ISSN No. 0976-5697

Volume 6, No. 3, May 2015 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An authentication and authorization approach for the network of knowledge architecture

T. Babu Rao
M.TECH (student)
Department of Computer Science and Engineering
Bapatla College of Engineering, Bapatla.
babu.ashok908@gmail.com

Dr Shaik Nazeer
Associate professor
Department of computer science and Engineering
Bapatla College of engineering, Bapatla
drnazeersk@gmail.com

T. D. Ravi Kiran
Assistant professor,
Department of Information Technology,
PVP Siddhartha Institute of Technology, Vijayawada.
tdrk002@gmail.com

M.Sundarababu
Assistant professor
Department of Information Technology
PVP Siddhartha institute of Technology, Vijayawada
sundar539@gmail.com

Abstract: Several projects propose an knowledge centric approach to the network of the future. Such an approach makes efficient content distribution possible by making knowledge retrieval host-independent and integration into the network storage for caching knowledge. Requests for particular content can, thus, be satisfied by any host or server holding a copy. One well-established approach of knowledge centric networks is the Network of Knowledge (Network knowledge architecture) architecture, the approach is based on the Publish/Subscribe model, where hosts can join a network, publish data, and subscribe to publications. The Network knowledge architecture introduces two main stages namely, the Publication and Data Retrieval through which hosts publish and retrieve data. Also, a distributed Name Resolution System (NRS) has been introduced to map the data to its Originators. The NRS is vulnerable to masquerading and content poisoning attacks through invalid data registration. Therefore, the paper proposes a Registration stage to take place before the publication and data retrieval stage. This new stage will identify and authenticate hosts before being able to access the Network knowledge architecture system. Furthermore, the Registration stage uses (cap) abilities-based access policy to mitigate the issue of unauthorized access to data objects. The proposed solutions have been formally verified using formal methods approach.

I. INTRODUCTION

Knowledge-Centric Networking (KCN) is an emerging paradigm envisaged by a growing body of researchers. KCN architectures leverage the role of knowledge as the building block of the Internet architecture as opposed to the current end-host oriented paradigm. KCN architectures have better support for multicast, mobility, and security (Fotiou et al., 2012). In KCN architectures, efficient knowledge dissemination is expected to be supported by dispersing an knowledge item in many network locations using in-network caches and Content Distribution Networks (CDNs) (Sipat et al., 2009).

The Network of Knowledge architecture is an KCN approach developed as part of the Scalable and Adaptive Internet Solutions (SAIL) project (Edwall, 2013). The SAIL Network knowledge architecture project is centred around a well-defined set of architecture invariants (such as unique naming, location-independence and a strict knowledge-centric service model) and puts particular emphasis on supporting multi-technology/multi-domain interoperability (Kutscher et al., 2013). The project also takes into account developments elsewhere in KCN research

In Network knowledge architecture, data objects such as web pages, articles or videos are named and identified using the Uniform Resource Identifier for Named Knowledge (URI-ni) format (Baker et al., 2012), hence these objects are referred to as Named Data Objects (NDOs). The Network knowledge architecture is composed of three main components:

The Originators: These are Network knowledge architecture nodes acting as source of NDOs and willing to make these objects accessible to Benefactors.

The Benefactors (or Requesters): These are Network knowledge architecture nodes that request specific NDOs.

The Network knowledge architecture System: This is represented as a network of Network knowledge architecture routing/forwarding nodes, spanning over the inter-domain topology along which payload data is delivered. Three types of nodes are needed for the operation of the Network knowledge architecture system: (1) cache-capable nodes to support the functionality of in-network caching of NDOs (2) Name-Based routers which route and forward NDOs towards Benefactors and (3) the Name Resolution System (NRS) is a distributed system which is aware of the network locations where an NDO might potentially be available for retrieval. Generally speaking, the operation of the Network knowledge architecture goes through two stages: the Publication Stage, where Originators publish their NDOs to the Network knowledge architecture system. The Data Retrieval Stage, where Benefactors request specific NDOs from the Network knowledge architecture system. The requested NDOs will be then forwarded to towards the requesting Benefactors. These two stages will be explained in Section 2.

