acts as public key. The private key is generated from the public key, the secret key and public parameters of a server called Private Key Generator (PKG). The validity of keys depends on the validity of the PKG public parameters. To ensure trust in these parameters, a PKI is deployed and integrated in our proposal.

This paper is structured as follows: Section II presents the NDN project with emphasis on the security and naming system. Section III provides background information on IBC and HIBC algorithms and then describes the proposed solution. Section IV analyzes the related work. Finally, section V concludes the paper.

II. NAMED DATA NETWORKING

ICN constitutes one of the promising results of Internet of the Future research activities. Van Jacobson (a leading contributor to the technological bases of current Internet [8]) is one of the first visionaries who proposed this approach. In 2006, he gave a Google TechTalk entitled "A New Way to Look at Networking" in which he presented his ICN project named Content Centric Networking (CCN) [4][9]. This project was launched by Palo Alto Research Center (PARC). It has produced a protocol specifications and open source software named CCNx. In September 2010, CCN was selected among the four projects of the National Science Foundation's Future Internet Architecture (FIA) [5] [10] [11] [12]. In this new context, CCN is officially called Named Data Networking (NDN) and PARC collaborates with a team of nine universities, led by University of California, Los Angeles (UCLA).

NDN retains "the Internet's hourglass architecture". It just changes the "thin waist" by using data names instead of IP addresses. The project keeps the design decisions that make TCP/IP simple, robust, and scalable while overcoming the problems of current Internet.

NDN can run over anything, including IP, and anything can run over NDN, including IP. It then represents a "universal overlay" [5].

There are two packet types in NDN: Interest and Data (Fig.1). Interest packet represents a request for content. It consists of content name, selector and nonce fields. Data packet represents the response to an Interest packet. It contains the requested information object. This packet is composed of a content name, signed info and a signature on the entire packet (the content name, data, and signed info). It satisfies an interest if its name is equal to that contained in the Interest packet and it can be sent by any node receiving the Interest packet and having the required data.

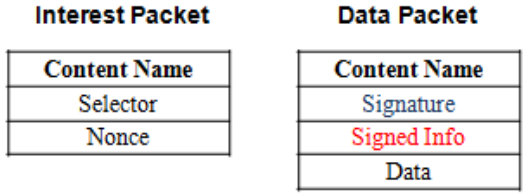

Fig. 1. NDN Packet Types

A. *Naming*

NDN names are opaque to the network and specific to applications, which allow the naming schemes to evolve independently of the network. They are human-readable and hierarchically organized. These names are composed of explicit components, delimited by a character. The delimiters are not part of the name. The first part of the name contains a globally routable name; the second part provides an organizational name. Finally, the last part shows the versioning and segmentation functionality.

In the example shown in Fig. 2, the third segment of the first version of a paper (NoF.pdf) produced by telecom-parisTech can have the name '/telecom-paristech.fr/paper/NoF.pdf/V1/S3'. The '/'indicates a boundary between the components of the name.

Fig. 2. Example content name

The hierarchy allows routing scalability via aggregation. The readability gives the user the ability to remember content names and to request them directly. It also establishes a relation between the name and what the user wants [1].

To produce a content name, a deterministic algorithm can be employed allowing the requester and the producer to generate the same name based on information known to both. The requester can also use a partial name to retrieve data [5].

B. *Security*

In ICN, the user can benefit from any available copy of content (through caching) [1]. Security can no longer be tied to a content location or to a particular host. Therefore, a content-oriented security model is adopted.

According to NDN, robust security model requires the following security services [4] [13]:

- Validity: there is no change in the data (integrity) or in the correspondence between the name and its content (authenticity).
- Provenance: data are published by an appropriate publisher in measure to produce these contents. This combines the notion of publisher authentication and publisher identification.
- Relevance/Pertinence: data represents the answer to a question posed by the receiver.
- Access control: the access to data is limited to authorized entities.
- Confidentiality: data are readable only by authorized entities.