Currently, the research concentrates mainly on defining the Network knowledge architecture overall architecture as well as the structure of the Network knowledge architecture messages such as the Get-Req/ Get-Resp and Publish-Req/Publish-Resp (more details about these messages in Section 2). The security-related research is still at the stage of defining threat models, highlighting various possible attacks as in Edwall (2013) and defining basic security measures as part of the URI-ni naming scheme (Baker et al., 2012). Therefore, this paper introduces a new approach to address the authentication and authorization issues of

CONFERENCE PAPER
4th National Conference on Recent Trends in Information Technology 2015 on 25/03/2015
Organized by Dept. of IT, Prasad V. Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada-7 (A.P.) India

implementing the Network knowledge architecture.

Our main concern here is the security of the Publication Stage, where Originators publish NDOs to the Network knowledge architecture system. Another major concern is to address the issue of unauthorized access to published NDOs. For a secure publication, two requirements need to be verified namely, the authenticity of Originators and the validity of the published NDOs. Indeed, a malicious node might spoof another Originator ID and publish invalid NDOs. This is very similar to poisoning attacks against Domain Name Server (DNS) or routing tables (Gregg, 2006). To stop such attacks, we need to thwart masquerading threats; therefore, a pre-publication stage, called Registration Stage, is proposed in this paper. During the Registration Stage, both Originators and Benefactors need to authenticate themselves with the Network knowledge architecture system. Therefore, as part of the Registration Stage, we propose a new authentication protocol based on the ID-Based Cryptography (IBC) (Shamir, 1985). The IBC helps to certify the messages sender as the real owner of the NDO that will update the Network knowledge architecture system. The main advantage of using the IBC over traditional Public Key Infrastructure is that since the public key will be derived from the nodes' identifiers, IBC eliminates the need for a public key distribution infrastructure details about IBC are in Section 5.2.

To address the issue of an unauthorized access of NDOs, the paper will introduce an authorization and access control approach based on the (cap)abilities-based access control policy (Gollmann, 2011; Chen, 2014). The (cap)abilities based access control policy has been used to secure the microkernel of the Valencia's Simple Tasker (VSTa) operating system. The proposed authorization (access control) approach is integrated with the proposed authentication protocol as core components of the Registration Stage tool (Lowe et al., 2009). In summary, the paper's contribution is to introduce an integrated authentication and authorization approach that achieves the following

- To verify the identity of data Originators and Benefactors through a novel ID-Based authentication protocol.
- To tackle the issue of unauthorized access to published data by using a cap(ability)-based access policy.

The proposed security measures have been verified using a formal methods approach based on the Casper/FDR. The rest of this paper is organized as follows: the Network knowledge architecture system is described in Section 2. Section 3 defines the security problem of the Registration Stage of the Network knowledge architecture. Section 4 describes some related work. The proposed Registration Stage along with the authentication and authorization mechanisms are presented in Section 5. The paper concludes in the conclusion section.

II. AN OVERVIEW OF THE NETWORK KNOWLEDGE ARCHITECTURE:

In Network knowledge architecture, Originators advertise potential publications in the Network knowledge architecture system and serve the data contents upon receiving requests. The Network knowledge architecture system acts as a middleman between Originators and Benefactors and is involved in configuring the forwarding path for data delivery (Edwall, 2013). Three pairs of messages have been defined as part of the Network knowledge architecture:

The GET-REQ/GET-RESP messages: The GET message is used by a requester to request an NDO from the Network knowledge architecture network. A node responding to the GET message would send a GET-RESP that is linked to the GET request using the message-Id (msg-id) from the GET message.

The PUBLISH-REQ/PUBLISH-RESP messages: The PUBLISH message allows a Originator to push the name and a copy of the NDO to the network. A node receiving a PUBLISH message may choose to cache the NDO according to local policy and avail-ability of resources and returns PUBLISH-RESP message, other-wise, it may choose to forward the message to other nodes without sending the response message.

The SEARCH/SEARCH-RESP messages: The SEARCH message allows the requester to send a set of query tokens containing search keywords. The node that receives the Search message, will respond if the NDO is in its own cache or forward the search message. The message are supposed to be transported over a convergence layer(cl) protocol. As stated in etal.(2013), no cl protocol has been defined yet but any protocol that allows Network knowledge architecture messages to be passed without loss of knowledge can be used as a Network knowledge architecture Convergence Layer (Network knowledge architecture-CL) protocol. These three pairs of message define the transactions of the Publication and Data Retrieval Stages as follows:

1. The Publish Stage: Originators publish their NDOs to the Network knowledge architecture system by sending the PUBLISH-REQ message to the first hop node which might choose to cache the included knowledge and responds with a PUBLISH-RESP message. Otherwise, it passes the PUBLISH-REQ to the next hop route. A node that caches NDO might update the NRS with the location of the NDO.
2. The Data Retrieval Stage: As shown in Fig. 1, the Network knowledge architecture combines two modes for data retrieval:
   (a) The name resolution: In this mode, the Originator publishes an NDO using PUBLISH message with a Name Resolution Service (NRS). In this case, a requester will approach the NRS first (using the GET message) which will direct him to the knowledge Originator.

   (b) The name-based routing: In this mode, the GET message will be forwarded hop-by-hop between Network knowledge architecture nodes until a cached copy of the requested NDO is found or the original Originator is reached.

III. PROBLEM DEFINITION

In Network knowledge architecture, like other KCN architectures, the primary goal is to retrieve content from the network, regardless of their locations. As described in the previous section, the Network knowledge architecture has

CONFERENCE PAPER
4th National Conference on Recent Trends in Information Technology 2015 on 25/03/2015
Organized by Dept. of IT, Prasad V. Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada-7 (A.P.) India

defined the required messages to publish and retrieve NDOs. However, there is no specified approach to secure these messages, rather, security in Network knowledge architecture is mainly based on object naming scheme. With the Network knowledge architecture naming scheme, each NDO is given a unique identifier (ID) with cryptographic properties. Together with additional metadata, the ID can be used to verify data integrity, owner authenticity and several other security properties (Dannewitz et al., 2010). The scheme relies on proven mechanisms like cryptographic hashing and public-key certificate chains to reduce the risk of vulnerabilities. In this sense, Network knowledge architecture's view of security is mainly focused on knowledge security regardless of the security of the underlying transport protocols.

The authors believe the fact that despite the migration of the predominant usage of the Internet from host-centric to the knowledge centric model, the underlying content delivery mechanism remains host-centric. As a consequence, some conflicts arise due to the usage of host-centric mechanisms in anknowledge centric networks, such as content identification and resolution, trust establishment and security. Therefore, we believe in the need for a hybrid security approach that addresses security at both knowledge and infrastructural levels.

As explained in the Introduction section, one serious threat against the Network knowledge architecture is when a fake Originator registers invalid NDOs with the NSR during the Publication Stage. Obviously, this poisons the whole system, leads to invalid responses to Benefactors' requests which is considered as a form of Denial of Service (DoS) attacks. Another threat is when unauthorized users get access to data due to the lack of access control and authorization mechanisms. The solution presented in this paper strives to address these issues by holding Originators and Benefactors accountable for their actions and making sure that NDOs could only be published and accessed by identified parties. To achieve this, our approach proposes that Originators and Benefactors need initially to go through a Registration Stage where they will be authenticated and given security tokens that define their permissions. The proposed authentication mechanisms in the Registration Stage is based on the ID-Based Cryptography approach, while the pro-posed authorization mechanism is based on the (cap)ability based access control policy. After a successful registration, Originators and Benefactors could use the Network knowledge architecture system to publish and request NDOs.

IV. ID-BASED CRYPTOGRAPHY (IBC)

The IBC is a cryptographic scheme was first proposed by Shamir (1985). The scheme enables users to communicate securely and verify each other's signature without exchanging public or private keys. However, the scheme requires the presence of Trusted Key Generation (TKG) centres.

IBC's operation: Unlike the normal Public Key Infrastructure (PKI) where a TKG randomly generates pairs of public/private keys, each node in IBC chooses its identifier (address or name) as a public key. Practically, any publicly known knowledge that uniquely identifies the node could be used as a public key. The TKG generates the corresponding private key and securely distributes it to the node. When a node (A) wants to communicate with another node (B), node A will sign the message using its private key and encrypt the result with the node B's public key. Upon receiving the message, node B will decrypt the message using its private key and verify the signature using node A's public key. The IBC represents an efficient and easy to implement system which removes some of the overhead encountered in PKI for key management and digital certificate issuance/revocation.

However, the security of the IBC is based on the secrecy of the private key.

To deal with this issue, the node needs to combine additional knowledge such as timestamps to their identifiers when generating the public key. This procedure will guarantee a periodic update of the public key. However, it introduces a key-management problem where all users must have the most recent public key for the node.