Relevance is explicit in the Content Name since the content name in Interest packet is meaningful and it is equal to content name in Data packet. Publisher identification is ensured when the name contains valid information about the real-world identity of this entity. However, a mechanism is needed to verify the validity of this information. Also, the public key should be bound with its owner real-world identity since this key will be used in producer authentication.

In order to provide confidentiality and access control, NDN adopts an encryption-based model. Decryption keys must be known by authorized entities. Confidentiality and access control then become a key management problem.

To ensure the publisher authentication and data validity, all content is digitally signed by the original content provider's private key. The signature is calculated on the entire packet (the content name, data, and signed info); thus securely binding a piece of data to its name. The verification of this signature requires the producer public key. This key can be recovered, as an NDN data, based on information provided in the field signed info. To build trust in this key, a PKI can be deployed. The certificate used will link the identity of the content producer to its public key. In addition to the issue of high number of certificates to be generated and to the inefficiency of proposed revocation solutions [14], the "NDN with PKI" faces the problem of how to determine the producer identity, which made this scheme vulnerable to an attack described in the next subsection.

C. *Potential Attack*

Despite the fact that CCN/NDN adopts a content-oriented security model to overcome some attacks, it remains vulnerable to other attacks such as interest flooding and content/cache poisoning. Several researches are initiated to mitigate these attacks [5] [15]. This subsection addresses a serious attack that has been never handled. Indeed, if the name of the content doesn't contain enough valid information about the identity of the producer, an attack can be launched as follows:

- By hearing an Interest packet, an attacker produces false content.
- He binds it with the content name requested through a digital signature.

- He can then send to the requester a Data packet containing the same name, a false content, information about his own key (in the signed info field) and associated digital signature.
- By receiving this content, the requester retrieves the public key as well as the certificate of the attacker as NDN data.
- The requester cannot perceive the attack because Data packet seems legitimate and bears a legitimate signature.

The requester initially only knows the content name. However, he needs the producer public key to verify the digital signature. A link between the name and the corresponding public key is then necessary. If such a link is not provided the attack described above can then be launched.

D. *Conclusion*

Naming plays a critical role in security. Indeed, to ensure security services, certain requirements must be satisfied. For data integrity, the name should establish a binding between the name and the publisher's public key (to verify signature). To ensure data authenticity, the name should establish a binding with the content. This is ensured, in NDN, by the digital signature linking the name to its content. To verify the provenance, three potential bindings should be ensured: (1) a binding between the publisher real-world identity and the name, (2) a binding between real-world identity and the publisher public key and (3) a binding between the publisher public key and the name. Bindings are transitive, providing any two of them implies the third one [16]. Finally, to ensure pertinence, the name should be human-readable and meaningful.

Figure 3 describes the required bindings between the content name and other entities to ensure security services. The absence of any of these requirements makes the NDN scheme vulnerable to the potential attack presented in section II.C.

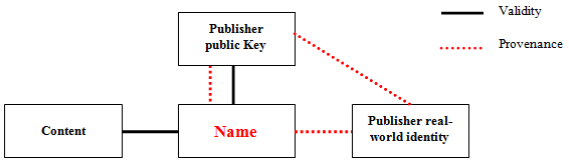

Fig. 3.Required bindings between the name and security services

III. Proposed Solution

The problem in NDN naming scheme is that it does not establish a link between the name and the publisher public Key. We propose an adaptation of the NDN naming system to ensure this link while maintaining names readability and hierarchical form. The proposed solution is based on Hierarchical Identity-Based Cryptography (HIBC) where the public key is directly derived from the data name [6].