4.2.Authorization and access control

Most computer security uses the access control mode shown in Fig. 2, and this model comprises the following elements (Paquet, 2009):

- Principals/subjects: These are the source of access requests.
- Requests to perform operations on objects.
- A reference monitor: This is a guard for each object that examines access requests for the object and decides whether to grant it.
- Objects: These represent resources such as files, devices, or processes..

The reference monitor bases its decision on the principal making the request, the operation in the request, and an access rule that controls which principals may perform that operation on the object. To do its work the monitor needs a trustworthy way to know both the source of the request (via authentication process) and the access rule. Obtaining the source of the request is called authentication; interpreting the access rule is called authorization. Thus authentication answers the question "Who said this?", and authorization answers the question "Who is trusted to access this?". Usually the access rule is attached to the object; such a rule is called an Access Control List or ACL. For each operation the ACL specifies a set of authorized principals, and the monitor grants a request if its principal is trusted at least as much as some principal that is authorized to do the operation in the request (Paquet, 2009). In the context of KCNs, access control policies are needed to guarantee that NDOs could be published by authorized sources and the access to these NDOs are only given to authorized Benefactors.

4.3. Verifying security protocols using Casper/FDR:

Previously, Analysing security protocols used to go through two stages. Firstly, Modelling the protocol using a theoretical notation or language such as the CSP (Lowe et al., 2009). Secondly, verifying the protocol using a model checker such as Failures-Divergence Refinement (FDR) (Formal Systems, 1993). However, describing a system or a protocol using CSP is a quite difficult and error-prone task; therefore, Gavin Lowe has developed the CASPER/FDR tool to model security protocols, it accepts a simple and

human-friendly input file that describes the system and compiles it into CSP code which is then checked using the FDR model checker. Casper/FDR has been used to model communication and security protocols as in Aiash and Aiash (2013). The CASPER's input file that describes the systems consists of eight headers as explained in Table 1.

V. THE PROPOSED SOLUTION

As discussed earlier, we propose a new stage to take place before the Publication and Data Retrieval stages. This section discusses our proposal of using the IBC protocol to secure the Registration procedure of the Network knowledge architecture.

5.1. System definition

In Network knowledge architecture, data sources publish NDOs by registering a name/ locator binding with the NRS using the Publish message or announcing routing knowledge in a routing protocol. Any Network knowledge architecture node holding a copy of the NDO can optionally register the copy with the NRS. Benefactors will approach the NRS requesting for a specific NDO, and the NRS will first resolve the NDO into a set of available locators and then retrieve the a copy of the data from best available source.

In order to provide a secure data publication and retrieval, we advocate the need for a registration stage during which both Originators and Benefactors need to identify themselves to the NRS and acquire a security tokens that define their privileges and access rights. Two types of security tokens namely, Object and Subject tokens are generated by the NRS. During the Registration Stage, a node needs to disclose its role (Originator, Benefactor or both) and after the authentication process, it will receive corresponding tokens (subject, object or both). The security tokens will define security levels for NDOs as for Objects Tokens (ObjToken) and for Benefactors as for Subject Tokens (SubToken). The rules of access will be checked and enforced by the NRS which will be acting as a Reference Monitor, more details about the authorization and access control approach is in Section 5.3.

5.2. The proposed authentication protocol

As shown in Fig. 3, and based on the notations, the secure Registration Stage using the IBC goes as follows:

Msg1: TKG→Orig: {SK(Orig)}{K1}

Msg2: TKG→NRS: {SK(NRS)}[K2}

The TKG provides the two communicating parties (Pub, NRS) with their private keys SK(Pub), SK(NRS) in messages 1 and 2. These messages are encrypted using the pre-shared secret keys K1, K2, respectively.

Msg3: Pub→NRS: {Reg-Req} pK(NRS)},{h(Reg-Req)} {SK(Orig)}

The originator sends a Register-Request (Reg-Req) packet which includes knowledge about the node role (Pub or Sub) and a one-time message ID in Msg3. The content of this message is encrypted using the NRS's public key (which is publicly known) and digitally signed using the private key of the originator.