A. *Background Information*

1) *Identity Based Cryptography*

Identity Based cryptography (IBC) is a cryptosystem in which any string can form a valid public key. The private key is obtained from the public key multiplied by the secret key of the PKG [17]. IBC is composed of two important primitives: Identity Based Encryption (IBE) and Identity-Based Signature (IBS).

a) Identity-Based Encryption

Identity-based Encryption (IBE) system is based on four algorithms: Setup, Encrypt, Extract, and Decrypt [7] [18]:

- **Setup**: The PKG generates its public parameters called *params* and its master secret *S*.
- **Encrypt:** To send an encrypted message *M* to the user with identity *ID*, an encryptor calculates the user public key Q_{ID} *based on ID and params.* He then takes *M, params* and Q_{ID} as input to generate ciphertext *C*.
- **Extract**: Given a user identity *ID*, the PKG computes the public key Q_{ID}. It then calculates user's private $D_{ID} = S\,Q_{ID}$, which is sent securely to the receiver.
- **Decrypt:** The receiver uses its private key D_{ID} and *params* to decrypt the ciphertext *C*.

b) Identity-Based Signature

Identity-based Signature (IBS) system is based on four algorithms: Setup, Extract, Sign and Verify [19].Setup and Extract are the same as those described in IBE.

- **Sign:** To sign a message M the signer with identity ID uses his private key D_{ID}, *params* and *M* as input to generate the signature σ.
- **Verify:** The user takes *params*, Q_{ID}, *M* and σ as input to verify signature σ on message *M*.

Figure 4 illustrates an Identity-Based Signature scheme.

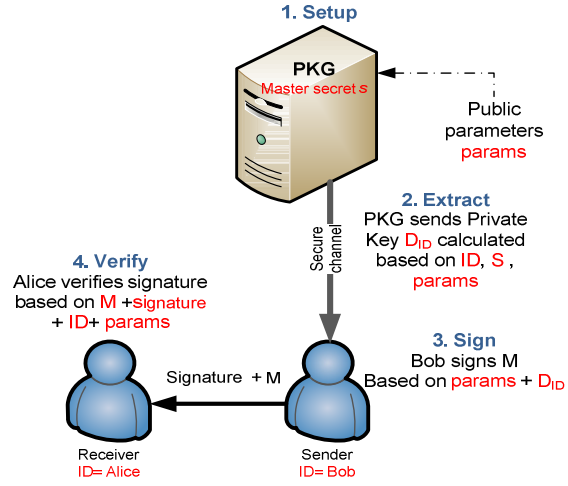

Fig. 4. Identity-Based Signature scheme

2) *Hierarchical Identity-Based Cryptography*

Hierarchical Identity-Based Cryptography (HIBC) is a variation of IBC that reflects an organizational hierarchy. Indeed, this cryptosystem does not have a single PKG that owns the master key and has to deliver private keys for all users. A root PKG is only required to produce private keys for domain-level PKGs, and it delegates private key generation and identity authentication to lower-level PKGs.

The identity of an entity is composed of the identity of every PKG in the user's ancestry. A at level t, this identity is given by its ID-tuple (ID1, ID2..IDt),where IDi corresponds to the ith level node. Each PKG at level t may derive the private keys for its immediate children with ID-tuples of the form (ID1, ID2…IDt, IDt+1).

Encryption and signature work similarly to IBE and IBS. But, there is a setup algorithm for PKG root and a setup algorithm for lower-level PKG [6]. The ID-tuple is used as the public key [20] [21]. Only the root PKG has public parameters which are used by lower level PKG [6]. The HIBC security depends on these parameters since they are used as input in signature (and verification) and encryption (and decryption) operations.

B. Integration of identity-based cryptography in NDN

The proposed solution is hybrid in a sense that it uses the HIBC (with its multi-level PKGs) and Public Key Infrastructure (PKI). The NDN name keeps its hierarchical structure. In addition, it will include the producer identifier and information on the editing period or the validity period of the content. This name is used as an HIBC public key.

To illustrate how our solution operates, we consider the example (Fig.5) of a paper written by a student (with ID 13572312) at telecom-parisTech.

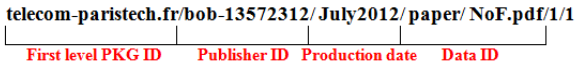

Fig. 5. Name structure in NDN with the HIBC integration

The part "*telecom-paristech.fr/bob-13572312*" identifies the producer in a unique way since every student or employee is identified by a unique ID (13572312 for Bob). The part "*July2012*"indicates the publication date of this paper, and finally the *"paper/ NoF.pdf"* identifies a specific content issued by this publisher on that date. The root PKG is directly attached to telecom-parisTech, which is responsible for generating private keys for its employees and students. Every employee or student generates a private key for each produced content and is responsible for authenticating the content and ensuring the uniqueness of its identity.

The public parameters of the root PKG are recovered from the field "signed info" of the Data packet (Fig.1). They are combined with the content name to verify the packet signature. Since HIBC security depends on these parameters, we propose to bootstrap trust in these parameters using a PKI. Indeed, the field "signed info" may contain the digital signature of the public parameters. The private key of the first level PKG (directly attached to the root PKG) is used to compute this signature. Trust in the corresponding public key can be obtained with a certificate (recovered as an NDN data). This certificate is signed by a private key based on the identity of a trusted third party with known public parameters. One certificate is then required for a set of producers (in this example a single certificate for all students and employees of telecom-parisTech). Figure 6 describes the set of exchanged messages between a requester and a data possessor when NDN adopts our solution. In this figure, the used keys PK1, PK2 and PK3 are respectively the private keys of the first level PKG telecom-paristech, data and certification authority.

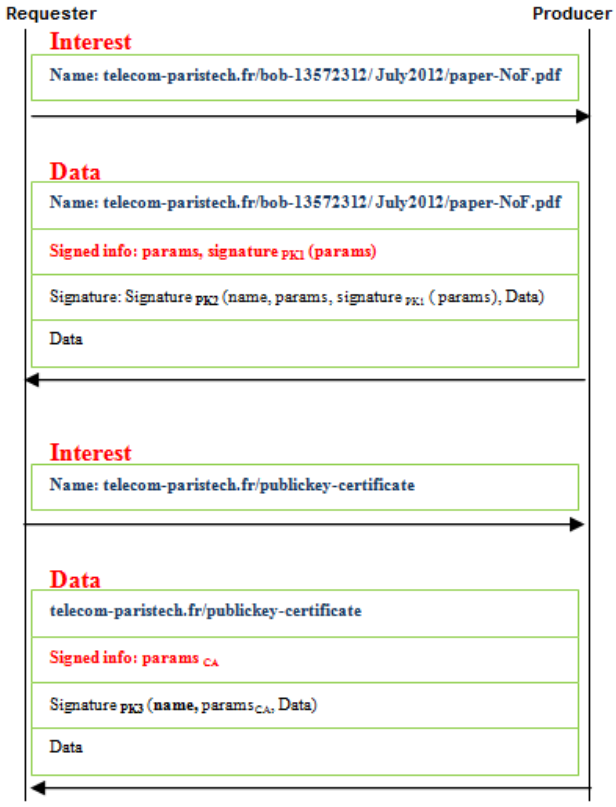

Fig. 6. Packet exchanges in NDN with HIBC and PKI

In order to ensure access control and confidentiality in case the number of authorized entities is limited and known by the content producer, a symmetric encryption can be used. Indeed, it offers a much lower computing cost than asymmetric encryption. The key used can be sent to the authorized entities encrypted with their identities (hierarchical identities of authorized entities act as HIBC public keys). It can be retrieved along with their data. The corresponding Data packet then contains content encrypted with the symmetric key and all the encryptions of symmetric key (one per entity encrypted with its identity using Hierarchical Identity-Based Encryption). Although such a packet causes overhead, it allows the requester to retrieve nearest copy of content and to take advantage of caching capabilities.