Msg4: NRS→Orig: {Reg-Res), ObjToken}{PK(Orig)},

{h(Reg-Resp, ObjToken)}{SK(NRS)}

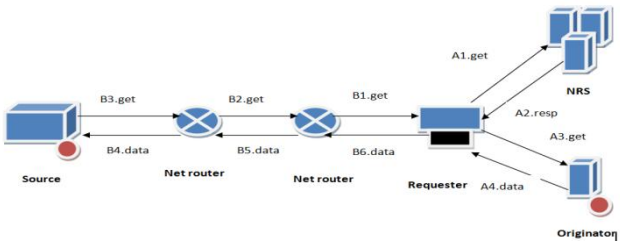


Figure.1. The Network knowledge Message Flow. The Name Resolution mode, The Name-Based Routing

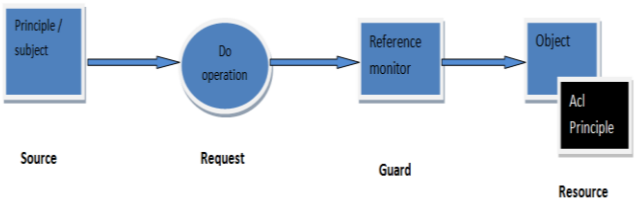
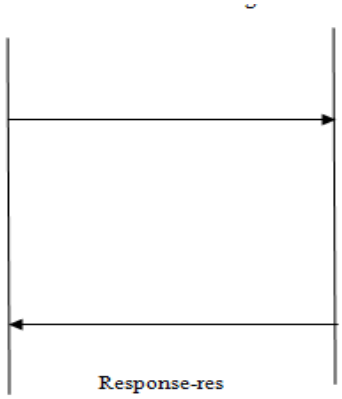


Figure 2.The fundamental model of access control

Upon receiving msg3, the NRS will use its private key SK(NRS) to decrypt the message and then verify the signature using the Pub's public key PK(Pub). Finally, the NRS will hash the included Reg-Req and compare the result with the received signed value. Only if the two values are equal, the NRS composes a Register-Response (Reg-Resp) packet as msg4 which includes the received message ID (Msg-ID) and an Object Token (ObjToken). This message is encrypted using the Pub's public key and digitally signed using the NRS's private key. The Pub will check the included Msg-ID and only when the check succeeds, the Pub authenticates the NRS and accepts the token. The protocol's steps are shown in Fig. 4.

It is worth to point out that the same proposed protocol should be used for Registering Benefactors before accessing NDOs. The only difference in this case will be the use of Subject Token (SubToken) instead of the Object Token. At the end of the Registration Stage, the NRS will have a list of all authorized Benefactors and Originators.

CONFERENCE PAPER
4th National Conference on Recent Trends in Information Technology 2015 on 25/03/2015
Organized by Dept. of IT, Prasad V. Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada-7 (A.P.) India



The Registration stage

5.2.1. Formal analysis using Casper/FDR

To formally analyze the proposed solution, we simulate the system using Casper/FDR tool. The eight headings of the simulated system are described below.

The #Free Variables section defines the variables and functions that are used in the protocol. The term "Free Variables" refers to the fact that these variables will be represented by instances of actual values when running the protocol. For instance, the variables na, nb, seq2, n1 are of type Nonce. The functions PK and SK return an agent's public key and private key, respectively. These functions will be defined later in the #Functions. The "InverseKeys" keyword defines the keys that are inverses of one another like PK and SK.

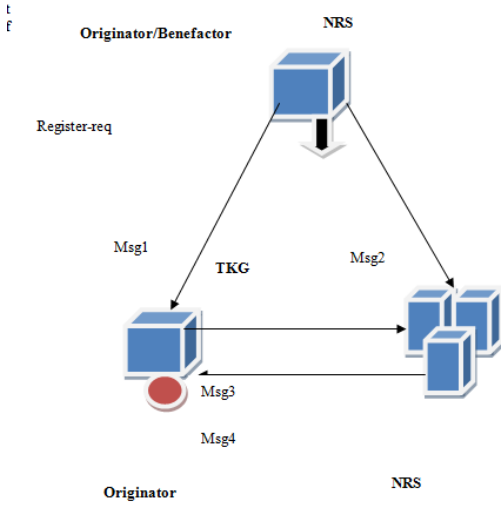


Figure 4.proposed security protocol

Table I. The headers of Casper's input file

The header	Description
# Free variables	Defines the agents, variables and functions In the protocol.
# Processes	Represents each agent as a process
# Protocol description	Showsall the messages exchanged between the agents.
# Specification	Specifies the security properties to be checked.
# Actual variables	Defines the real variables, in the actual system to be checked.
# Functions	Defines all the functions used in the protocol.
# System	Lists the agents participating in the actual system with their parameters instantiated.
# Intruder knowledge	Specifies the intruder's knowledge and capabilities.