The producer must know the root PKG public parameters of authorized entities. He can retrieve them as NDN data. The number of parameters to retrieve is less important than the number of public keys (in the case of PKI) since several entities may belong to the same root PKG.

Our proposal bypasses the attack described previously in section II.C since a direct link between the name and content is provided. It reduces also the number of used certificates. Indeed, a single certificate is required for a set of producers (in this example a single certificate for all students and employees of telecom-parisTech). In addition, it facilitates decryption keys distribution for confidentiality and access control. Finally,

it represents a solution for the key revocation problem because the Content name may contain information about the expiration date of the generated key. Table I summarizes the advantages of HIBC-based NDN compared with NDN.

TABLE I. NDN COMPARISON WITH AND WITHOUT HIBC

Security service	CCN	CCN with HIBC
Validity	Requires a link between the public key and the name	Ensured
Provenance	Requires links between: • The Publisher real-world identity and the name • The publisher real-world identity and the public key • The public key and the name	Ensured
Access control & confidentiality	A key management problem	Symmetric key sent encrypted with the identities of authorized entities
Pertinence	Ensured: meaningful name	Ensured

IV. RELATED WORK

Although several enhancements have been made for NDN, but the only security-oriented enhancement based on the naming system we could identify is the name-based trust and security approach for CCN proposed in [22]. In the following, we analyze this approach and compare it with our solution.

The proposal in [22] is built on top of identity-based cryptography (IBC). The identity used as public key can be derived from content's owner or provider identity. It can also be derived from the name or prefix of content. The signed info is composed of sign_id and pkg_sp fields: sign_id represents the identity used for signature verification and pkg_sp represents the PKG public parameters.

If content's owner identity or the prefix of data name is used as a public key, only a link between a public key and a part of the name is established. An attack can be easily launched. The following example illustrates this attack:

- Bob is a student in Telecom-ParisTech. His marks are signed with the administration private key. They are published under the name telecom-paristech.fr /administration/studentsmarks/Bob
- By hearing an Interest packet with this name, Bob produces false content.
- He puts in the *sign_id* field his identity and sends to the requester a Data packet containing the same name, a false content, its identity, *params* and digital signature (using his private key).
- By receiving this content, the requester cannot perceive the attack.

If content name is used as a public key, a name registration service (NRS) is introduced. Indeed, before any content publication, a name registration should be performed. Thus, an additional entity to NDN architecture is introduced.

In addition, the use of Hierarchical Identity-Based Cryptography offers a more scalable architecture since the private key distribution and ID authenticity workload are shared by multiple PKG. Finally, HIBC is more adapted to NDN. Public keys in this system are better suited to the hierarchical format of NDN names. It eliminates content registration since every PKG is responsible of the unicity and the authenticity of its children ID.

V. CONCLUSION

CCN/NDN project is one of the major ICN candidates for Future Internet architectures. Its fundamental research challenge is to offer an architecture that solves today's Internet problems related to routing, mobility, fast forwarding, and security. It offers an excellent platform to ensure theses challenges. Both traditional and new trust mechanisms can be deployed.

In this paper, we first presented an analysis of CCN/NDN project. We focused in particular on the security and naming systems. We identified some limitations in proposed solution for security system. Then, we proposed an enhancement to this system, capable of solving the identified attacks. Our solution is based on a hybrid scheme which combines public-key infrastructure (PKI) and Hierarchical Identity-Based Cryptography (HIBC).
It fits in perfectly with the structures of the various objects of this project, and it does not require any change in the naming structures which makes its validation implicit.

REFERENCES

[1] BengtAhlgren, Christian Dannewitz, Claudio Imbrenda, Dirk Kutscher, BörjeOhlman: A survey of information-centric networking. IEEE Communications Magazine 50(7): 26-36 (2012).