#Free variables,
Originator
NRS: Agent,

na, nb,seq2, n1: Nonce
MID :
MessageIDSubToken
:SubjectTokenObjToken
: ObjectToken

PK : Agent→PublicKey
SK :
Agent→PrivateKey K1,
K2 : PreSharedKey
TKG : Server
M, m2,Ack : Messages
InverseKeys = (PK; SK), (K1, K1),
(K2, K2)
h :HashFunction

EIDPre:EIDPrefix
Hash1: hashvalues

The #Processes heading defines each involved agent in the protocol as a CSP process. The keyword "knows" defines the knowledge that the agent in question is expected to have at the beginning of the protocol run. In our system, INITIATOR, RESPON-DER and SERVER are the names of the process representing the Originator, the Name Resolution Service and the Trusted Ticket Granting, respectively. The values within the brackets and after the "knows" keyword define the agents' initial knowledge.

#Processes

INITIATOR(Pub, NRS, TKG, K1, nb, m, MID) knows PK(Orig)

PK(NRS), SK(Pub)
RESPONDER(NRS, TKG, K2, m2, SubToken, ObjToken) knows

PK(Pub), PK(NRS), SK(NRS)
SERVER(TKG, Pub, NRS, K1, K2, na) knows PK, SK(Orig), SK(NRS)

Where the notations I_ NRS, I_Pub and I_TKG

represent the case where the Intruder impersonates the NRS, Pub and TKG, respectively. This is an active Man-in-the-Middle attack; the Intruder intercepts and replays messages 1 and 2. Since the Pub is not sure of the identity of the NRS, the intruder manages to impersonate the NRS and fools the Pub to use its (rather than the NRS's) public key to encrypt message 3a. Consequently, the message ID will be compromised, and the Pub will run the protocol mistakenly believing it is with the NRS, while in reality it is with the Intruder. As a consequences of this attack, the intruder will be able get the name/location binding at the publication stage and mix them in away to deny Benefactors from getting the requested data and hence launch a DoS attack.

There are two ways to stop such attack: firstly using an out-of-band approach in which the Pubs should be pre-configured to use an authoritative NRS in its domain or network. This could be simply achieved during the network configuration in a similar way to configuring the default DNS server or the default gateway in a network. Secondly, by requesting the NRS to explicitly identify and authenticate itself to the Pub via providing a digital certificate that could be verified by a trusted third party such as the TKG or a Certificate Authority (CA).

5.3 The authorization and access control

During the Registration Stage, once a party (Benefactor or Originators) is authenticated, the NRS will generate a security token. Two types of tokens are generated: Object Tokens, attached with the published NDOs and Subject Tokens attached with Benefactors. These tokens define objects and subjects abilities. An ability is represented as a dot-separated sequence of numbers, called a label. So, an ability is a string :i_1:i_2:i_3…i_n for some value n where i_1, i_2, i_3…; i_n are integers. Examples of abilities are .1.2.3, .4, or 10.0.0.5. Upon successful registration, both NDOs (objects) and Benefactors (subjects) will be given labels (abilities). Access for an NDO is given if the NDO's label is a prefix of the Benefactor's label. For instance, an NDO with a label ".3" could only be accessed by Benefactors with abilities like ".3.1", ".3.2.3", ".3.1.2"...etc. This way, whenever an authenticated Benefactor requests an NDO, he needs to present the right label that confirms his right to access the NDO.

With the proposed protocol in Section 5.2, labels are generated by the NRS so Benefactors can't promote themselves to access other NDOs. Furthermore, to maintain the integrity of the labels and making sure they have not be tampered with, labels are integrated in a security tokens (SubToken, ObjToken) which are hashed and digitally signed by the NRS. Additionally, the security tokens are time stamped and have expiry date after which new tokens are needed. When generating the token, it should be noted that no Subtokens have a validity period longer than that of the corresponding ObjToken. Using the time stamp and the expiry time will minimize the risk of a both active and passive replay.

VI. CONCLUSION

Building a scalable knowledge-centric architecture involves several challenges. This includes the development of an knowledge model and a naming framework which support efficient knowledge dissemination with improved security properties. The Network knowledge architecture is a promising architecture for data dissemination and retrieval that is based on the Publish/Subscribe model. In this model, Originators publish their data (through the Publication stage) to the NRS system which then launch these data to Benefactors upon request (through the Data Retrieval Stage). This paper explains how the Publication Stage might be vulnerable to masquerading and content poisoning attacks which might happen when an unauthenticated node publishes invalid data to the system. The paper also highlights the issue of an authorized access to published data. To address these challenges, an integrated authentication and authorization approach is proposed in the paper. While the proposed authentication protocol is based on the IBC protocol and achieves mutual authentication between Originators and the Network knowledge architecture system, the proposed authorization approach is based on cap(ability) access policy. The proposed approaches have been formally verified using formal method approach.

VII. REFERENCES

[1] Aiash M.A formal analysis of authentication protocols for mobile devices in next generation networks. Concurr Comput Pract Exp. http://dx.doi.org/10.1002/cpe. 3260.

[2] AiashM.A novel security protocol for address resolving in the location/ID split architecture. In: Network and system security NSS2013,vol.7873;2013.p.68–79.

[3] Baker H, StradlingR,FarrellS,KutscherD,OhlmanB. The named knowledge(NI) URI scheme: optional features, Technical Report, Network Working Group; 2012.URL ⟨http://tools.ietf.org/html/draft-hallambaker-decade-ni-params-03⟩.

[4] Chen HC.A multi issued tag key agreement with time constraint for homeland defense sub-department in NFC environment. JNetw Comput Appl 2014:88–98.

[5] Dannewitz C,GolicJ, Ohlman B,AhlgrenB. Secure naming for a network of knowledge. In:INFOCOM;2010.p.1–6. http://dx.doi.org/10.1109/INFCOMW. 2010.5466661.

[6] EdwallT.The network of knowledge: architecture and applications, Technical Report,SAIL Scalable and Adaptable Internet Solutions; 2013.URL ⟨http://www.sail-project.eu/wpcontent/uploads/2011/08/SAIL_DB1_v1_0_final-Public.pdf⟩. Formal Systems, Failures divergencerefinement:fdr2usermanualandtutorial; 1993.

[7] FotiouN, MariasF,PolyzosC. Access control enforcement delegation for knowledge centric networking architectures .In: Proceedings of the second edition of the KCNworkshop on knowledge centric networking, KCN'12,ACM, NewYork,NY,USA;2012.p.85–90. http://dx.doi.org/10.1145/2342488. 2342507.

[8] Gollmann D.Computer security. 3rd edition England:Wiley;2011.

[9] Gregg M.Certified ethical hacker. USA: Que Publishing;2006.
[10] Kutscher D,FarrellS, Davies E. The net in fprotocol, Technical Report, Network Working Group;2013.URL⟨http://tools.ietf.org/id/draft-kutscher-KCNrg-netinf- proto-01.txt⟩.
[11] Lowe G, Broad foot P ,Dillo way C,Hui M. Casper: a compiler for the analysis of security protocols.Oxford;2009.
[12] Paquet C. Implementing Cisco IOS network security. USA: Cisco Press;2009.
[13] Shamir A. Identity based crypto systems and signature schemes. In:CRYPTO84 on Advances in cryptology. Springer Verlag;1985.
[14] Sipat T, Al Qudah Z, Michael R. Content delivery networks: protection or threat? In: ESORICS, Lecture Notes in Computer Science.Springer;2009.p.371–89.
[15] Teemu K, Mohit C ,B yung Gon C, Andrey E,Hyun K,Scott S, Etal. A data oriented (and beyond)network architecture.In:Proceedings of the 2007conference on applications, technologies, architectures, and protocols for computer communications, SIGCOMM'07,2007.p.181192. http://dx.doi.org/10.1145/1282380. 1282402.
[16] Zhang X, Niu T, Lao F, Guo Z. Topology-aware content centric networking. In: SIGCOMM,2013, p.559–60. http://dx.doi.org/10.1145/2486001.2491729.

CONFERENCE PAPER
4th National Conference on Recent Trends in Information Technology 2015 on 25/03/2015
Organized by Dept. of IT, Prasad V. Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada-7 (A.P.) India