[2] G. Kunzmann, D. Staehle. NetInf Content Delivery and Operations .SAIL project deliverable. D.B.2. May 2012.

[3] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, I. Stoica, *A Data-Oriented (And Beyond) Network Architecture.* ACM Sigcomm 2007.

[4] V. Jacobson, D.K. Smetters, J.D. Thornton, M. Plass, N. Briggs, and R. Braynard. Networking named content. Communications of the ACM, 55(1):117–124, 2012.

[5] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J.D. Thornton, D.K. Smetters, B. Zhang, G. Tsudik, D. Massey, C. Papadopoulos, et al. Named data networking (ndn) project. Technical report, PARC, Tech. report ndn- 0001, 2010.

[6] C. Gentry and A. Silverberg. Hierarchical id-based cryptography. Advances in Cryptology ASIACRYPT 2002, pages 149–155, 2002.

[7] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. Advances in CryptologyCRYPTO 2001, pages 213–229. Springer, 2001.

[8] V. Jacobson. Congestion avoidance and control. In ACM SIGCOMM Computer Communication Review, volume 18, pages 314–329. ACM, 1988.

[9] V. Jacobson, D.K. Smetters, J.D. Thornton, M.F. Plass, N.H. Briggs, and R.L. Braynard. Networking named content. In Proceedings of the 5th international conference on Emerging

networking experiments and technologies, pages 1–12. ACM, 2009.

[10] A. Baid and D. Raychaudhuri. Wireless access considerations for the mobilityfirst future internet architecture. Proceedings of IEEE Sarnoff Symposium 2012, Newark, NJ, May 2012.

[11] A. Anand, F. Dogar, D. Han, B. Li, H. Lim, M. Machado, W. Wu, A. Akella, D.G. Andersen, J.W. Byers, et al. Xia: an architecture for an evolvable and trustworthy internet. In Proceedings of the 10th ACM Workshop on Hot Topics in Networks, page 2. ACM, 2011.

[12] T. Anderson, K. Birman, R. Broberg, M. Caesar, D. Comer, C. Cotton, M. Freedman, A. Haeberlen, Z. Ives, A. Krishnamurthy, et al. Nebula-a future internet that supports trustworthy cloud computing. White Paper, 2010.

[13] D.K. Smetters and V. Jacobson. Securing network content. Technical report, PARC, 2009.

[14] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 2560 (Proposed Standard), June 1999.

[15] Paolo Gasti, Gene Tsudik, Ersin Uzun, Lixia Zhang: DoS and DDoS in Named-Data Networking CoRR abs/1208.0952: (2012).

[16] A. Ghodsi, T. Koponen, J. Rajahalme, P. Sarolahti, and S. Shenker. Naming in content-oriented architectures. In Proc of SIGCOMM Workshop on ICN, 2011.

[17] L.B.R.I. Mohamed ABID. Des mécanismes d'authentification basés sur l'identité de l'utilisateur pour renforcer la sécurit´e des réseaux. PhD thesis, Université de Technologie de Compiègne, 2011.

[18] A. Ahmad, A. Biri, H. Afifi, and D. Zeghlache. Tibc: Trade-off between identity-based and certificateless cryptography for future internet. In Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on, pages 2866–2870. IEEE, 2009.

[19] A. Kumar and H.J. Lee. Performance comparison of identity based encryption and identity based signature.

[20] H.W. Lim. On the application of identity-based cryptography in grid security. Information Security Group, 2006.

[21] R. Patra, S. Surana, and S. Nedevschi. Hierarchical identity based cryptography for end-to-end security in dtns. In Intelligent Computer Communication and Processing, 2008. ICCP 2008. 4th International Conference on, pages 223–230. IEEE, 2008.

[22] Xinwen Zhang, Katharine Chang, HuijunXiong, Yonggang Wen, Guangyu Shi, Guoqiang Wang: Towards name-based trust and security for content-centric network. ICNP 2011: 1-6.